# ШЛЯХИ УДОСКОНАЛЕННЯ ДЕРЖАВНИХ МЕХАНІЗМІВ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

# WAYS OF IMPROVING STATE MECHANISMS IN THE SPHERE OF NATIONAL SECURITY

УДК 351:316.332
DOI https://doi.org/10.32782/pma2663-5240-2024.42.19

**Лашук О.С.**
к. наук з держ. упр.,
доцент кафедри менеджменту
та адміністрування
Національний університет
«Чернігівська політехніка»
ORCID ID: 0000-0002-6910-5674

**Лілікович П.В.**
к. наук з держ. упр.,
доцент кафедри формування
та розвитку
професійної компетентності персоналу
Пенітенціарна академія України
ORCID ID: 0000-0002-3166-1616

**Сенченко І.В.**
магістр з публічного управління
Національний університет
«Чернігівська політехніка»

*У статті запропоновано шляхи вдосконалення державних механізмів у сфері національної безпеки. Необхідність протистояти гібридним загрозам і швидким, різким змінам середовища безпеки зробила формування національної стійкості надзвичайно важливим. Це, зокрема, запровадження низки нових механізмів, які забезпечують адаптацію існуючих систем забезпечення національної безпеки до нових умов без істотних втрат та набуття здатності своєчасно та ефективно реагувати на широкий спектр ситуацій. Запропоновано заходи для належного зміцнення можливостей різних учасників для протидії інформаційним загрозам, які стає дедалі важче ідентифікувати.*

*Практика розробки та впровадження механізмів забезпечення національної стабільності вже певною мірою поширилася у світі. Як правило, країни починають із застосування відповідних механізмів до пріоритетних сфер. Найпоширенішими з них наразі є протидія тероризму, захист критичної інфраструктури, кібербезпека, реагування на надзвичайні ситуації природного та техногенного характеру, забезпечення безперервності бізнес-процесів. і т.д. Реалізація цих механізмів, в принципі, здійснюється шляхом прийняття відповідних програм, планів впровадження, методичних рекомендацій тощо.*

*Безпека, розвиток і можливість використання інформації в середовищі забезпечує адекватний захист від різних інформаційних загроз. Зростання медіа-атак, ботів і фейкових атак з початку повномасштабного вторгнення свідчить про те, що в сучасних реаліях країна має якнайшвидше реагувати та покращувати заходи інформаційної безпеки. Інформаційна безпека та культурні питання виставки – це питання, які виховують людину, суспільство та націю.*

*Варто зазначити, що проблема низького рівня інформаційної культури виникає в умовах, коли весь обсяг інформації спрямований на маніпулювання громадською думкою, свідомістю людини та подається за допомогою фізіологічних, психологічних методів і засобів сприйняття. Це знижує здатність людини критично сприймати, аналізувати та оцінювати отриману інформацію. У цьому випадку здатність до формування власної думки практично відсутня.*

**Ключові слова:** *національна безпека, механізм державного управління, повномасштабне вторгнення, кібербезпека, інформаційна безпека, розвиток, державна політика.*

*The article proposes ways to improve state mechanisms of strategic communications in the security and defense sector of Ukraine. The need to confront hybrid-type threats and rapid and sudden changes in the security environment makes the question of building national resilience relevant. This includes, in particular, the introduction of a number of new mechanisms that will allow the existing systems of ensuring national security to acquire the ability to adapt without significant losses to new conditions, to respond in a timely and effective manner to a wide range of threats that are becoming increasingly difficult to identify, to properly strengthen the capabilities of various actors etc.*

*The practice of developing and implementing mechanisms for ensuring national stability has already gained a certain prevalence in the world. As a rule, countries begin to apply appropriate mechanisms in their priority areas, among which the most typical currently are counterterrorism, protection of critical infrastructure, cyber security, response to emergency situations of natural and man-made origin, ensuring the continuity of business processes, etc. Implementation of such mechanisms is carried out, as a rule, by adopting relevant programs, action plans, guidelines, etc.*

*Security, development and viability of information in the environment creates adequate protection against various information threats. The increase in the number of media attacks since the beginning of the full-scale invasion, bots, and fakes shows that in today's realities, the state should counter and improve information security tools as soon as possible. The issue of information security and culture in times of war is a matter of educating a person, society and the state.*

*It is worth noting that in conditions where the entire volume of information is aimed at manipulating public opinion, human consciousness and is presented with the help of physiological and psychological methods and means of its perception, the issue of a low level of information culture arises, which causes a decrease in a person's ability to critically perceive, analyze and evaluate received information. In this case, the ability to form one's own opinion is practically absent.*

**Key words:** *national security, mechanism of state administration, full-scale invasion, cyber security, information security, development, state policy.*

**Постановка проблеми.** У сучасних реаліях війни важко недооцінити роль інформації як інструменту протистояння, хоча насправді вона є зброєю. Сучасна інформація дає змогу вигравати війни та політичні кризи без жодного пострілу, породжуючи та розпалюючи внутрішні протиріччя. Ця тактика є особливістю нового покоління – гібридних війн, у яких військовий фактор має першорядне, але не вирішальне значення. У сучасних реаліях фейкові новини або маніпуляційна інформація може посіяти в суспільстві страх та панічні настрої, дестабілізувати політичну та соціально-економічну ситуацію в Україні. Вторгаючись в український

інформаційний простір, ворог змінює інформаційне середовище. Протидіяти наративам агресора, фейкам та пропаганді ворога можна лише через дієві механізми захисту інформаційної сфери, підвищення рівня медійної грамотності населення та надання доступу до якісної інформації з перевірених джерел. Це все і є здатність держави створити умови для достатньо високого рівня захищення інформації.

Інформаційна безпека вимагає належного рівня інформаційної культури, тобто теоретичної та практичної підготовки особистості, що забезпечується навчанням медіаграмотності. Високий рівень критичного мислення створює умови для гармонійного розвитку та задоволення інформаційних потреб людини незалежно від виникнення інформаційних загроз. У роботі автором на прикладі Чернігівської області показано аспекти захисту інформаційної безпеки держави в умовах воєнного стану. Визначено основні напрямки захисту інформації та безпосередньо типові загрози інформаційній безпеці.

**Аналіз останніх досліджень і публікацій.** Проте, незважаючи на значні наукові дослідження у подальшій розробці, питання реалізації інформаційної безпеки для забезпечення національної безпеки потребує аналізу.

Оскільки питання інформаційної безпеки, яка є частиною національної безпеки, сьогодні є одним з найважливіших у державі, то йому приділяється значна увага вчених та практиків. Досліджували проблеми регулювання інформаційної безпеки в воєнний час такі вчені, як М. Дмитренко, Ю. Горбань, В. Бондаренко Ф. Медвідь, А. Пишна, Я. Михальский, О. Черевко, Д. Смотрич, Л. Браілко, Г. Удренас, Т. Француз-Яковець, І. Залєвська, І. Шинкаренко, та ін.

**Аналіз останніх досліджень і публікацій.** Питаннями інформаційної безпеки, проблемами її захисту, захисту національного інформаційного простору було присвячено багато наукових праць у таких вчених, як: Петрика В., В. Почепцова та інших фахівців. Однак, не зважаючи на значну увагу вищезазначених фахівців, дослідження механізмів державного регулювання у сфері інформаційної безпеки потребує уточнення, аналізу та дослідження.

**Постановка завдання. Мета статті** полягає у дослідженні основних механізмів державного регулювання захисту інформаційної безпеки та діяльності медійного простору у воєнний час на прикладі Чернігівської області, що впливає на забезпечення національної безпеки України вцілому. Особливим завданням є охарактеризувати суспільно-мобілізаційний потенціал державної інформаційної політики України в умовах повномасштабного воєнного вторгнення Російської Федерації та визначити її ефективність з огляду на характер протистояння та перспективи продовження бойових дій на прикладі Чернігівської області.

**Виклад основного матеріалу.** Державна політика захисту у сфері національної безпеки України спрямована насамперед на створення передумов для розвитку потенціалу інформаційної сфери України, забезпечення очікуваного розвитку та забезпечення того, щоб зовнішні негативні впливи не становили реальної небезпеки для України. Національна інформаційна безпека країни. Основним завданням систем захисту інформації є забезпечення стійкості цього розвитку та запобігання негативному впливу третіх осіб. Практична реалізація цього підходу до національної інформаційної безпеки може здійснюватися виключно за умов участі всіх внутрішніх суб'єктів інформаційних відносин та ефективної взаємодії між державою, громадянським суспільством, приватним сектором та окремими громадянами. Інтереси ефективного розвитку інформаційної сфери та спільного захисту таких розробок від зовнішніх загроз.

Національна інформаційна безпека є досить складним, системним і багаторівневим явищем, на яке можуть впливати такі чинники, як внутрішнє та зовнішнє середовище, глобальні зміни, внутрішньополітична ситуація та ситуація в інформаційному суспільстві. З огляду на події, що відбуваються в нашій державі, загрозам національній безпеці приділяється значна увага, оскільки вони впливають на економічний, політичний та соціальний простір [3].

Інформаційна безпека в Україні забезпечується шляхом захисту національного інформаційного простору від інформаційних загроз та сприяння сталому розвитку для реалізації життєво важливих інтересів і потреб громадян, суспільства і держави в інформаційній сфері.

У рамках національної інформаційної політики необхідно закласти основу для вирішення таких завдань, як формування єдиного інформаційного простору та вихід у глобальний інформаційний простір, забезпечення інформаційної безпеки людини, суспільства і нації, формування інформаційного простору. Формування демократично орієнтованої суспільної свідомості, становлення сфери інформаційних послуг, розширення правового регулювання суспільних відносин, у тому числі пов'язаних із отриманням, розповсюдженням і використанням інформації [4].

Повномасштабна війна зробила горизонтальні зв'язки між громадянами реальністю. Причиною цього стала нагальна необхідність

прискореного обміну важливою інформацією, яку не змогли забезпечити ні центральне телебачення, ні місцеві ЗМІ. Наприклад, у перші дні повномасштабного військового вторгнення до рф, коли кількість біженців від війни різко зросла, з'явилися оголошення про наявність палива для автомобілів на певних маршрутах та можливість знайти притулок на ніч або терміновий ремонт автомобіля була надзвичайно важливою інформацією. Популярною була також інформація про відсутність заторів на трасах та допомогу волонтерів. При цьому, як правило, перевага надавалася повідомленням, отриманим від родичів або близьких людей.

У травні 2022 року Київський міжнародний інститут соціології повідомив, що 76,6% українців використовують соціальні мережі як джерело інформації, телебачення – 66,7%, Інтернет (без соціальних мереж) – 61,2%, радіо – 28,4%, друковані видання ЗМІ – лише 15,7% респондентів (рис. 1).

При цьому 60,5% респондентів довіряють повідомленням в ефірі, а майже 54% – сайтам соціальних мереж [5]. Ці дані демонструють розуміння того, що соціальні мережі не були найнадійнішим джерелом інформації, але вони дозволяли отримати інформацію відносно швидко. Проте з розвитком соціальних мереж і обміну миттєвими повідомленнями з'явилися додаткові можливості для поширення російських наративів і фейків. Для деяких блогерів фінансовий аспект залишався пріоритетним у діяльності, що спонукало їх поширювати неперевірені повідомлення з нібито сенсаційними, необ'єктивними коментарями чи необ'єктивними висновками. Критерієм публікації частини інформації була перспектива залучення якомога більшої кількості користувачів. Водночас навіть в умовах повномасштабної війни деякі блогери виступали за «поглиблення дружніх відносин з Росією», не розуміючи, як «політики можуть посварити два братніх народи». Такі блогери засуджували рішення вищого керівництва організовувати опір ворогу, оскільки в результаті бойових дій неминуче гинуть люди.

Але, закликаючи до мирного «врегулювання конфлікту», вони загалом уникали розмов про територіальні претензії РФ до України, жахливі наслідки ворожих обстрілів та перспективи існування незалежної Української соборної держави. Так, 34% респондентів виступили проти запровадження таких норм, а 30% підтримали цю ідею. Ті, хто виступає проти запровадження державного регулювання, наголошують, що Інтернет має залишатися простором для вільного вираження думок і суджень, а ефективність державної політики щодо регулювання діяльності блогерів викликає сумніви. Переважна більшість прихильників регулювання блогів виступають за поширення регулювання на всіх блогерів без винятку[6].

Аналізуючи проблему забезпечення інформаційної безпеки громадян і держави під час воєнних дій і конфліктів, можна зробити висновок, що інформаційна безпека відіграє дуже важливу роль, особливо у воєнний час. Зрештою, дезінформація може викликати паніку серед населення, негативно вплинути на перебіг подій, прискорити внутрішню міграції

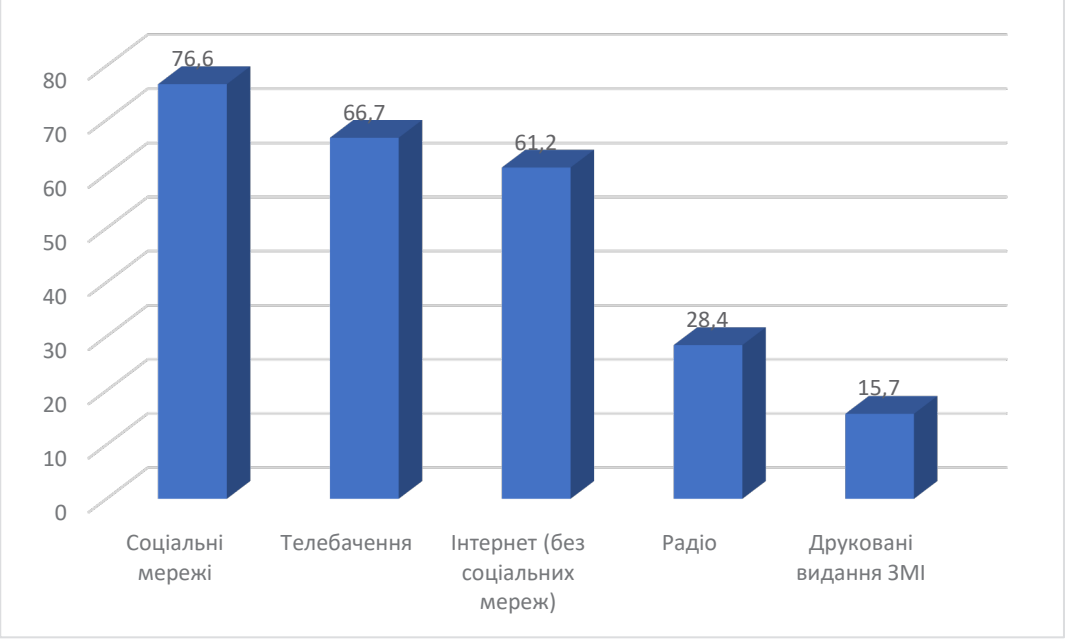


**Рис. 1. Результати опитування джерел отримання інформації українцями у 2023 році**

цію населення, що може негативно вплинути на боєздатність Збройних Сил України та фізичний і психічний стан громадян. Ефективно протистояти інформаційним атакам, на нашу думку, представляється можливим шляхом залучення до цього процесу міжнародних організацій, інституцій та міжнародної спільноти в цілому. Практика показує, що інформаційна війна не має кордонів. Настав час захистити публічний інформаційний простір нашої країни від ворожих впливів і навіювань.

З першого дня повномасштабного вторгнення Чернігівська область стала територією активних бойових дій. Частина області з лютого опинилася в окупації, а саме місто Чернігів - в повній блокаді. Ворог невпинно руйнував інфраструктуру, щоденно здійснював ракетно-бомбові обстріли житлових масивів, лікарень, дитячих садочків та шкіл. Значних втрат зазнали об'єкти телерадіоінформаційної структури (була знищена техніка, комунікації, студії).

Загальні принципи захисту персональних даних – це набір основних положень та правил, яких повинні дотримуватися під час обробки та зберігання персональних даних. Ці принципи стосуються всіх суб'єктів обробки персональних даних, таких як компанії, урядові органи тощо.

До основних принципів захисту персональних даних належать такі.

1. Законність, добросовісність і прозорість.
2. Мінімізація даних.
3. Точність.
4. Обмеження зберігання.
5. Інтегрітет даних і конфіденційність.
6. Відповідальність.

Війна стала важким випробуванням для мовників і провайдерів всієї України, Чернігівської області в тому числі. З перших дній повномасштабної війни чернігівським медійникам доводилося працювати в умовах активних бойових дій.

Реаліями для багатьох компаній постало: руйнування мереж і обладнання, робота в окупації та блокадному місті під постійними обстрілами, однак найважче – непоправна втрата колег. В день повномасштабного вторгнення всі телерадіокомпанії Чернігівської області інформували населення, виходили з оперативними повідомленнями та сповіщеннями, передавали звернення Президента та керівників громад, підключилися до трансляції всеукраїнського телемарафону «Єдині новини» для оперативного сповіщення населення регіону.

**Висновки.** У сучасному інформаційному суспільстві ворог не втрачає можливості використовувати фейкову або зманіпулювану інформацію на свою користь, сіяти страх і паніку в суспільстві, дестабілізувати політичну та соціально-економічну ситуацію в Україні. . Ворог намагається проникнути в український інформаційний простір та підірвати ідентичність українських громадян. Актуальність даної статті полягає в необхідності аналізу наявних механізмів протидії інформаційним операціям держави-агресора в контексті забезпечення національної безпеки. Варто відзначити низьку проблематичність в умовах, коли вся сукупність інформації розрахована на маніпулювання громадською думкою, свідомістю людини і подається за допомогою фізіологічних, психологічних методів і засобів сприйняття. У міру розвитку інформаційної культури та зниження критичних когнітивних здібностей людини аналіз та оцінка отриманої інформації стають важливими.

Цілком правильно вважати, що національна інформаційна безпека передбачає: належний рівень інформаційної культури, тобто теоретичну і практичну підготовку особистості, що забезпечує захист і реалізацію її життєво важливих інтересів і гармонійний розвиток в умовах інформаційного суспільства, незалежно від наявності інформаційних загроз; здатність держави створити умови для гармонійного розвитку та задоволення інформаційних потреб особи незалежно від наявності інформаційних загроз; забезпечення, розвиток і використання інформаційного середовища в інтересах особи; захист від різноманітних інформаційних загроз.

**ЛІТЕРАТУРА:**

1. Указ Президента України Про рішення Ради національної безпеки і оборони України "Про нову редакцію Воєнної доктрини України" від 2 вересня 2015 року №555/2015. URL: https://zakon.rada.gov.ua/laws/show/555/2015#Text

2. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Humanitarian vision*. 2016. Вип. 2 (1). С. 27–32.

3. Панченко О. А., Панченко Л. В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві: дис… докт. мед. наук: Київ, 2015. С. 32–38.

4. Дзямулич М. І, Вплив сучасних інформаційних систем і технологій на формування цифрової економіки. *Економічний форум: канд. економ. наук*: Луцьк, 2022. С. 2–9.

5. Кирильчук, Є.О., Проблеми національної інформаційної безпеки України в контексті сучасних національних державотворчих процесів та світової інтеграції. Наукові праці МАУП, 2018. 1(36), с. 60–63.

6. Дубов Д.В. Стратегічні комунікації: проблеми концептуалізації та практичної реалізації. Стратегічні пріоритети, 2016. № 4 (41). С. 9—23.

7. Деркач О. В. Пріоритетні напрями реалізації державної політики у сфері безпеки українсько-російського державного кордону. Інвестиції: практика та досвід. 2014. № 18. С. 141–144.