УДК 349.3:332.1:331.101
DOI https://doi.org/10.32782/TNU-2663-6468/2025.1/08

Горник В.Г.
Таврійський національний університет імені В.І. Вернадського

Євмєшкіна О.Л.
Таврійський національний університет імені В.І. Вернадського

Сімак С.В.
Таврійський національний університет імені В.І. Вернадського

ІННОВАЦІЙНІ ПІДХОДИ ДО ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ В КРАЇНАХ ЄС І КРАЇНАХ-КАНДИДАТАХ ІЗ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ

Стаття присвячена розкриттю інноваційних підходів до цифрової трансформації публічного управління в країнах ЄС і країнах-кандидатах із забезпечення інформаційної та енергетичної безпеки. З'ясовано, що найважливіше поточне завдання, вирішення якого потребує сфера, яка забезпечує державну енергетичну безпеку, полягає в тому, аби на практиці ефективно реалізувати раніше визначені стратегічні цілі й інструменти, за допомогою яких вони будуть впроваджені. Щоб цього досягти, всі гілки влади мають діяти спільно і злагоджено, потрібно встановити відповідальність і належний контроль. У нинішніх реаліях необхідність забезпечити енергетичну безпеку стала дійсно глобальною проблемою, водночас прийнятна та визнана всіма сторонами стратегія, завдяки якій можна було б забезпечити світову чи загальноєвропейську енергетичну безпеку, відсутня. Відсутня єдина енергетична політика Євросоюзу – це певна загроза для процесу, в ході якого має бути забезпечена енергетична безпека і самим країнам-учасницям співдружності, і країнам-сусідам (зокрема й Україні). Суть національних стратегічних намірів великою мірою полягають у тому, щоб реалізувати вигідний геополітичний стан держави, яка є потужним транзитером ПЕР. Відсутня єдина думка про конкретні проекти й механізми, за допомогою яких вони будуть реалізовані, дуже негативно позначається на розвитку сфери енергетики та можливості реалізувати Енергетичну стратегію держави.

Встановлено: проаналізувавши досвід, отриманий провідними світовими державами, можна дійти висновку, що в українських умовах особливу увагу в галузі забезпечення інформаційної та енергетичної безпеки варто зосередити на тому, щоб: узгодити нормативно-правові акти з вимогами нинішніх реалій (наявність кібератак, масових заворушень, воєнних дій, епідемій); запровадити національну систему стійкості; створити головний орган, зоною відповідальності якого буде забезпечення інформаційної та енергетичної безпеки на рівні держави; налагодити партнерську співпрацю між державою, органами місцевого самоврядування, громадськими організаціями, приватними бізнес-структурами та міжнародними партнерами в питаннях забезпечення інформаційної та енергетичної безпеки; проводити міжвідомчі навчання й тренування, в яких братиме участь населення, щоб підвищити обізнаність і готовність реагувати на появу загроз інформаційній та енергетичній безпеці.

Ключові слова: *публічне управління, державна політика, національна безпека, енергетична безпека, інформаційна безпека.*

Постановка проблеми. В цілому національні економіки та світове співтовариство відчувають загострення істотних загроз, які обумовлені наявністю невирішених проблем в енергетичній безпеці. Насамперед вони проявляються в тому, що зростає міжнародний тероризм, в окремих країнах політичні режими перебувають у нестабільному стані, зазнає глобальних змін клімат, неминуче виснажується ресурсна база, якою володіє вуглеводна сировина. Енергетичними кризами, що відбулися в 70-х, було продемонстровано наслідки того, що були скорочені міжрегіональні постачання енергоносіїв. Суть головної проблеми наступна: у своїй більшості найбільш розвинені держави й регіони, які споживають енергоресурси, не мають достатніх сировинних енергетичних

запасів. В контексті того, що енергетичні ресурси користуються все більшим попитом, ситуація, коли одні регіони залежать від того, як інші постачають енергоносії, набуває дедалі загрозливіших обрисів. Сполучені Штати Америки, приміром, зараз володіють часткою нетто-імпорту первинної енергії сумарно та споживання в межах майже 26 відсотків. В цій країні понад половину нафти, яка споживається, складає імпорт. Японія в межах 90 відсотків перебуває в залежності від імпортних первинних енергоресурсів. Досить напружений стан справ із залежністю від імпортної енергетики і в держав ЄС. Приміром, російський природний газ забезпечує майже 25 відсотків сумарного користування газом у Євросоюзі. У теперішніх умовах і в найближчому майбутньому міжнародна торгівля енергоресурсами характеризуватиметься тим, що взаємозалежність між постачальниками, країнами-транзитерами і країнами, які споживають енергоресурси, зростатиме і зазнаватиме ускладнень. Відбувається зміна всієї ринкової структури – центрів, де здійснюється видобуток, центрів споживання та основних шляхів, якими доставляються енергоносії, відтак, необхідність забезпечити енергобезпеку набуває особливої актуальності.

Нині більшість світових країн реалізують концепцію, посередництвом якої можна захистити критичну інформаційну інфраструктуру й у котрій має акцентуватися на поточних проблемах, повинні міститися способи того, як їх вирішити, вона мусить бути у відповідності з сучасними глобальними викликами, надто коли йдеться про безпеку, стійкість, надійність, функціональність, цілісність. Тож потреба захистити критичну інфраструктуру від великої кількості небезпек, які несуть кіберзагрози та інформаційні ризики, є пріоритетною в глобальному масштабі та відіграє ключову роль, коли необхідно підтримати адекватну роботу, здійснювану системами життєдіяльності, забезпечити сталий процес, під час якого розвиваються суспільства й національні економіки.

Аналіз останніх досліджень і публікацій. Завдяки тому, що ця тема актуальна, науковці не обходять її увагою, зокрема цікаві дослідження провели О. Батюк, С. Братель, О. Герасименко, І. Гора, К. Ковальов, А. Помаза-Пономаренко, Д. Тарадуда та інші. На нинішньому етапі розвитку європейський енергетичний ринок супроводжують численні невирішені проблеми. Найголовніша проблема, яка давно завдає хвилювань світовій спільноті та нерідко є вирішальною у міжнародних взаєминах, полягає в тому, наскільки енергетичний ринок насичений ресурсним потенціалом, щоб постійно забезпечувати людство й усю національну економіку енергоносіями. Попри те, що енергетична безпека є питанням актуальним, між теоретиками і практиками нині відсутня єдність щодо того, як тлумачити її суть та управлінську методику. Приділяється недостатньо уваги тому, щоб реалізувати енергозберігаючі технології та забезпечити обладнанням різні підприємства, стимулювати економне поводження з енергоресурсами й запобігати їхнім втратам; користуватися прогресивними показниками нормування питомих витрат паливно-енергетичних ресурсів. В нинішній час бракує чітких та ґрунтовних методик, щоб оцінити енергетичну безпеку. Відбулося загострення проблеми, пов'язаної з державною енергетичною безпекою, і в Україні. Беручи до уваги, на якому рівні перебуває сучасний технологічний розвиток, і те, що наша країна на 60 відсотків залежна від зовнішніх енергетичних джерел, ключовий чинник, який забезпечить системну вітчизняну конкурентоздатність, полягає в умінні ефективно користуватися, насамперед, власними паливно-енергетичними ресурсами.

Постановка завдання. Метою статті є розкриття інноваційних підходів до цифрової трансформації публічного управління в країнах ЄС і країнах-кандидатах із забезпечення інформаційної та енергетичної безпеки.

Виклад основного матеріалу. В нинішніх реаліях наявність постійного процесу, під час якого впроваджуються новітні технології, свідчить про високу розвиненість держави, він відіграє роль визначального фактора конкурентоздатності її економіки, а відтак – і обов'язкової умови, виконавши яку, можна досягти мети, що їх визначають національні інтереси. Разом з тим, крім багатьох переваг, технологічним прогресом формується безпрецедентна залежність як окремих людей, так і соціуму загалом, від інформаційних, комунікаційних, транспортних, енергетичних, фінансових та інших систем.

Державою-агресором ведеться дуже активна гібридна боротьба, і найбільш ефективний її вияв стався, коли рф розпочала неоголошену війну в Україні. Незаконно анексувавши Крим 2014 року, росією продовжується й нині ведення гібридної війни з нашою країною та іншими державами, аби отримати бажані політичні результати, приміром, підірвати прозахідні уряди, розколоти й ослабити вплив Альянсу чи просувати свої власні економічні інтереси. Відтак через

існування проблем, створених гібридною війною енергетичному сектору, ймовірно може порушитися політична, соціальна, військова ефективність та злагоджена робота НАТО. Щоб подолати ці загрози, потрібно багато часу і зусиль, аби Альянсу вдалося розв'язати проблеми, пов'язані з залежністю країн-учасниць, та виступити платформою, на якій буде сформовано загальну картину з представленими комплексним оперативним ризиком та чинниками вразливості.

Енергетичний сектор є однією ж важливих цілей функціонування будь-якої держави та міжнародних об'єднань. Вони змушені швидко адаптуватися до умов зростаючої гібридної війни. Власне кажучи, протягом останніх десяти років гібридні загрози різко зросли у всьому світі: від кібератак до дезінформаційних кампаній та потайних військових операцій. Загрози виникають усе частіше, набуваючи більш комплексного, руйнівного та силового характеру. Наслідки гібридної боротьби важливі як для економіки, так і для державної політики, особливо стосовно енергетичного сектору. Держава-агресор створила низку гібридних загроз проти енергетичних об'єктів, зокрема й критичної інфраструктури загалом в Україні, а також проти політики держав-членів НАТО, інших країн світу [1].

Серед міжнародних організацій, основною метою яких є саме безпека, НАТО найбільш ефективно модернізувала політику щодо інформаційної безпеки. Організація заснувала центри у країнах-членах як багатонаціональні інститути для розробки доктрини кібербезпеки, вдосконалення міждержавної взаємодії, впровадження теоретичних напрацювань у практиці протидії кіберзагрозам, обміну досвідом кіберзахисту представників країн-членів і країн-партнерів. Наразі Центр кібербезпеки НАТО функціонує в Естонії, він не є підрозділом військового командування або структури збройних сил НАТО, а персонал та фінансування забезпечуються державами-спонсорами та державами-учасниками [2].

Керівники країн НАТО наголошують на важливості енергетичної безпеки, на їх погляд, стабільне та надійне енергопостачання, диверсифікація шляхів імпорту, постачальників та енергоресурсів, а також взаємопов'язаність енергомереж мають ключове значення та підвищують стійкість перед політичним й економічним тиском. Хоча за ці питання відповідає, насамперед, державна влада, події в енергетичній сфері можуть мати значні політичні наслідки та наслідки для безпеки країн НАТО, а також торкнутися партнерів Альянсу [3].

На сьогодні кібербезпека є стратегічною проблемою державного значення, яка зачіпає всі верстви населення. Державна політика з кібербезпеки служить засобом посилення національної безпеки і надійності інформаційних систем держави. Стратегії з кібербезпеки були прийняті такими державами як США, Швеція, Естонія, Фінляндія, Чехія, Франція, Німеччина, Литва, Великобританія, Канада, Японія, Індія, Австралія, Нова Зеландія, Колумбія тощо. Список країн наочно показує, що проблема кібербезпеки визнається актуальною в усьому світі [4].

Активну політику щодо забезпечення інформаційної безпеки проводить і Європейський Союз. Гарантування міжнародної інформаційної безпеки та її складової – кібербезпеки стало одним із пріоритетних напрямів діяльності ЄС. У 2001 р. Європейською Комісією було представлено перший документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід», в якому була представлена концепція вирішення проблеми інформаційної безпеки. У документі використовується термін «мережева та інформаційна безпека», який трактується як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі і системи [5].

Становлення нормативно-правової бази у сфері забезпечення інформаційної та енергетичної безпеки є тривалим процесом. Найбільших успіхів вважається у цій сфері досягли Сполучені Штати Америки. У 2002 р. в США прийнятий Акт щодо інформації з критичної інфраструктури (Critical Infrastructure Information Act («США»), яким регулювався обмін інформацією з питань оцінки вразливості та загроз інфраструктурі, також і пов'язаних із терористичними загрозами. Закон запровадив термін «інформація щодо критичної інфраструктури» і розуміння інформації, яка зазвичай не перебуває під увагою суспільства та належить до безпеки функціонування критичної інфраструктури чи захищених систем. Цим Актом визначений урядовий орган – Департамент внутрішньої безпеки, який мав відповідати за збір, аналіз і поширення інформації з метою вжиття необхідних заходів для захисту критичної інфраструктури. Одночасно законом установлювалися вимоги до використання такої інформації (запроваджується режим обмеженого доступу) для недопущення зловживань і захисту суб'єктів

господарювання (операторів інфраструктури) від поширення вразливої комерційної інформації. Відтоді США посіли лідерські позиції у цій сфері, зокрема завдяки застосуванню апробованих на інших напрямах сучасних управлінських підходів, удосконаленню інформаційно-аналітичної підтримки процесу прийняття рішень, використанню новітніх технологій та активному поширенню різноманітних форм і форматів підготовки кадрів і населення для забезпечення захисту та стійкості критичної інфраструктури. Одним із прикладів цього є створення в 2018 р. у системі Міністерства внутрішньої безпеки США Агентства з питань кібербезпеки та безпеки інфраструктури, що функціонує як оперативна складова, яка на національному рівні керує зусиллями, спрямованими на усвідомлення та управління ризиками, сформованими загрозами критичній інфраструктурі країни [6].

Провідні світові країни скористалися досвідом Сполучених Штатів Америки, коли створювали власні системи забезпечення інформаційної та енергетичної безпеки. Його застосовують і в теперішніх умовах, в яких розвивається аналізована галузь суспільних взаємин. Використовує досвід США в царині, де функціонують системи забезпечення інформаційної та енергетичної безпеки, й наша країна.

Під час дослідження зарубіжного досвіду забезпечення інформаційної та енергетичної безпеки увагу слід звернути і на досвід Німеччини. Нормативно-правовими актами, які забезпечують інформаційну та енергетичну безпеку в Німеччині є: Національна стратегія захисту критичної інфраструктури (2009 р.), Стратегія кібербезпеки Німеччини (2016 р.), Закон «Про безпеку інформаційних технологій (2015 р.), UP KRITIS: державно-приватне партнерство із захисту критичних інфраструктур, BSI (2014 р.), Спільна інтернет-платформа BSI та BBK щодо захисту критичної інфраструктури, плани захисту критичної інфраструктури. Основну участь у забезпеченні інформаційної та енергетичної безпеки покладено на такі установи: Федеральне відомство з інформаційної безпеки, Федеральне відомство з охорони Конституції, Федеральне управління цивільного захисту та ліквідації наслідків стихійних лих, Федеральна кримінальна поліція, Федеральне агентство технічного сприяння [7].

У Франції загрози забезпеченню інформаційної та енергетичної безпеки зосереджені на кіберзагрозах та терористичних загрозах. З метою протидії кіберзлочинності та тероризму діє Генеральний секретаріат із питань оборони та національної безпеки (SGDSN), який аналізує відкриту інформацію та розвіддані у сфері захисту критичної інфраструктури, стежить за недопущенням різних загроз – як внутрішніх, так і зовнішніх. У Нідерландах основні загрози для інформаційної та енергетичної безпеки визначаються через національну оцінку ризиків і включають тероризм, кіберзагрози, забезпечення національної безпеки та кризове управління. Національний координаційний центр із питань боротьби з тероризмом та забезпечення безпеки (NCTV) відповідає за координацію діяльності поліції, судової влади, служб безпеки та інших організацій у сфері боротьби з тероризмом. Румунія поділяє загрози для інформаційної та енергетичної безпеки на такі, що можуть мати природний, випадковий або умисний характер. Природні загрози охоплюють стихійні лиха, випадкові загрози включають техногенні аварії, а умисні загрози включають терористичні акти та злочинні дії [8].

Проаналізований досвід, отриманий провідними світовими країнами, доводить, що в галузі забезпечення інформаційної та енергетичної безпеки Україна має особливо зосередитися на тому, щоб:

– нормативно-правові акти, в яких відбувається регулювання суспільних відносин у галузі забезпечення інформаційної та енергетичної безпеки, відповідали вимогам нинішніх реалій (наявність кібератак, масових заворушень, воєнних дій, епідемій);

– запровадити національну систему стійкості;

– створити головний орган, зоною відповідальності якого буде забезпечення інформаційної та енергетичної безпеки на рівні держави;

– налагодити партнерську співпрацю між державою, органами місцевого самоврядування, громадськими організаціями, приватними бізнес-структурами та міжнародними партнерами в питаннях забезпечення інформаційної та енергетичної безпеки;

– проводити міжвідомчі навчання й тренування, в яких братиме участь населення, щоб підвищити обізнаність і готовність реагувати на появу загроз інформаційній та енергетичній безпеці.

Висновки. Отже, враховуючи характерні властивості, притаманні елементам, що входять у національну безпеку, можна стверджувати, що надзвичайно важливо реалізувати заходи, націлені на те, щоб підтримувати в належному стані енергетичну й соціальну безпеку, контекстом функціонування якої є гібридна війна. Під її негатив-

ний вплив потрапили всі світові країни, зокрема й Україна. Встановлено, що у зв'язку з тим, що активно розвиваються інформаційно-комунікаційні технології та зростає залежність від них, відбулася поява нової царини протиборства, одну зі сторін котрої представляє російська федерація, яка негативно впливає на політичні та військові функції Північноатлантичного Альянсу в цілому та нашої держави в тому числі. Зауважено на тому, що рушієм еволюційних перетворень, яких зазнає гібридна війна, виступають: повсюдне цифрове підключення, заперечення причетності до атак та наявність переваг у порушенні діяльності, яку виконує критично важлива енергетична інфраструктура, завдяки операціям, залежним від мережевої роботи. Ще більш ускладнюється ситуація в Україні через те, що рф завдає масованих атак вітчизняній критичній інфраструктурі. Мета цього, зокрема, полягає в тому, щоб дестабілізувати українське суспільство, щоб у людей зросли невдоволення, апатія, агресія, конфлікти та ін. У зв'язку з цим необхідно наполягти, щоб вітчизняні державні органи в боротьбі з неоголошеною війною рф виконували подвійну роль: відстоювали власний суверенітет і територіальну цілісність та захищали енергетичну безпеку й критичну інфраструктуру від руйнівної дії, яку спричиняє вплив російської федерації. Підтримка в цій ситуації може бути надана міжнародною технічною допомогою, в тому числі НАТО. Встановлено, що Північноатлантичний Альянс володіє унікальним становищем, завдяки чому він може здійснити: посилення роботи, яку виконують держави-члени і яка нівелює вразливість, та узагальнення уроків, засвоєних у цій галузі. З'ясовано, що задля цього 2012 року у Вільнюсі відбулося створення Центру передового досвіду НАТО з енергетичної безпеки. Разом з тим Альянс підтримав і формування 2017 року в Гельсінкі Європейського центру, основою якого став передовий досвід того, як протистояти гібридним загрозам. НАТО має досягнути належного рівня оперативної співпраці заради стримування потенційно руйнівних гібридних нападів російської федерації на об'єкти енергетичної інфраструктури та їхньої подальшої відбудови в разі завданої нападами шкоди.

Список літератури:

1. Помаза-Пономаренко А., Тарадуда Д. Світовий досвід протистояння впливу гібридної війни на національну й енергетичну безпеку та її об'єкти. *Публічне управління: концепції, парадигма, розвиток, удосконалення.* 2024. Випуск 9. С. 142-150.

2. NATO Cooperative Cyber Defence Centre (CCDCOE). URL: https://surl.li/avhqkf

3. Dupuy A.C., Nussbaum D., Butrimas V., Granitsas A. Energy Security in the Age of Hybrid Warfare. URL: https://surl.li/qryfcw

4. Ковальов КЄ. Інформаційна безпека: міжнародно-правовий аспект. *Інформація і право*. 2023. № 4 (47). С. 159-167.

5. Network and information security: proposal for a european policy approach. URL: https://surl.li/mdcxpv

6. Гора І.В., Батюк О.В. Окремі питання захисту об'єктів критичної інфраструктури: зарубіжний досвід. *Соціально-правові студії.* 2021. Випуск 1 (11). С. 132-139.

7. Братель С.Г. Досвід зарубіжних країн у сфері забезпечення безпеки об'єктів критичної інфраструктури. URL: http://www.sulj.oduvs.od.ua/archive/2023/3/41.pdf.

8. Герасименко О.М. Загрози об'єктам критичної інфраструктури України в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету.* 2024. Випуск 84. С. 257-263.

Hornyk V.H., Yevmieshkina O.L., Simak S.V. INNOVATIVE APPROACHES TO DIGITAL TRANSFORMATION OF PUBLIC ADMINISTRATION IN EU COUNTRIES AND CANDIDATE COUNTRIES TO ENSURING INFORMATION AND ENERGY SECURITY

The article is devoted to the disclosure of innovative approaches to the digital transformation of public administration in the EU countries and candidate countries to ensure information and energy security. It was found that the most important current task in the field of ensuring the country's energy security is the practical and effective implementation of previously defined strategic goals and mechanisms for their implementation. This requires joint and mutually agreed actions of all branches of government, the establishment of responsibility and proper control. Today, the problems of ensuring energy security have acquired a truly global nature, while there is no acceptable and mutually recognized strategy for ensuring energy security at the global or pan-European level. The absence of a single EU energy policy is a certain threat to ensuring the energy security of both the member states of the commonwealth themselves and neighboring countries (including Ukraine). Ukraine's strategic intentions largely consist in realizing the country's advantageous geopolitical position as one of the powerful transitors of the FER. The lack of common views on specific projects and mechanisms for

their implementation significantly hampers the development of the energy sector and the implementation of the country's Energy Strategy.

It was determined that the results of the analysis of the experience of leading countries in the world indicate that in Ukraine, special attention in the field of ensuring information and energy security should be directed to: bringing regulatory and legal acts into line with today's requirements (cyberattacks, mass unrest, military actions, epidemics); implementing a national resilience system; creating a main body responsible for ensuring information and energy security at the national level; establishing a partnership between the state, local governments, public associations, private business and international partners on issues of ensuring information and energy security; conducting interdepartmental exercises and training with the participation of the population in order to increase the level of awareness and readiness to respond to threats to information and energy security.

Key words: *public administration, state policy, national security, energy security, information security.*