УДК 620.9:005.332.5]:004.89:338.246.8 DOI: 10.26906/EiR.2026.2(101).4665
JEL H56, O32

ЦИФРОВІЗАЦІЯ ЕНЕРГЕТИЧНОГО СЕКТОРУ: КІБЕРРИЗИКИ, ВРАЗЛИВОСТІ РОЗУМНИХ МЕРЕЖ ТА МЕХАНІЗМИ ЗАХИСТУ ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Чичкало-Кондрацька Ірина Борисівна*, доктор економічних наук, професор,
завідувач кафедри міжнародних економічних відносин та туризму
Національний університет «Полтавська політехніка
імені Юрія Кондратюка»

**ORCID 0000-0003-3123-841X*

Дата надходження статті: 17.03.2026
Дата прийняття статті: 07.04.2026
Дата публікації статті: 29.05.2026

Вступ. Наукові дискурси щодо енергетичної безпеки розвинулися у відповідь на спочатку окремі політичні програми, зокрема постачання палива для армії та транспорту, безперебійне постачання електроенергії, забезпечення ефективності функціонування енергетичного ринку й інвестицій. У результаті виникли три різні перспективні напрями досліджень енергетичної безпеки: «суверенітету» з корінням у політичній науці; «надійності», яка потребує технічних розробок; основи стійкого розвитку, що вимагає досліджень в сфері економіки та аналізу складних систем [1]. Наразі проблеми енергетичної безпеки дедалі більше переплітаються, тому їх неможливо проаналізувати в межах єдиного напряму. Доцільним є міждисциплінарний підхід, який об'єднує теорії, методи та знання з різних підходів.

Крім того, в останні роки отримали розвиток нові процеси, виникли нові загрози енергетичній безпеці. Так, зростаюча залежність від цифрових технологій та взаємопов'язаних систем зробила енергетичний сектор більш вразливим до кібератак. Безумовно це обумовлено критичним характером його інфраструктури. Щоб забезпечити стабільність, безпеку та стійкість цих життєво важливих систем, кібербезпека стала дуже важливою для енергетичного сектору. Вона захищає від несанкціонованого доступу, використання, розкриття, переривання, зміни або знищення комп'ютерних систем, мереж та конфіденційної інформації. Слід відзначити, що є і позитивні наслідки цифровізації: завдяки технічним проривам, таким як високошвидкісний Інтернет та Інтернет речей (IoT), енергетичний бізнес отримав суттєве зростання за останні роки. Ці технології змінили те, як підприємства працюють через кордони, без встановлених меж. Це відкрило можливості для зростання в багатьох галузях економіки. Енергетичний сектор не є винятком, оскільки його критична інфраструктура тепер пов'язана по всьому світу, що робить захист активів життєво важливим для успішного управління.

Огляд останніх джерел досліджень і публікацій. Енергетична безпека є практичною проблемою більше століття, а також стала окремою галуззю наукових досліджень за останні кілька десятиліть. Водночас, можливості сучасних досліджень енергетичної безпеки для формування енергетичної політики були обмеженими. Історичне коріння ідей енергетичної безпеки може пояснити це обмеження. Такі ідеї виникли як відповіді на кілька окремих політичних проблем.

Так, у першій половині 20-го століття, кульмінацією якої стала Друга світова війна, поняття енергетичної безпеки було тісно пов'язане з постачанням палива для військових. До кінця 20-го століття енергетична безпека вже не була суто геополітичною проблемою, хоча забезпечення доступу до палива, що продається на міжнародному рівні, особливо нафти, все ще було в її центрі. Тодішні виклики енергетичній безпеці обумовили необхідність враховувати вразливості складних технічних систем, глобальні

обмеження, роль ринків та інвестицій, що вивело наукові дослідження на орбіту дискурсів в галузях природничих, технічних та економічних наук [1].

Подальші політичні та інтеграційні виклики вимагали розширення фокусу дослідження фахівцями з енергетичної безпеки як з конкретних, так і загальних питань: як зменшити залежність від іноземної нафти, як забезпечити надійне постачання електроенергії, як зробити енергетичні системи безпечнішими [2, 3]. Це передбачало пошук комплексних рішень для численних проблем енергетичної безпеки.

Окремі дослідження були спрямовані на встановлення ефективної межі витрат і диверсифікації, використовуючи теорію портфеля для балансування витрат та ризиків постачання, застосовуючи її, наприклад, до енергосистеми Великої Британії [3]. Фахівці наголошували на тому, що для енергетичної політики важливим є досягнення різноманітності, щоб уникнути надмірної залежності від одного виду палива чи технології.

Вітчизняні науковці також активно досліджують проблему енергетичної безпеки, яка особливо загострилась з початку повномасштабної російсько-української війни. Вчені розробляють концептуальні засади енергетичної безпеки з урахуванням сучасних викликів, зумовлених одночасно наростаючими кризами в енергетиці, еко-номіці та геополітиці [4], оцінюють деструктивні чинники, що мають вагомий вплив на здійснення глобального енергетичного переходу [5], розглядають перспективні шляхи зміцнення енергетичної безпеки та потенційні сценарії розвитку світової енергетики [6].

Таким чином, огляд наукових праць в цій сфері показує, що дослідження енергетичної безпеки історично розвивалися в межах кількох окремих напрямів, реагуючи на окремі політичні виклики. Ця еволюція призвела до появи декількох конкретних наукових та політичних спільнот, які досліджували проблеми енергетичної безпеки з різних точок зору. Кожна з цих спільнот зосереджувалася на певній системі проблем та представляла окремий набір відповідей.

Однак сучасна складність та швидкі темпи трансформації енергетичних систем призводять до того, що ці проблеми більше не можуть бути ефективно вивчені або вирішені ізольовано одна від одної. Крім того, в останні роки суттєвий вплив мають нові виклики для енергетичної інфраструктури, пов’язані з кібербезпекою та кібертероризмом.

Метою нашої статті є аналіз цифровізації енергетичних систем, виділення відмінностей розумних енергетичних мереж, виявлення загроз кібербезпеці енергетичного сектору, розгляд економічного впливу кібератак, визначення запобіжних заходів та захисних механізмів.

Основний матеріал дослідження і результати. Енергетична безпека є однією з головних цілей енергетичної політики держави. Однак фахівці розглядають багато визначень енергетичної безпеки. Найширша концепція включає всі ризики, які спричинені ланцюгом постачання енергії або впливають на нього [7]. Енергетичну безпеку характеризують відповідно до джерел ризику, масштабів впливу та рівня відчутності, зокрема швидкість, розмір, стійкість, поширення та неминучість впливу. Це підводить нас до визначення енергетичної безпеки як безперервності поставок енергії відносно попиту.

Безпека постачання є важливою метою енергетичної політики в багатьох країнах світу. Проведений аналіз показав, що головними стовпами енергетичної політики Європейського Союзу є ефективність, сталий розвиток, безпека енергопостачання, зелений перехід [8].

У США основна увага в енергетичній безпеці традиційно зосереджувалася на зменшенні вразливості до політичного шантажу, що спонукало політиків закликати до енергетичної незалежності та збільшення частки відновлюваної енергії. З іншого боку, в Бразилії, де зараз бачення енергетичної незалежності вже стало реальністю, були періоди, коли політики виступали за збільшення частки імпорту викопного палива та зменшення частки відновлюваної енергії для сприяння енергетичній безпеці.

За відсутності чіткого визначення, енергетична безпека стала загальним терміном для багатьох різних політичних цілей. Тому енергетична політика країн може мати різну мету для досягнення енергетичної безпеки: захист цін на енергетичні ресурси; надійне постачання палива; захист економіки від перебоїв у постачанні енергетичних послуг, дозволяючи цінам на сировинні товари зростати в періоди дефіциту; зменшення небезпеки від аварій; не допущення розширення ядерної промисловості, що є потенційною загрозою енергетичній безпеці тощо.

Але слід зазначити, що, незважаючи на різні підходи до концепції енергетичної безпеки, між фахівцями існує згода щодо того, що вона пов'язана з ризиками. Однак кількість загроз, які спричинені або впливають на ланцюг постачання енергії, є величезною. Основною причиною відмінностей між

концепціями енергетичної безпеки є, таким чином, спосіб, у який автори обирають підмножину цих загроз, яку вони розглядають.

На основі огляду літератури ми виявили, що спільною концепцією, що лежить в основі всіх визначень енергетичної безпеки, є відсутність, захист або адаптивність до загроз, що спричинені чи впливають на ланцюг постачання енергії. Через складність одночасного вимірювання всіх цих загроз окремі автори обмежують концепцію енергетичної безпеки одним або кількома з вимірів.

Ми згодні з фахівцями [9], що стійкість енергетичної системи залежить від самої системи та загрози. Серйозні збої можуть завдати збитків, які перевищують багаторічні доходи сектору. Ми хочемо звузити концепцію енергетичної безпеки, щоб зменшити дублювання між різними цілями енергетичної політики. Відповідні типи загроз змінюються разом зі зміною систем. Тому ми зосередимося на впливі цифровізації енергетичного сектору та кіберзагроз на енергетичну безпеку.

Інтернет став потужним засобом комунікації у всьому світі, що дозволяє кібертерористам координувати та планувати атаки, потенційно уникаючи виявлення. Тим часом, розгортання розумних енергетичних систем з використанням інновацій ІКТ спричинило розвиток енергетичного сектору, але також створило нові вразливості, особливо тому, що енергетика тісно пов'язана з критичною інфраструктурою. Хоча інструменти кібербезпеки відносно доступні, вони можуть бути складними та використовуватися для захисних цілей, потенційно завдаючи шкоди країнам.

Збільшення цифрових можливостей енергетичних систем робить їх більш ефективними та захищеними від традиційних загроз, наприклад, екстремальні погодні явища та технічні збої. Водночас, цифровізація наражає енергетичний сектор на кібератаки і збільшує масштаб атаки [10]. Хоча кібератаки залишаються відповідальними лише за невелику частину збоїв в енергопостачаннях, потенційна шкода є значною та швидко зростає.

Тобто наслідки успішної кібератаки на енергетичний сектор можуть бути серйозними та тривалими. Кібератака може спричинити перебої у подачі електроенергії, розлив нафти або ядерні аварії, що призведе до економічних втрат, шкоди навколишньому середовищу та навіть смерті людей. Кібератаки на енергетичний сектор також можуть мати каскадний вплив на інші сектори, такі як транспорт, охорона здоров'я, зв'язок та ін., що призведе до подальших порушень.

Енергетичний сектор стикається з ризиками кібербезпеки, спричиненими як синтаксичними, так і семантичними атаками [11]. Синтаксичні атаки спрямовані на програмне забезпечення та комунікаційні структури, створюючи такі загрози, як несанкціонований доступ та перебої в роботі енергомережі. Використання семантичних вразливостей призводить до помилкової інтерпретації даних, ризикуючи прийняттям неправильних рішень системами управління енергією та ставлячи під загрозу розподіл, стабільність мережі та роботу обладнання.

Таким чином, потенційні наслідки кібератак можуть включати крадіжку даних чи електроенергії, припинення електропостачання, порушення нормальної роботи енергетичної системи та навіть знищення обладнання [12]. Найпоширеніше групування кібератак та відповідні цілі захисту стосуються доступності, цілісності та конфіденційності компонентів енергетичної системи [13]. Атаки на доступність спрямовані на затримку, блокування або пошкодження зв'язку; атаки на цілісність – на зміну або порушення обміну даними; атаки на конфіденційність – на отримання несанкціонованої інформації. Доступність та цілісність мають вирішальне значення для надійної роботи енергетичних систем. Порушення конфіденційності не є критичним у цьому відношенні, але її важливість зростає зі збільшенням кількості «розумних» клієнтів та обсягу конфіденційних даних.

Цифровізація енергетичних систем особливо інтенсивна в так званих розумних мережах (РМ), які обробляють великі обсяги даних про енергопостачання й попит для оптимальної та ефективної роботи енергетичних систем. Численні літературні джерела з РМ часто не враховують проблеми безпеки, зосереджуючись більше на технічній реалізації та відповідних перевагах [14].

Цифрові мережі в енергетичній інфраструктурі відрізняються від усталених мереж інформаційних та комунікаційних технологій, таких як Інтернет, що суттєво обмежує можливість застосування існуючих рішень у сфері кібербезпеки. Відмінності з очевидними наслідками для кібербезпеки включають наступне [13, 14]:

– тривалість життєвого циклу компонентів набагато довша, ніж у побутовій електроніці;

– віддаленість багатьох компонентів робить дистанційне керування та оновлення економічною необхідністю, водночас обмежуючи можливі варіанти цифрової та фізичної безпеки;

– вимоги до швидкості набагато суворіші, ніж у традиційних мережах передачі даних;

– хоча майже всі системи обробки даних можна тимчасово зупинити та перезавантажити у разі зараження, такі процедури в енергосистемах були б складними та дорогими;

– цілі конфіденційності та безпеки можуть суперечити одна одній.

Традиційно споживачі енергії були досить пасивними учасниками. Розглянемо трансформації, які відбулися в останній час і пов'язані з цифровізацією споживачів енергетичних систем. Ситуація змінюється зі збільшенням обсягу потоків даних та можливостей керування. Поряд із цим збільшується й кількість ризиків. По-перше, зростають проблеми, пов'язані з конфіденційністю даних. Персональна інформація з РМ (наприклад, моделі споживання, що вказують на використання приладів та присутність людей вдома) сама по собі або в поєднанні з даними споживачів з Інтернету [14] може дати змогу злодіям вдаватися до дій. По-друге, розумні пристрої можуть бути зламані для маніпулювання поведінкою споживачів, що спричиняє проблеми як для споживачів, так і для всієї мережі (наприклад, збільшення пікового споживання, зниження профілів напруги). По-третє, поширення можливостей керування енергосистемою відбувається принаймні частково за рахунок традиційних системних операторів. Розумними споживачами можна маніпулювати або зламати їхні системи [15], але традиційним операторам буде набагато важче виправити ситуацію.

Хоча досить багато компаній зазнало кібератак, у тому числі і в Україні, кількість успішних масштабних кібератак залишається обмеженою [16]. Але нещодавно спостерігалися нові типи кібератак. До них належать ботнети, атаки нульового дня та розподілена відмова в обслуговуванні [11, 17]. Від нових прихованих та багатоетапних атак надзвичайно важко захиститися, і багатьом компаніям доводиться спочатку вирішувати базові проблеми безпеки. Наприклад, початковий доступ до енергетичної інфраструктури в деяких великих кібератаках було отримано через електронні листи [14].

Зв'язок між енергетичними кібератаками та економічними наслідками є значним, оскільки енергетичний сектор відіграє вирішальну роль в економіці багатьох країн. Перебої з постачанням енергії або пошкодження енергетичної інфраструктури можуть мати серйозні економічні наслідки, що призводять до зниження продуктивності й економічного зростання, а також до підвищення безробіття та інфляції. Більше того, кібератаки в енергетиці можуть безпосередньо впливати на ціни на енергоносії, що спричиняє збільшення витрат споживачів. Наприклад, кібератака на енергомережу України ще у 2015 році призвела до тимчасового зростання цін, оскільки країна була змушена покладатися на дорожчі джерела електроенергії [17].

Суттєвими можуть бути і прямі економічні наслідки кібератак. Енергетичні компанії часто роблять значний внесок у національну економіку, тому кібератаки на ці організації можуть мати серйозні фінансові наслідки. Наприклад, кібератака на Saudi Aramco у 2012 році завдала збитків приблизно на 1 мільярд доларів, тоді як атака через шкідливе програмне забезпечення NotPetya на Maersk у 2017 році призвела до втрати компанією понад 300 мільйонів доларів доходу [17]. Таким чином, енергетичні кібератаки становлять серйозну загрозу для енергетичного сектору та економіки в цілому, що робить їх важливим пріоритетом для урядів та бізнесу.

Глобальні збитки від кіберзлочинності оцінювалися за даними McAfee в 2013 році в 3 трильйони доларів; за даними Cyber Ventures склали 600 мільярдів доларів станом на 2017 рік [17]. За прогнозами, кіберзлочинність в найближчий час становитиме близька 6 трильйонів доларів.

Таким чином, будь-яка загроза енергетичній інфраструктурі матиме неминучі наслідки, що спричиняють збитки. Ці економічні втрати можуть призвести до збоїв у роботі бізнесу, зниження продуктивності, фінансових збитків та шкоди репутації, залежно від масштабу атаки або місця її зосередження. Економічний вплив може бути руйнівним, як у випадку кібератак, так і кібертероризму. Це також матиме численні наслідки для суспільства, компаній та людей.

Багато країн інвестують значні кошти у засоби захисту енергетичного сектору. Заходи захисту кібербезпеки охоплюють людей, програмне забезпечення, фізичну інфраструктуру та архітектуру енергетичної системи [13, 14].

Що стосується людей, то слід виділити такі заходи: кібергігієну, обмеження доступу, політику паролів, навчання користувачів, міжвідомчу комунікацію. Для програмного забезпечення слід наголосити на важливості таких заходів: своєчасні оновлення, суворий брандмауер, антивірусне програмне забезпечення, резервні копії, мережеві протоколи, криптографія.

Методи проектування мережевих протоколів дозволяють виявляти та блокувати атаки типу «відмова в обслуговуванні» на основі характеристик сигналу (сила та збої передачі для виявлення, частота передачі та адреса джерела для блокування). Мережеві заходи можуть допомогти забезпечити доступність, але є неефективними для забезпечення цілісності та конфіденційності операцій енергетичної системи [13].

Криптографічні заходи допомагають у всіх аспектах енергетичної системи (доступність, цілісність та конфіденційність). Доступні різні типи криптографії, що відрізняються симетрією ключа дешифрування та часом передачі. Основною дилемою вибору певного типу криптографії є баланс між забезпеченням певного рівня безпеки та необхідними ресурсами [13].

Децентралізація критично важливих можливостей цифрової енергетичної системи вимагає протидії методам поширення шкідливого програмного забезпечення без використання атакованої мережі [14].

Як встановлення, так і використання цих заходів вимагають обізнаності про кіберситуацію, яка включає знання поточної ситуації в мережі, розвитку ситуації під час атаки, якості зібраної інформації, впливу атак на критичне обладнання, поведінки зловмисника та можливих майбутніх кроків [14]. Впровадження достатніх заходів кібербезпеки в енергетичному секторі, що спираються лише на внутрішнє забезпечення якості та сертифікацію, може бути недостатнім. Можливо знадобитися регулювання, подібне до того, що застосовується в секторі охорони здоров'я. Важливим питанням є те, яка частина цифрового ланцюжка створення вартості повинна перебувати під контролем уряду. Інша потенційно необхідна роль уряду в сфері кібербезпеки енергетичної системи включає обмін певною розвідувальною інформацією та створення екосистеми реагування на кіберінциденти.

Висновки. Таким чином, енергетичні системи піддаються численним загрозам, потенційний вплив яких варіюється від незначних (енергетичні системи можуть поглинати їх без зміни продуктивності) до загрозливих для суспільства та економіки (відновлення триває роками). Концепція енергетичної безпеки передбачає перспективу для розробки контрзаходів для вирішення багатьох із цих загроз. Вона дозволяє боротися з помірними перебоями більш економічним способом і є важливою для подолання екстремальних та менш відомих загроз. Зокрема, забезпечення енергобезпеки вимагає, щоб енергетичний сектор залишався пильним перед обличчям постійно мінливих кіберзагроз і продовжував розробляти та впроваджувати ефективні стратегії управління ризиками для захисту від кібертероризму.

Розглядаючи перспективи подальших наукових розробок у цьому напрямі, слід зазначити, що структурні зміни, які очікуються в рамках енергетичного переходу, можуть зменшити багато актуальних на даний момент ризиків, але, у той же час, посилити інші вразливості. Деякі з найважливіших загроз для майбутніх енергетичних систем можуть бути абсолютно неактуальними для існуючих систем. Це вказує на необхідність широкого переосмислення загроз енергетичній безпеці в перспективних сценаріях розвитку. До майбутніх оцінок слід ставитися з обережністю, оскільки хибне відчуття безпеки саме по собі є серйозною вразливістю. Також не слід забувати, що зміни в масштабі можуть призвести до змін у характері загроз. Зростаюча взаємопов'язаність систем, зокрема, збільшує складність, приховуючи прогалини в енергетичній безпеці та зростаючі витрати, які в найгіршому випадку можуть знищити отриману економію від об'єднання систем.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ:

1. Cherp A., Jewell J. The three perspectives on energy security: intellectual history, disciplinary roots and the potential for integration. *Current Opinion in Environmental Sustainability*. 2011. Vol. 3, Issue 4. P. 202–212. DOI: https://doi.org/10.1016/j.cosust.2011.07.001

2. Lovins A. B., Lovins L. H. *Brittle Power: Energy Strategy for National Security*. Andover, MA: Brick House Publishing Co., 2010. 485 p.

3. Skea J. Valuing Diversity in Energy Supplies. *Energy Policy*. 2010. Vol. 38, Issue 7. P. 3608–3621. DOI: https://doi.org/10.1016/j.enpol.2010.02.038

4. Мазаракі А., Мельник Т. Енергетична безпека: нові виклики та світові тренди. *Scientia fructuosa*. 2024. Т. 155, № 3. С. 4–22. DOI: https://doi.org/10.31617/1.2024(155)01

5. Рябець Н., Тимків І. Глобальна енергетична безпека: концепт, фактори та шляхи забезпечення. *Економіка та суспільство*. 2024. № 61. DOI: https://doi.org/10.32782/2524-0072/2024-61-120

6. Ксендзук В. В., Покотило М. Ю. Енергетична безпека України та світу: оцінка наслідків впливу російсько-української війни та прогнози трансформації ринку. *Економіка, управління та адміністрування*. 2025. №2(112). С. 46–53. DOI: https://doi.org/10.26642/ema-2025-2(112)-46-53

7. Winzer C. Conceptualizing energy security. *Energy Policy*. 2012. Vol. 46. P. 36–48.

8. Чичкало-Кондрацька І. Б. Інституційні трансформації енергетичного сектору в умовах євроінтеграції: безпековий підхід. *Ефективна економіка*. 2026. № 3. DOI: https://doi.org/10.32702/2307-2105.2026.3.15

9. Jasiūnas J., Lund P. D., Mikkola J. Energy system resilience – A review. *Renewable and Sustainable Energy Reviews*. 2021. Vol. 150. 111476. DOI: https://doi.org/10.1016/j.rser.2021.111476

10. Langer L., Skopik F., Smith P., Kammerstetter M. From old to new: assessing cybersecurity risks for the evolving intelligent network. *Computers & Security*. 2016. Vol. 62. P. 165–176. DOI: https://doi.org/10.1016/j.cose.2016.07.008

11. Leshchyna R. Cybersecurity and privacy in standards for intelligent networks – a comprehensive survey. *Computer Standards & Interfaces*. 2018. Vol. 56. P. 62–73. DOI: https://doi.org/10.1016/j.csi.2017.09.005

12. Song C. K., Han A., Liu C. K. Power grid cybersecurity: state-of-the-art. *International Journal of Electrical Power & Energy Systems*. 2018. Vol. 99. P. 45–56. DOI: https://doi.org/10.1016/j.ijepes.2017.12.020

13. Wang W., Lu Z. Cybersecurity in the smart grid: a review and challenges. *Computers & Electrical Engineering*. 2018. Vol. 67. P. 469–482. DOI: https://doi.org/10.1016/j.compeleceng.2018.01.015

14. Eder-Neuhauser P., Zseby T., Fabini J., Vormayr G. Cyberattack models for smart grid environments. *Sustainable Energy, Grids and Networks*. 2017. Vol. 12. P. 10–29. DOI: https://doi.org/10.1016/j.segan.2017.08.002

15. Cloppenburg S., Bokelo M. Digital platforms and the future of energy supply: promises and dangers for the next stage of the energy transition. *Energy Research & Social Science*. 2019. Vol. 49. P. 68–73. DOI: https://doi.org/10.1016/j.erss.2018.10.016

16. Hagen J. Developing Cyber Resilience in the Energy Sector. *International Journal of Critical Infrastructure Protection*. 2018. Vol. 20. P. 26–27. DOI: https://doi.org/10.1016/j.ijcip.2017.11.003

17. Venkatachary S. K., Prasad J., Alagappan A., Andrews L. J. B., Raj R. A., Duraisamy S. Cybersecurity and cyber-terrorism challenges to energy-related infrastructures. Cybersecurity frameworks and economics. Comprehensive review. *International Journal of Critical Infrastructure Protection*. 2024. Vol. 45. 100677. DOI: https://doi.org/10.1016/j.ijcip.2024.100677

REFERENCES:

1. Cherp, A., & Jewell, J. (2011). The three perspectives on energy security: intellectual history, disciplinary roots and the potential for integration. *Current Opinion in Environmental Sustainability,* no. 3 (4), pp. 202–212. DOI: https://doi.org/10.1016/j.cosust.2011.07.001

2. Lovins, A. B., & Lovins, L. H. (2010). *Brittle Power: Energy Strategy for National Security*. Brick House Publishing Co.

3. Skea, J. (2010). Valuing diversity in energy supplies. *Energy Policy,* no. 38 (7), pp. 3608–3621. DOI: https://doi.org/10.1016/j.enpol.2010.02.038

4. Mazaraki, A., & Melnyk, T. (2024). Enerhetychna bezpeka: novi vyklyky ta svitovi trendy [Energy security: new challenges and global trends]. *Scientia fructuosa,* no. 155 (3), pp. 4–22. DOI: https://doi.org/10.31617/1.2024(155)01

5. Riabets, N., & Tymkiv, I. (2024). Hlobalna enerhetychna bezpeka: kontsept, faktory ta shliakhy zabezpechennia [Global energy security: concept, factors and ways to ensure it]. *Ekonomika ta suspilstvo*, no. (61). DOI: https://doi.org/10.32782/2524-0072/2024-61-120

6. Ksendzuk, V. V., & Pokotylo, M. Yu. (2025). Enerhetychna bezpeka Ukrainy ta svitu: otsinka naslidkiv vplyvu rosiisko-ukrainskoi viiny ta prohnozy transformatsii rynku [Energy security of Ukraine and the world]. *Ekonomika, upravlinnia ta administruvannia,* no. 2 (112), pp. 46–53. DOI: https://doi.org/10.26642/ema-2025-2(112)-46-53

7. Winzer, C. (2012). Conceptualizing energy security. *Energy Policy,* no. 46, pp. 36–48.

8. Chychkalo-Kondratska, I. B. (2026). Instytutsiini transformatsii enerhetychnoho sektoru v umovakh yevrointehratsii: bezpekovyi pidkhid [Institutional transformations of the energy sector in the context of European integration: a security approach]. *Efektyvna ekonomika*, no. (3). DOI: https://doi.org/10.32702/2307-2105.2026.3.15

9. Jasiūnas, J., Lund, P. D., & Mikkola, J. (2021). Energy system resilience – A review. *Renewable and Sustainable Energy Reviews,* no. 150, 111476. DOI: https://doi.org/10.1016/j.rser.2021.111476

10. Langer, L., Skopik, F., Smith, P., & Kammerstetter, M. (2016). From old to new: assessing cybersecurity risks for the evolving intelligent network. *Computers & Security,* no. 62, pp. 165–176. DOI: https://doi.org/10.1016/j.cose.2016.07.008

11. Leshchyna, R. (2018). Cybersecurity and privacy in standards for intelligent networks – a comprehensive survey. *Computer Standards & Interfaces,* no. 56, pp. 62–73. DOI: https://doi.org/10.1016/j.csi.2017.09.005

12. Song, C. K., Han, A., & Liu, C. K. (2018). Power grid cybersecurity: state-of-the-art. *International Journal of Electrical Power & Energy Systems,* no. 99, pp. 45–56. DOI: https://doi.org/10.1016/j.ijepes.2017.12.020

13. Wang, W., & Lu, Z. (2018). Cybersecurity in the smart grid: a review and challenges. *Computers & Electrical Engineering,* no. 67, pp. 469–482. DOI: https://doi.org/10.1016/j.compeleceng.2018.01.015

14. Eder-Neuhauser, P., Zseby, T., Fabini, J., & Vormayr, G. (2017). Cyberattack models for smart grid environments. *Sustainable Energy, Grids and Networks,* no. 12, pp. 10–29. DOI: https://doi.org/10.1016/j.segan.2017.08.002

15. Cloppenburg, S., & Bokelo, M. (2019). Digital platforms and the future of energy supply: promises and dangers for the next stage of the energy transition. *Energy Research & Social Science,* no. 49, pp. 68–73. DOI: https://doi.org/10.1016/j.erss.2018.10.016

16. Hagen, J. (2018). Developing Cyber Resilience in the Energy Sector. *International Journal of Critical Infrastructure Protection,* no. 20, pp. 26–27. DOI: https://doi.org/10.1016/j.ijcip.2017.11.003

17. Venkatachary, S. K., Prasad, J., Alagappan, A., Andrews, L. J. B., Raj, R. A., & Duraisamy, S. (2024). Cybersecurity and cyber-terrorism challenges to energy-related infrastructures. Cybersecurity frameworks and economics. Comprehensive review. *International Journal of Critical Infrastructure Protection,* no. 45, 100677. DOI: https://doi.org/10.1016/j.ijcip.2024.100677

УДК 620.9:005.332.5]:004.89:338.246.8
JEL H56; O32

Чичкало-Кондрацька Ірина Борисівна, доктор економічних наук, професор, завідувач кафедри міжнародних економічних відносин та туризму, Національний університет «Полтавська політехніка імені Юрія Кондратюка». **Цифровізація енергетичного сектору: кіберризики, вразливості розумних мереж та механізми захисту енергетичної безпеки держави.**

Обґрунтовано, що, не дивлячись на різноманітність підходів, спільною концепцією, яка лежить в основі більшості визначень енергетичної безпеки, є відсутність, захист або адаптивність до загроз, що спричинені чи впливають на ланцюг постачання енергії. У статті розглянуто вплив цифровізації енергетичного сектору та кіберзагроз на енергетичну безпеку. Виділено відмінності розумних енергетичних мереж та узагальнено загрози кібербезпеці енергетичного сектору. Розглянуто потенційні наслідки та економічний вплив кібератак на енергетичний сектор, що може призвести до фінансових втрат, шкоди навколишньому середовищу та навіть мати каскадний вплив на інші сектори, оскільки він відіграє вирішальну роль в економіці багатьох країн. Узагальнено запобіжні заходи та захисні механізми кібербезпеки, які охоплюють людей, програмне забезпечення, фізичну інфраструктуру та архітектуру енергетичної системи.

Ключові слова: енергетична безпека, цифровізація, енергетичний сектор, нафтогазовий сектор, розумні мережі, кібербезпека, державне регулювання, цифрові технології, кіберризики, критична інфраструктура, кіберзагрози.

UDC 620.9:005.332.5]:004.89:338.246.8
JEL H56; O32

Iryna Chychkalo-Kondratska, Doctor of Economic Sciences, Professor, Head of the Department of International Economic Relations and Tourism, National University "Yuri Kondratyuk Poltava Polytechnic". **Digitalization of the energy sector: cyber risks, vulnerabilities of smart grids and mechanisms to protect the energy security of the state.**

It is argued that the common concept underlying most definitions of energy security is the absence of, protection from, or adaptability to threats that arise from or affect the energy supply chain. The relevant types of threats change along with the change of systems. The article examines the impact of digitalization of the energy sector and cyber threats on energy security. The growing use of information technologies in the energy sector, including energy networks, oil and gas pipelines, and other critical infrastructure, has made this sector more vulnerable to cyber attacks. The differences of smart energy networks are highlighted and cybersecurity threats to the energy sector are summarized. Cyberterrorism poses a significant risk to the energy sector and requires careful attention and management to ensure the safe and reliable operation of energy infrastructure. The article provides an overview of cyber threats. The energy sector faces cybersecurity risks caused by both syntactic and semantic attacks. But, on the other hand, thanks to digitalization, the system efficiency and resilience to traditional persistent threats and threats of technical failures are increased. The potential consequences and economic impact of cyberattacks on the energy sector are considered, which can lead to financial losses, environmental damage and even human deaths. Cyberattacks on the energy sector can also have a cascading effect on other sectors, as the energy sector plays a crucial role in the economies of many countries. Cybersecurity precautions and defense mechanisms are summarized, covering people, software, physical infrastructure and architecture of the energy system. Ensuring energy security requires that the energy sector remain vigilant in the face of evolving cyber threats and continue to develop and implement effective risk management strategies to protect against cyberterrorism.

Key words: energy security, digitalization, energy sector, oil and gas, smart grids, cybersecurity, government regulation, digital technologies, cyber risks, critical infrastructure, cyber threats.