УДК 349.3:332.1:331.101
DOI https://doi.org/10.32782/TNU-2663-6468/2024.6/05

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

ЦИФРОВІЗАЦІЯ ЯК ІНСТРУМЕНТ ПУБЛІЧНОГО УПРАВЛІННЯ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ

Стаття присвячена дослідженню цифровізації в якості одного з головних інструментів публічного управління в контексті забезпечення інформаційної та енергетичної безпеки, яка вважається важливим елементом національної безпеки України, а в період повномасштабної війни вона відіграє дедалі більшу роль і для безпеки Європи, в тому числі в аспекті енергетичного переходу і гарантування передумов стабільного майбутнього. Подано визначення суті терміну «цифровізація» різними вченими, базуючись на котрих з'ясовано, що цифровізація, котру прийнято вважати комплексним використанням комп'ютерних інтерфейсів, стає все більше всеохоплюючим і різноманітним феноменом у всіх секторах соціально-економічної системи. Визначено основну мету й деякі нюанси цифровізації енергетичної сфери. Виокремлено основні засади утворення й функціонування механізму впливу цифровізації на гарантування інформаційної, а також енергетичної безпеки.

Досліджено головні загрози інформаційній та енергетичній безпеці. Водночас із позитивним впливом застосування цифрових технологій здатне ставити під загрозу користувачів щодо значних цифрових ризиків і кіберзагрози, спричиняючи матеріальні й моральні збитки, а також репутаційні втрати. Потенційно може постати ряд проблем, які пов'язані з неоднаковим доступом до цифрових технологій, зосередженням ринкової влади в руках малої групи розвинених в технологічному контексті компаній, змогою контролювання й маніпуляцій зі сторони держави, потребою зростання захисту персональної інформації та цифрових активів, кібербезпекою, зменшенням ризиків несанкціонованого доступу до мереж та ін.

Визначено, що цифровізація здатна розв'язати проблеми, що тільки зростатимуть у перспективі, розгорнувши у трьох площинах: «раціональне» виробництво енергії, «раціональне» поводження з нею і розрахунками з клієнтами і «розумне» споживання. З цією метою запропоновано вводити такі вектори: децентралізація виробництва енергії, розвиток технологій розумних мереж, цифровізація енергетичної інфраструктури, введення технологій інтернету речей, формування єдиної цифрової енергетичної платформи, розвиток цифрових клієнтських сервісів.

Ключові слова: *цифровізація, інформаційна безпека, енергетика, енергетична безпека, ризики, принципи.*

Постановка проблеми. Коли розпочалася повномасштабна військова агресія росії проти України, передусім гостро стали простежуватися виклики щодо інформаційних систем, як в секторі оборони й національної безпеки, так і у напрямках енергетичної безпеки, а також інших головних векторів здійснення функцій публічного управління. Інформаційна та енергетична безпека – базис здійснення дієвих функцій публічного управління гарантування суспільно-політичних і соціально-економічних процесів. Обставини повної військової агресії – вкрай важке випробування для інформаційної та енергетичної безпеки держави. В такій ситуації інформаційна та енергетична безпека являється вкрай значущою, тому що в залежності від результативності заходів, затверджених у цьому контексті, можуть залежати наслідки війни. На державному рівні на тлі повної військової агресії, інформаційна та енергетична безпека повинна забезпечуватися на декіль-

ких рівнях. Насамперед держава мусить володіти досконалою системою збирання й розгляду відомостей з різних джерел, аби швидко відповідати на зміни в обставинах на полі бою й усвідомлювати інтенції супротивника. Потім вагоме значення має гарантування безпеки інформаційної інфраструктури країни. Це значить – захист від хакерських атак, вірусів й решти загроз, які здатні порушити функціонування інформаційних систем, які застосовуються військовими і цивільними владними органами. Крім того, значущою складовою інформаційної та енергетичної безпеки вважається підготовка і навчання військового, а також цивільного персоналу стосовно захисту даних і реагування на загрози інформаційного характеру. така підготовка може містити курси з кібербезпеки, тренінги з психології війни, навчання застосуванню сучасних технологій і систем захисту даних. Таким чином, зважаючи на значну актуальність розгляду, доречно звернутися на дослідження цього питання.

Аналіз останніх досліджень і публікацій. Актуальність теми формує увагу авторів до цієї тематики, так, викликають інтерес праці І. Абрамовича, С. Дмитрука, В. Міщенка, Т. Подорожної, М. Сакала, С. Савчука, М. Сухоноса, Є. Тіщенка та інших. Однак в обставинах нових викликів суспільства України доречно звернутися до актуальних проблем цифровізації в якості одного з головних інструментів публічного управління в контексті забезпечення інформаційної та енергетичної безпеки.

Постановка завдання. Метою статті є дослідження цифровізації в якості одного з головних інструментів публічного управління в контексті забезпечення інформаційної та енергетичної безпеки.

Виклад основного матеріалу. Органи публічної влади пристосовуються до нових обставин діяльності в ІТ-сфері, зважаючи на нові значні виклики, загрози й ризики. Зростання протиправного впливу на інформаційні ресурси у системі публічного управління потребують здійснення додаткових заходів стосовно забезпечення інформаційної та енергетичної безпеки. Оскільки виникнення нових інформаційних технологій обумовлює зміну усталених парадигм, формує нові правила стосовно застосування інформаційних систем, забезпечивши водночас черговий поштовх щодо переходу в цифровий сектор функціонування публічних органів та недержавних організацій.

Довгий період проблема гарантування інформаційної та енергетичної безпеки – вагомий елемент національної безпеки України, а в ході повномасштабної війни вона відіграє дедалі більшу роль і для безпеки Європи, в тому числі у розрізі енергетичного переходу й гарантування підгрунтя стабільного майбутнього. Їх розв'язання перебуває не тільки у військово-політичному аспекті, а також у використанні сучасних інструментів цифровізації.

Однією з головних умов економічної безпеки держави є ефективна енергетична політика щодо сталого енергопостачання. У даний час світовий енергетичний сектор характеризується обмеженнями та вичерпанням запасів вуглеводнів, зростаючим попитом на енергію, коливаннями цін на енергоносії та підвищенням екологічних вимог до їх використання [1]. Визначальний вплив на розвиток енергетичного сектору в сучасних умовах мають тренди цифровізації та інформатизації, тренди декарбонізації, поступове впровадження здобутків Четвертої промислової революції, а також соціально-економічна нестабільність в глобальному масштабі [2].

Цифровізація – це процес перетворення аналогової інформації чи процесів на цифровий формат, що забезпечує їх представлення та обробку за допомогою цифрових технологій. Це важливий стрімкий процес, що охоплює різні сфери життя, такі як бізнес, освіта, охорона здоров'я та багато інших. Цифровізація дозволяє покращити ефективність, зручність та доступність багатьох послуг і продуктів, сприяє інноваціям та розвитку суспільства в цілому. Цифровізація є глибоким процесом трансформації, який передбачає переведення різноманітної інформації, включаючи текст, звуки, зображення та відео, у цифровий формат. Цифровізація відіграє ключову роль у сучасному світі, забезпечуючи підвищення продуктивності, оптимізацію процесів та сприяє інноваціям. Застосування цифрових технологій у бізнесі дозволяє автоматизувати задачі, вдосконалювати виробництво, розробляти нові продукти та послуги, а також поліпшує взаємодію з клієнтами [3].

На нинішній стадії людського прогресу цифровізація, котру визнано вважати комплексним використанням комп'ютерних інтерфейсів, стає все більш всеохоплюючим і різноаспектним феноменом у всіх секторах соціально-економічної системи. Поняття такого плану, як «цифрова екологія» й «цифрова екосистема», починають застосовувати всюди, й вони розповсюджуються на всі сектори стабільного розвитку, зокрема економічний, соціальний і екологічний. Обов'язково відбувається розвиток інфраструктури переда-

вання інформації, її збереження й опрацювання. Зважаючи на розвиток цифрових технологій реально й неминуче утворюється інша реальність, котру прийнято називати «хмарною». Якраз цю «хмарну» реальність досліджують як чергову еволюційну стадію розвитку раніше утвореної моделі соціально-економічного й техніко-технологічного порядку суспільства.

Метою цифровізації енергетичного сектору є забезпечення гнучкого, відритого, прозорого ринку торгівлі енергією з рівною можливістю участі кожного суб'єкта. Приклади застосування цифрових технологій в енергетичній галузі у світі включають: технології блокчейну, бізнес-платформи, дрони та дистанційна реєстрація, штучний інтелект, великі дані, інтернет речей, розумні мережі, технологія «цифрового близнюка» і т.д. [4].

У сфері енергетики цифровізація відіграє ключову роль у вдосконаленні виробництва, передачі та споживання електроенергії. Ось деякі аспекти цифровізації в цій галузі:

1. Моніторинг та управління: Цифрові системи моніторингу дозволяють збирати дані з енергетичних об'єктів в режимі реального часу. Це включає в себе інформацію про виробництво, передачу та споживання енергії.

2. Смарт-мережі: Цифровізація сприяє створенню смарт-мереж, де дані передаються автоматично та можуть бути опрацьовані для оптимізації розподілу енергії. Це дозволяє втручатися у мережу для зменшення втрат енергії та підвищення її стабільності.

3. Енергоефективність: За допомогою сенсорів та аналітики дані можуть використовуватися для виявлення місць зайвого споживання енергії. Це дозволяє впроваджувати енергозберігаючі технології та оптимізувати виробництво.

4. Прогнозування попиту: Аналіз великих даних (Big Data) дозволяє створювати моделі для прогнозування попиту на енергію в майбутньому. Це допомагає енергетичним компаніям планувати виробництво та передачу енергії заздалегідь, зменшуючи ризики нестачі чи перевиробництва.

5. Віддалене управління: Цифрові системи дозволяють віддалено контролювати та управляти енергетичними об'єктами, що забезпечує більш гнучкий та ефективний контроль над енергопостачанням. Цифровізація в енергетиці сприяє підвищенню надійності, зменшенню витрат та створює умови для переходу до сталого та ефективного енергетичного майбутнього [5].

Ключовими принципами формування та функціонування механізму впливу цифровізації на забезпечення інформаційної та енергетичної безпеки, на наш погляд, повинні бути:

– системність (цифровізація розглядається як системний процес, що впливає на всі сфери економіки і суспільства, формуючи нові виробничі відносини на базі інформаційно-технологічного та інтелектуального капіталу);

– комплексність (стратегічне управління процесами цифровізації з метою забезпечення взаємопов'язаності та підпорядкованості цілей);

– цільова спрямованість та орієнтація на досягнення ключових завдань, передбачених державною політикою в галузі цифровізації;

– стандартизованість (запровадження та дотримання міжнародних і національних стандартів, які визначають умови впровадження та використання цифрових технологій);

– пропорційність (забезпечення відповідності між використанням цифрових технологій і завданнями соціально-економічного розвитку);

– збалансованість (забезпечення рівноваги між інтересами держави, бізнесу, громадян і суспільства, надання всім суб'єктам рівних можливостей для доступу до методів та інструментів використовуваного механізму);

– гнучкість (здатність швидко адаптуватися та оперативно реагувати на зміни у цифровому середовищі);

– керованість (забезпечення належного рівня взаємодії та чітке визначення обов'язків і відповідальності суб'єктів та об'єктів управління);

– ефективність (забезпечення окупності витрат та досягнення ефекту синергії від впровадження і використання цифрових технологій);

– соціальна спрямованість (врахування етичних принципів використання цифрових технологій та інтересів широких верств суспільства);

– інтегрованість у світову систему цифрової економіки та цифрового бізнесу за умови збереження цифрового суверенітету країни [6].

Вплив сучасних інформаційно-комунікаційних технологій проявляється насамперед у сфері особистих прав, серед яких особливе місце посідає право на недоторканність приватного життя. Без інформаційної безпеки не може бути недоторканності приватного життя. Тому забезпечення інформаційної безпеки особистості становить основу правового захисту недоторканності приватного життя. З розвитком технологій істотно збільшуються обсяги та швидкість обміну інформацією, розширюється спектр можливих способів її збирання, обробки, надання та поширення. У підсумку шкода, яка може бути завдана індивідові внаслідок розкриття тієї чи іншої інформа-

ції або у зв'язку зі збереженням її в таємниці, також зростає. Утім, держава завжди оперативніше реагує на можливості, які надають нові інформаційно-комунікаційні технології для захисту публічних інтересів, ніж приватних. Це пов'язано з тим, що стійкість функціонування інститутів публічної влади, збереження правопорядку є необхідною передумовою дотримання прав людини. Більшість держав відреагувало на загрози національній безпеці, що зросли останнім часом, розширивши повноваження органів влади з доступу до особистої інформації, її збору та обробки, які зараз не обмежені якимись окремими категоріями інформації. При цьому в різних державах підходи до забезпечення пропорційності вживаних заходів щодо забезпечення національної безпеки також можуть відрізнятися [7].

Водночас із позитивним впливом застосування цифрових технологій здатне ставити під загрозу користувачів щодо значних цифрових ризиків і кіберзагрози, спричиняючи матеріальні й моральні збитки, а також репутаційні втрати. Потенційно може постати ряд проблем, які пов'язані з неоднаковим доступом до цифрових технологій, зосередженням ринкової влади в руках малої групи розвинених в технологічному контексті компаній, змогою контролювання й маніпуляцій зі сторони держави, потребою зростання захисту персональної інформації та цифрових активів, кібербезпекою, зменшенням ризиків несанкціонованого доступу до мереж та ін.

Таким чином, новітні виклики та загрози інформаційній та енергетичній безпеці можливо класифікувати на внутрішні й зовнішні. До внутрішніх загроз в інформаційній та енергетичній сфері відносимо:

1) постійне порушення правил стосовно порядку використання даних обмеженого доступу;

2) неіснування чи неналежний ступінь кваліфікації працівників щодо застосування інформаційних та комп'ютерних приладів, а також іншої продукції, що потрібна для гарантування інформаційної та енергетичної безпеки;

3) застосування іноземних технологій та технічних інструментів в інформаційних процесах;

4) порушення правових норм стосовно захисту авторських прав у процесі напрацювання та введення секретних винаходів, зроблених, в тому числі, відповідно до державного замовлення;

5) колізії й правові прогалини в національному законодавстві під час регулювання відносин в секторі інформаційної та енергетичної безпеки та ін.

Серед зовнішніх загроз в інформаційній та енергетичній сфері можна назвати:

1) активні розвідувальні й контрнаступальні заходи іноземних органів спецслужб, а саме російської федерації;

2) постійні агресивні інформаційні заходи через кібератаки на об'єкти інформаційних інфраструктур;

3) використання методів та інструментів інформаційної війни зі сторони російської федерації, застосовуючи когнітивну зброю проти національних інтересів України;

4) застосування специфічних прийомів у інформаційній сфері, що стосуються інтересів міждержавної співпраці у секторі гарантування інформаційної та енергетичної безпеки;

5) використання методології фільтрації цифрового контенту в інтернеті, щоб обмежити розповсюдження правдивих відомостей щодо політики держави й ініціативи, які вона просуває (це має відношення, в тому числі, до відомостей, що висвітлюється у фейсбуці та ін.).

Висновки. Отже, хоч цифровізація забезпечує чимало змог для розвитку як сфери, так і певного підприємства, вона, крім того, здатна зробити значно вразливішими енергетичні системи до кібератак. Наразі шкода, заподіяна енергетичним системам кібератаками, – порівняно незначна. Щодо влаштування самі атаки стають більш простими, в той час як ризики порушення кібербезпеки збільшуються, коли розвивається цифрове устаткування й інтернет речей. Найбільші кібератаки, що вчиняли для того, аби заподіяти шкоди енергетичній системі останніми роками, показують, наскільки вразливі інформаційні системи та підтверджують потребу гарантування кібербезпеки підприємства, проте профілактика кібератак повною мірою не є можливою, хоч їхній негативний вплив можливо обмежити, коли гарантувати відповідний ступінь безпеки на державному рівні й на рівні підприємства. Формування стабільної системи залежить від осмислення й розуміння усіма заінтересованими сторонами потенційних ризиків. Цифрова безпека має стати головною під час здійснення технологічних досліджень і напрацювань та, крім того, братися до уваги при написанні стратегії розвитку підприємства, сфери або держави. Цифровізація здатна розв'язати проблеми, що тільки зростатимуть у перспективі, розгорнувши у трьох площинах: «раціональне» виробництво енергії, «раціональне» поводження з нею і розрахунками з клієнтами і «розумне» споживання. З цією метою запропоновано вводити такі вектори: децентралізація виробництва енергії, розвиток технологій розумних мереж, цифровізація енергетичної інфраструктури, введення технологій інтернету речей, формування єдиної цифрової енергетичної платформи, розвиток цифрових клієнтських сервісів.

Список літератури:

1. Dzoba O., Marynchak L., Romashko O. A new approach to the assessment of effective management of gas supply diversification. *Baltic Journal of Economic Studies.* 2017. № 1. P. 24-30.
2. Абрамович І.О., Дмитрук С.М. Підвищення ефективності управління персоналом в контексті особливостей розвитку підприємств енергетичного сектору України. *Вісник соціально-економічних досліджень.* 2019. № 2-3 (70-71). С. 54-62.
3. Сакала М. Цифровізація у сфері енергетики. URL: http://188.190.43.194:7980/jspui/bitstream/123456789/12487/1/%D0%95%D0%92%D0%95%D0%A1%D0%9F-23-424-426.pdf
4. Савчук С. Перспективи розвитку енергетичної галузі в умовах цифровізації. *Scientific Collection «InterConf»*. 2024. № 204. С. 57-60.
5. Сухонос М.К. Використання інформаційних систем і технологій для муніципального утворення і систем енергозабезпечення міст. URL: http://nbuv.gov.ua/UJRN/ecee_2010_3_4
6. Міщенко В.І., Тіщенко Є.О. Методологічні засади формування механізму впливу цифровізації на забезпечення національно укоріненої стійкості та безпеки економічного розвитку. *Підприємництво та інновації.* 2024. Випуск 32. С. 71-80.
7. Подорожна Т.С. Забезпечення інформаційної безпеки України в умовах сучасних викликів та загроз з боку РФ. Електронне наукове видання «Аналітично-порівняльне правознавство». URL: https://app-journal.in.ua/wp-content/uploads/2023/12/87.pdf

Hornyk V.H., Yevmieshkina O.L., Simak S.V. DIGITALIZATION AS A PUBLIC ADMINISTRATION TOOL IN THE CONTEXT OF ENSURING INFORMATION AND ENERGY SECURITY

The article is devoted to the study of digitalization as one of the main tools of public administration in the context of ensuring information and energy security, which is a significant part of the national security of Ukraine, and during a full-scale war it is gaining increasing importance for the security of Europe, in particular in the context of energy transition and ensuring the conditions for a sustainable future. The interpretation of the essence of the concept of "digitalization" by various scientists is presented, on the basis of which it is established that digitalization, which is generally understood as the complex use of computer interfaces, is becoming an increasingly comprehensive and diverse phenomenon in all areas of the socio-economic system. The main goal and individual aspects of digitalization of the energy sector are highlighted. The main principles of the formation and functioning of the mechanism of influence of digitalization on ensuring information and energy security are determined.

The main threats to information and energy security are considered. Along with the positive impact of the use of digital technologies, it can expose users to significant digital risks and cyber threats, causing material and moral damage and reputational losses. A number of problems may potentially arise related to inequality of access to digital technologies, concentration of market power in the hands of a small group of technologically advanced companies, the possibility of control and manipulation by the state, the need to strengthen the protection of personal data and digital assets, cybersecurity, reducing the risks of unauthorized access to networks, etc.

It is established that digitalization can solve problems that will only intensify in the future, expanding in three dimensions: "rational" energy production, "rational" handling of it and settlements with customers, and "smart" consumption. To this end, it is proposed to implement the following steps: decentralization of energy production, development of smart grid technologies, digitalization of energy infrastructure, implementation of Internet of Things technologies, creation of a single digital energy platform, development of digital client services.

Key words: *digitalization, information security, energy, energy security, risks, principles.*