УДК 342.5.004.056
https://doi.org/10.32689/2617-2224-2022-5(33)-11

Тайєр Амро,
аспірант кафедри публічного адміністрування, Міжрегіональна Академія управління персоналом, 03039, м. Київ, вул. Фрометівська, 2, e-mail: kafedrapa@ukr.net, https://orcid.org/0009-0001-2029-7513

TaiierAmro,
PhD Student, Interregional Academy of Personnel Management, 03039, Kyiv, Frometivska str., 2, e-mail: kafedrapa@ukr.net, https://orcid.org/0009-0001-2029-7513

ВЗАЄМОЗВ'ЯЗОК СИСТЕМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ВОЄННОГО СТАНУ: МЕТОДИ ТА МОЖЛИВОСТІ

Анотація. У статті розглядається взаємозв'язок між системами забезпечення інформаційної безпеки та публічного управління в умовах воєнного стану. Мета публікації – аналіз взаємозв'язку між системами забезпечення інформаційної безпеки та публічного управління в умовах воєнного стану та визначення методів і можливостей для ефективного забезпечення інформаційної безпеки в цих умовах. Методологія. Складність й особливості досліджуваної теми зумовили використання сукупності методів емпіричного і теоретичного рівнів пізнання. Один з методів дослідження полягає у вивченні правових актів та документів, що регулюють функціонування цих систем. Наприклад, Закон України «Про інформацію» та ін. визначають правові засади забезпечення інформаційної безпеки, а також вимоги до збереження та розповсюдження державної інформації.

Наукова новизна. Стаття має наукову новизну, оскільки розглядається мало досліджена проблема. Автор аналізує поточний стан систем забезпечення інформаційної безпеки в умовах воєнного стану та пропонує нові методи та рішення для підвищення ефективності захисту інформації. Висновки. У публічному управлінні важливо мати системи, які допомагають ефективно координувати дії та ресурси щодо розповсюдження інформації. Наприклад, системи електронного управління можуть допомогти в управлінні кризовими ситуаціями та швидкому прийнятті рішень у воєнних умовах. Отже, взаємозв'язок між системами забезпечення інформаційної безпеки та публічного управління є вагомим у воєнних умовах. Розвиток технологій та систем координації може допомогти забезпечити ефективне управління кризовими ситуаціями та захистити інформаційні системи від кібератак.

Ключові слова: інформаційна безпека, публічне управління, воєнний стан, захист інформації, війна, методи захисту інформації, державні органи.

THE CONNECTION OF THE SYSTEM FOR ENSURING INFORMATION SECURITY AND PUBLIC ADMINISTRATION UNDER THE CONDITIONS OF WAR-TIME: METHODS AND POSSIBILITIES

Abstract. The article examines the relationship between information security and public administration systems under martial law. The purpose of the publication is to analyze the relationship between information security and public administration systems in the conditions of martial law and to determine the methods of effective provision of information security in these conditions. Methodology. The complexity and peculiarities of the researched topic led to the use of a set of methods of empirical and theoretical levels of knowledge. One of the methods of research arises in the study of legal acts and documents regulating the functioning of these systems. For example, the Law of Ukraine "On Information" and others. notification of the legal basis for ensuring information security, as well as requirements for the preservation and distribution of state information. Scientific news. The article has a scientific novelty, an understudied problem is considered. The author analyzes the current state

of the information security system under martial law and offers new methods and solutions to increase the effectiveness of information protection.

Conclusions. In public administration, it is important to have systems in place to help effectively coordinate information dissemination activities and resources. For example, electronic control systems can help in managing crisis situations and make quick decisions in wartime conditions. Therefore, the relationship between information security and public administration systems is important in military conditions. The development of technologies and coordination systems can help ensure effective management of crisis situations and protect information systems from cyber attacks.

Key words: information security, public administration, martial law, information protection, war, methods of information protection, state bodies.

---

1. Вступ. Під час повномасштабного вторгнення російської армії і початок війни, спонукало українську владу вжити заходи щодо інформаційної безпеки країни. Медійна війна активно ведеться ворогом проти нас, останнім часом вона стосується намаганням росії «очорнити» Україну перед світовою спільнотою.

Актуальність теми визначається тим, що в сучасному світі інформаційна безпека є важливою складовою національної безпеки будь-якої держави. У разі виникнення воєнного конфлікту, інформаційна безпека та ефективне публічне управління стають критично важливими для забезпечення успішного ведення бойових дій та мінімізації можливих наслідків. Також для вирішення проблем евакуації. Управління кризовими ситуаціями та забезпечення інформаційної безпеки є ключовими завданнями, які стоять перед керівництвом держави під час воєнного стану.

Узагальнюючи, можна сказати, що використання комунікативних технологій для поширення інформації з використанням безпекових чинників, допомагає урядовим інституціям ефективно реагувати на надзвичайні ситуації та забезпечувати ефективне публічне управління в цілому.

2. Дослідження сутності категорії поняття «інформаційна безпека». Інформаційна безпека – це стан, в якому захищена інформація від несанкціонованого доступу, втручання, руйнування, викрадення, втрати або пошкодження. Інформаційна безпека є важливим аспектом національної безпеки країни, оскільки інформація є критично важливим ресурсом для функціонування різних сфер життя, включаючи освіту, економіку, політику, науку, технології, оборону та безпеку.

Основні аспекти інформаційної безпеки включають захист конфіденційної інформації, забезпечення цілісності даних, доступність інформації та захист від кібератак. Забезпечення інформаційної безпеки передбачає впровадження комплексу технічних, організаційних та правових заходів, що дозволяють забезпечити захист інформації від можливих загроз.

Інформаційна безпека є надзвичайно важливою у сучасному світі, оскільки залежність від інформаційних технологій та електронного обміну даними стає все більшою. Це створює потребу в постійному удосконаленні заходів інформаційної безпеки для забезпечення ефективного захисту інформації та попередження можливих загроз.

Дослідженням поняття інформаційної безпеки присвячені багато праць у вітчизняній та зарубіжній літературі. Деякі автори визначають інформаційну безпеку як систему заходів, спрямованих на забезпечення надійності та захисту інформаційних технологій та даних від загроз.

Інші дослідники відзначають, що інформаційна безпека повинна бути розглянута в контексті соціальної та політичної ситуації, а також враховувати чинники економіки та культури.

Автор Захаренко К. дослідив значення інформаційної безпеки як важливого показника захищеності громадян, суспільства й держави, ним з'ясовано, що інформаційну безпеку варто розглядати в контексті запобігання тим шкідливим наслідкам, які можуть принести різні інформаційні загрози, а також пошук методів подолання цих наслідків із якомога меншою шкодою для народу (Захаренко, 2018).

Відзначимо, що дослідник Шемчук В. обґрунтовує поняття «інформаційна оборона», яке становить систему заходів захисту, інформаційної та віртуальної сфери, це в свою чергу убезпечує готовність до інформаційного впливу, зокрема, під час гібридної війни, прямого нападу інших держав, захист і розвиток власного інформаційного простору (Шемчук, 2019).

Відзначимо, що авторами в наукових працях аналізуються переважно питання інформаційної політики, гібридних загроз, інформаційних війн, інформаційної безпеки в Україні, натомість проблеми співвідношення категорій системи забезпечення інформаційної безпеки та публічного

управління в умовах воєнного стану вивчалися вкрай рідко.

Базовим документом політики нашої держави у сфері інформаційної безпеки є Стратегія інформаційної безпеки України. У ньому визначено сім основних стратегічних цілей у сфері інформаційної безпеки держави, можливість реалізації яких в умовах воєнного стану є вкрай необхідним завданням (Указ, 2021).

3. Публічне управління в забезпеченні інформаційної безпеки в умовах війни. Публічне управління має важливу роль у забезпеченні інформаційної безпеки в умовах воєнного стану. У таких умовах державні органи та інші зацікавлені сторони повинні працювати в єдиному інформаційному просторі та діяти в координації один з одним та дотримуватися Закону України «Про інформацію», у якому чітко зазначено, шо державна інформаційна політика – це сукупність основних напрямів і способів діяльності держави з одержання, використання, поширення та зберігання інформації (Закон, 1992).

Згідно з вітчизняними фахівцями, інформаційна політика держави має чотири основні напрями: розвиток національного інформаційного простору, розвиток інформаційного суспільства, розвиток офіційної комунікації та забезпечення інформаційної безпеки держави. Важливою складовою кожного з цих напрямів є державна політика інформаційної безпеки, адже вона забезпечує захист інформаційного суверенітету та інформаційних прав та свобод громадян. Крім того, державна політика інформаційної безпеки є важливим аспектом національної безпеки України (Мужанова, 2019, с. 80).

Публічне управління здійснює контроль за виконанням законодавства, яке стосується інформаційної безпеки, та забезпечує дотримання прав та свобод громадян. Крім того, публічні органи управління мають розробляти та впроваджувати стратегії та програми щодо захисту критично важливої інформації в умовах війни. Оскільки ворог намагатиметься заволодіти важливою інформацією.

Під час війни публічне управління відіграє важливу роль у моніторингу інформаційних потоків, а також в поширенні точної та достовірної інформації про ситуацію на фронті та в країні в цілому. Особливо небезпечними для безпеки держави і громадян є розміщення в публічному просторі інформації про критичну інфраструктуру, військові об'єкти, пересування військ тощо. Тому органи публічної влади мають звести до мінімуму поширення зазначеної інформації. Як зазначає А. Клочко, що «першочерговими завданнями захисту інформації в автоматизованій системі в процесі електронної взаємодії є запобігання, поширення, модифікація, знищення, копіювання, блокування та неправомірне тиражування інформації обмеженого доступу» (Клочко, 2022). Органам влади необхідно слідкувати за дотриманням статті 6. Публічна інформація з обмеженим доступом ЗУ Про доступ до публічної інформації. Так, **і**нформацією з обмеженим доступом є:

конфіденційна інформація; таємна інформація; службова інформація.

Зауважимо й те, що обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог: «1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя» (Закон, 2011, ст. 6).

Також публічні органи управління мають забезпечувати ефективну комунікацію між зацікавленими сторонами, щоб уникнути спотворення та недостовірної інформації.

Окрім того, публічне управління в умовах війни повинне забезпечити захист інформації від хакерських атак та кібернападів, а також запобігати поширенню фейків та дезінформації.

Отже, роль публічного управління у забезпеченні інформаційної безпеки в умовах війни полягає у забезпеченні контролю за дотриманням законодавства, розробці та впровадженні стратегій та програм захисту інформації.

5. Методи та можливості забезпечення інформаційної безпеки в умовах війни. Умови воєнного стану ставлять перед державою особливі виклики з питань забезпечення інформаційної безпеки та публічного управління. Воєнна загроза вимагає від держави швидкої та ефективної реакції, що передбачає наявність готових та досконало спланованих механізмів забезпечення інформаційної безпеки. У цьому контексті система забезпечення інформаційної безпеки та публічного управління в умовах воєнного стану має бути досконалою та добре підготовленою.

В умовах війни забезпечення інформаційної безпеки є надзвичайно важливою задачею, оскільки інформаційні атаки можуть нанести значну шкоду військовій стратегії та безпеці нації в цілому. Деякі методи та можливості забезпечення

інформаційної безпеки в умовах війни включають забезпечення кібербезпеки: це охорона комп'ютерних систем від несанкціонованого доступу, вірусів та інших шкідливих програм. Для забезпечення кібербезпеки в умовах війни можуть використовуватися різноманітні технічні та програмні засоби, такі як брандмауери, антивіруси, мережеві інструменти моніторингу та інші.

Забезпечення захисту інформації: це заходи для захисту конфіденційної інформації від несанкціонованого доступу. Забезпечення захисту інформації може включати шифрування, автентифікацію та інші методи.

Сприяння інформаційній війні: це використання інформації як зброї для ведення війни. В умовах війни інформаційна війна може включати розповсюдження дезінформації та пропаганди, використання соціальних мереж для впливу на громадську думку та інші методи.

Забезпечення фізичної безпеки інформації: це заходи для захисту комп'ютерної техніки та інших засобів зберігання інформації від фізичної руйнівної дії, такої як вандалізм або крадіжка.

У механізмі правового забезпечення діяльності публічних адміністрацій важливе місце займає громадський контроль. За умов дії правового режиму воєнного стану деякі нормотворчі процедури відбуваються у спрощеному порядку, а громадянська активність має певні обмеження. Отже, звичні для української політико-правової реальності інструменти коригування невдалих з точки зору громадськості правових новел (мітинги, блокування органів публічної влади тощо) нині не використовуються. Змінилися форми впливу на ефективність вказаного процесу: перевагу отримали експертні обговорення та публікації у засобах масової інформації (Жукова, 2022, с. 152).

Публічний службовець не має права обмежити доступ до інформації, не пояснивши, чому її оприлюднення завдасть більше шкоди, ніж принесе користі. Відповідно до Закону України «Про доступ до публічної інформації», гарантується кожному громадянину доступ до публічної інформації. Запровадження обмеження доступу до конкретної інформації за результатами розгляду запиту на інформацію допускається лише за умови застосування вимог пунктів 1-3 частини другої статті 6 Закону (Закон, 2011). Ці вимоги є «трискладовим тестом», який повинна пройти публічна інформація для визначення її відкритою чи обмеженою. Доступ до інформації може бути обмежено за умови додержання сукупності всіх трьох підстав (Гвоздік, 2022, с. 26).

Конфіденційною є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана такою на підставі закону (Закон, 1992).

В умовах воєнного стану, система забезпечення інформаційної безпеки та публічного управління стає важливим механізмом управління державою та забезпечення захисту інтересів громадян. В цьому контексті розглядається питання забезпечення безпеки інформаційного простору, управління інформацією, зокрема забезпечення конфіденційності та цілісності інформації, а також забезпечення взаємодії між різними державними структурами, військовими підрозділами та громадськістю.

Одним з найважливіших методів забезпечення інформаційної безпеки в умовах воєнного стану є розробка та впровадження спеціальних заходів технічного захисту інформації, які дозволяють забезпечувати конфіденційність і цілісність даних. До таких заходів відносяться розробка та впровадження захисту від несанкціонованого доступу до інформації, шифрування даних, створення резервних копій, контроль доступу до інформації та інші. Крім того, важливим методом є розробка та впровадження спеціальних заходів забезпечення кібербезпеки, які дозволяють захищати інформаційний простір від хакерських атак та інших загроз.

Ще одним важливим методом забезпечення інформаційної безпеки та публічного управління в умовах воєнного стану є забезпечення ефективної комунікації між державними структурами та військовими підрозділами.

Один з методів забезпечення інформаційної безпеки в умовах воєнного стану – це використання системи раннього попередження про надходження інформаційної загрози. Ця система дозволяє оперативно виявляти, аналізувати та реагувати на інформаційні загрози. Крім того, важливим методом є розвиток кібербезпеки, що включає в себе заходи з попередження кібератак та забезпечення захисту від таких атак.

Одним з можливих методів забезпечення публічного управління в умовах воєнного стану є використання інформаційних технологій та електронного управління. Це дозволяє забезпечувати оперативний обмін інформацією між різними державними органами, а також між цими органами та населенням. Крім того, важливим методом є впровадження систем електронного голосування, що дозволяє забезпечити швидке та безпечне голосування в умовах війни.

Ще одним важливим методом забезпечення публічного управління є розвиток системи публічної інформації та масової комунікації.

Для цього необхідно розвивати та підтримувати роботу ЗМІ та соцмереж.

Один із методів забезпечення інформаційної безпеки в умовах воєнного стану – це створення ефективної системи моніторингу та аналізу інформації. Для цього потрібні спеціалізовані центри, які мають відповідні комп'ютерні програми для автоматизації збору та обробки інформації. Ці центри, як своєрідні «Мозкові центри» мають бути здатні оперативно реагувати на будь-які зміни у ситуації та забезпечувати необхідну інформацію для прийняття рішень.

Дієвим методом є підвищення медіакультури населення, саме державними органами проводиться низка заходів, які стосуються інформаційної гігієни. Так, Залєвська, вказує те, щоб ворожа брехня не мала негативного впливу на населення, необхідно, за можливості, викривати всі фейки, що запускаються в український інформаційний простір (Залєвська, 2022. с. 22)

Ще одним методом є забезпечення кібербезпеки. В умовах війни кібератаки можуть спричинити серйозні наслідки для держави, тому необхідно забезпечувати захист критичних об'єктів, систем керування та комунікаційних мереж. Необхідно розробити відповідні стратегії та програми для запобігання та протидії кібератакам. Основним механізмом воєнно-інформаційної безпеки в умовах війни є розвідка і контррозвідка. Розвідка займається збором інформації про ворога, його зброю, техніку, тактику та плани. Контррозвідка ж займається захистом власної інформації та виявленням та припиненням шпигунської діяльності.

6. Висновки з дослідження і перспективи подальших розвідок у цьому напрямі. Отже, ефективна інформаційна діяльність може суттєво впливати на національну безпеку України. Взаємозв'язок між системами забезпечення інформаційної безпеки та публічного управління є вагомим у воєнних умовах. Розвиток технологій та систем координації може допомогти забезпечити ефективне управління кризовими ситуаціями та захистити інформаційні системи від кібератак. свідчить досвід локальних воєн останніх років. Забезпечення військової безпеки в XXI ст. буде залежати від інформаційних чинників. Так, відомий американський футуролог О. Тоффлер у книзі «Війна та антивійна» зазначає, що інформація стає найважливішим військово-стратегічним ресурсом щонайменше або навіть важливішим, аніж традиційні види озброєнь і військової техніки (Залєвська, 2022).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Гвоздік О. та ін. Дослідження «Вплив воєнного стану на громадську участь в Україні». 2022.
2. Закон України Про інформацію. 1992. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
3. Закон України Про доступ до публічної інформації. 2011. URL: https://minjust.gov.ua/m/str_35409
4. Залєвська І., Удренас Г. Інформаційна безпека україни в умовах російської військової агресії. 2022. URL: http://surl.li/gncmq
5. Захаренко К. Теоретичні засади дослідження інформаційної безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії*. № 2(4). 2018. URL: http://relint.vnu.edu.ua/index.php/relint/article/view/77
6. Жукова Євгенія Напрями вдосконалення правового забезпечення публічного адміністрування за умов воєнного стану. *Забезпечення публічної безпеки і порядку в умовах воєнного стану* : матеріали Всеукраїнської науково-практичної конференції (м. Кропивницький, 1 липня 2022 року). Донецький державний університет внутрішніх справ. Кропивницький, 2022. С. 151–153.
7. Клочко А. Забезпечення інформаційної безпеки в умовах сучасного суспільства. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2022. 3(63). С. 38–42. https://doi.org/10.32689/2523-4625-2022-3(63)-6
8. Мужанова Т. Інформаційна безпека держави. Київ, 2019. URL: http://surl.li/gnaoh
9. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7
10. Шемчук В. Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктрини й законодавчої основи. *Вчені записки ТНУ імені В. І. Вернадського. Серія : Юридичні науки*. Том 30(69). № 4. 2019.
11. Semenets-Orlova, I., Halytska, N., Klochko, A., Skakalska, I., & Kosyuk, N. (2019). Information Exchange and Communication Infrastructure in the Public Sector. In *CMiGIN* (pp. 519–529).
12. Semenets-Orlova, I. A., & Kyselova, Y. Y. (2018). Multidimensional management contemporary: generation of social meanings for a new collective identities. *Публічне урядування*, (4), 264–273.

REFERENCES:

1. Hvozdik O. ta in. Doslidzhennia «Vplyv voiennoho stanu na hromadsku uchast v Ukraini». 2022. [in Ukrainian].
2. Zakon Ukrainy Pro informatsiiu. 1992. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text [in Ukrainian].
3. Zakon Ukrainy Pro dostup do publichnoi informatsii. 2011. URL: https://minjust.gov.ua/m/str_35409 [in Ukrainian].

4. Zalievska I., Udrenas H. Informatsiina bezpeka ukrainy v umovakh rosiiskoi viiskovoi ahresii. 2022. URL: http://surl.li/gncmq [in Ukrainian].
5. Zakharenko K. Teoretychni zasady doslidzhennia informatsiinoi bezpeky. *Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii*. № 2(4). 2018. URL: http://relint.vnu.edu.ua/index.php/relint/article/view/77 [in Ukrainian].
6. Zhukova Yevheniia Napriamy vdoskonalennia pravovoho zabezpechennia publichnoho administruvannia za umov voiennoho stanu. *Zabezpechennia publichnoi bezpeky i poriadku v umovakh voiennoho stanu* : materialy Vseukrainskoi naukovo-praktychnoi konferentsii (m. Kropyvnytskyi, 1 lypnia 2022 roku). Donetskyi derzhavnyi universytet vnutrishnikh sprav. Kropyvnytskyi, 2022. S. 151–153. [in Ukrainian].
7. Klochko A. Zabezpechennia informatsiinoi bezpeky v umovakh suchasnoho suspilstva. *Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia*. 2022. 3(63). S. 38–42. https://doi.org/10.32689/2523-4625-2022-3(63)-6 [in Ukrainian].
8. Muzhanova T. Informatsiina bezpeka derzhavy. Kyiv, 2019. URL: http://surl.li/gnaoh[in Ukrainian].
9. Ukaz Prezydenta Ukrainy «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsiinoi bezpeky». URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7 [in Ukrainian].
10. Shemchuk V. Informatsiina bezpeka ta informatsiina oborona v konteksti rozvytku vitchyznianoi doktryny y zakonodavchoi osnovy. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia : Yurydychni nauky.* 2019. Tom 30(69). № 4 [in Ukrainian].
11. Semenets-Orlova, I., Halytska, N., Klochko, A., Skakalska, I., & Kosyuk, N. (2019). Information Exchange and Communication Infrastructure in the Public Sector. In CMiGIN (pp. 519–529).
12. Semenets-Orlova, I. A., & Kyselova, Y. Y. (2018). Multidimensional management contemporary: generation of social meanings for a new collective identities. *Публічне урядування*, (4), 264–273.