УДК 338.27+351.824.11
JEL L86 Q55 I28 O35

БЕЗПЕКОВІ АСПЕКТИ ПЕРЕХОДУ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ ДО ВИСОКОТЕХНОЛОГІЧНОГО ЕКОНОМІЧНОГО РОЗВИТКУ

Олійник Даниїла Іллівна,
доктор економічних наук, професор

Обґрунтовано перехід суб'єктів господарювання до високотехнологічного економічного розвитку на основі промислового Інтернету речей, який розглядається як об'єднана екосистема розумних машин, цифрових систем та людей, здатних провадити виробничі операції на новому інтелектуальному рівні. Доведено, що такий перехід спрямований у першу чергу на забезпечення надійного захисту від мережевих атак і прискорення трансформаційних можливостей безпеки, інтелекту та бездротового з'єднання за допомогою апаратного забезпечення цілісності пристроїв на основі зв'язку *5G* як нової інтелектуальної мережі для промислових об'єктів. Це підтверджує розвиток і поширення технологій, заявлених у доктрині *Industry* 4.0, та виникнення нового класу кіберфізичних промислових систем управління Інтернетом з особливостями інформаційної та функціональної безпеки. На прикладі побудови новітньої архітектури «розумної» мережі доведено, що найбільш ефективним способом задоволення соціальних вимог та забезпечення системи безпеки, експлуатації, екологічного захисту, вартості постачання та енергоефективності суб'єктів господарювання є використання інноваційних рішень і технологій при з'єднанні з новітньою архітектурою інтелектуальних мереж. Зроблено висновок про те, що суб'єктам господарювання необхідно здійснювати відповідні заходи інституційного та організаційного характеру щодо моделювання майбутнього розвитку на основі апробованих міжнародною практикою сценарних досліджень формування сучасної інноваційної мережевої інфраструктури, яка змінює динаміку виробництва енергії та починає трансформувати енергетичну мережу в *3Ds*-систему – набагато краще оцифровану, декарбонізовану та децентралізовану.

***Ключові слова*:** геоінформаційні платформи, децентралізація, декарбонізація, Інтернет енергія, інформаційні технології, кіберфізичні промислові системи, мережева інфраструктура, національні інноваційні системи, суб'єкти господарювання, промисловий Інтернет речей, цифровізація.

Oliinyk Danyila

SAFETY ASPECTS OF TRANSITION OF SUBJECTS OF ECONOMIC DEVELOPMENT TO HIGH-TECHNOLOGICAL ECONOMIC DEVELOPMENT

The transition of business entities to high-tech economic development on the basis of the industrial Internet of things is substantiated, which is considered as a united ecosystem of intelligent machines, digital systems and people capable of conducting production operations at a new intellectual level. It is proved that such a transition is primarily aimed at providing reliable protection against network attacks and accelerating the transformational capabilities of security, intelligence and wireless connectivity by hardware integrity of devices based on 5G communications as a new intellectual network for industrial applications. Objects confirming the development and spread of the technologies stated in the Industry 4.0 doctrine and the emergence of a new class of cyber-physical industrial Internet management systems with features

of informational and functional Copyrights security. On the example of constructing the latest architecture of the "smart" network, it has been proved that the most effective way to meet social requirements and to provide security, exploitation, environmental protection, and cost of supply and energy efficiency of business entities is to use innovative solutions and technologies when connected with the latest architecture of intellectual networks. The conclusion is made on the necessity for the business entities to take appropriate institutional and organizational measures regarding the modeling of future development on the basis of international practice tested scenario studies of the formation of a modern innovation network infrastructure that changes the dynamics of energy production and begins to transform the power grid into a 3Ds system – more digitized, decarbonated and decentralized.

Keywords: geoinformation platforms, decentralization, decarbonisation, Internet energy, information technology, cyber-physical industrial systems, network infrastructure, national innovation systems, busines sentities, industrial Internet ofthings, digitalization.

Постановка проблеми. Формування постіндустріального суспільства зумовило нові виклики економічного розвитку проблем, в основі яких лежить побудова інтелектуальних мереж, а саме: дотримання екологічних норм; забезпечення вищого рівня життя населення; посилення безпеки; запровадження нових моделей власності, як-от кооперативи та інноваційні підприємства; посилення корпоративного управління, спрямованого на довгострокову перспективу; здійснення децентралізації; забезпечення активної участі громадян. Розгортання мережевої інтелектуальної інфраструктури насамперед стосується цифрової трансформації електроенергетики, що є частиною цифрової економіки та спрямована на підвищення надійності та ефективності функціонування енергосистеми шляхом упровадження ризик-орієнтованого управління на базі цифрових технологій. Крім того, факторами ризику у сфері електроенергетики є спрямування на децентралізацію та цифровізацію, а також стійкість енергосистеми як проблема державної політики.

Світовий досвід переконує, що на функціонування суб'єктів господарювання істотно впливають поточна трансформація електроенергетики та розвиток децентралізованої генерації, зберігання, інтелектуальних мереж та активної участі споживачів з одночасним упровадженням внутрішнього енергетичного ринку. Оцифрування промислового сектору є однією з основних опор економічного розвитку країн. Однак залежно від своєчасності реагування на світові виклики цифровізації можуть виникати можливості потенційного розвитку або загроз. Складність, з якою суб'єкти господарювання нині зіштовхнулися, полягає в єдиному розумінні конкретики щодо питань інтеграції до цифрових мереж, які забезпечили б реалізацію цифровізації об'єктів мережевої інфраструктури, а також уможливили б адекватну оцінку ресурсів, необхідних для високотехнологічного економічного розвитку [1].

Ключовим елементом цифровізації суб'єктів господарювання виступає узгоджена діяльність всіх заінтересованих сторін у впровадженні цифрових технологій та цифрових промислових платформ через створення ланцюгів вартості. Найкращою енергетичною політикою для управління таким переходом є баланс між безпекою, доступністю та стійкістю, який отримав назву «енергетична трилема». Відтак його дотримання вимагає зміни філософії для забезпечення сталого переходу. Прикладами формування промислових галузей наступного покоління для *вертикальних секторів* у ЄС слугують цифрові платформи з'єднаних «розумних» фабрик (*Connected Smart Factories*), «розумного» сільського господарства та «розумної» цифрової трансформації охорони здоров'я, а для *горизонтальних* – промислові інформаційні платформи та Інтернет речей (*Internet of Things, IoT*). Забезпечення переходу суб'єктів господарювання до високотехнологічного економічного розвитку й цифрової трансформації, у т. ч. із вдосконаленням ринкового дизайну, що супроводжується відповідним розвитком інфраструктури, потребує переосмислення та теоретико-методологічного оновлення, у якому було б взято до уваги сучасні трансформаційні процеси розгортання інтелектуальної мережевої інфраструктури. Саме цим зумовлена **актуальність** питань, які висвітлюються у статті.

[1] *Довідково.* Високотехнологічний економічний розвиток у цій статті розглядається відповідно до високотехнологічної класифікації технологій та інновацій виробничих галузей на основі статистичної класифікації господарської діяльності (*NACE Rev.2*) Євростату, що описує виробничі та службові операції.

Аналіз останніх досліджень та публікацій. Теоретичні й практичні аспекти розгортання інтелектуальної мережевої інфраструктури та її вплив на економічний розвиток здебільшого розроблені в працях Т. Боуена, М. Сігала, Е. Хупера, Д. Чея. Проблемам розробки технологій інтелектуальних мереж, стандартів та їх еволюції присвячені роботи Т. Магеданца, Р. Попеску-Зелетина, М. Сірла, К. Соломодіса та інших учених. Вагомий внесок у дослідження проблем майбутнього розвитку інтелектуальної мережевої інфраструктури та нової європейської ініціативи щодо безпеки зробили такі вчені, як С. Деннісон, Г. Маскарих, В. Мое, Г. Мунсон, Л. Рапнуїл, У. Франке, С. Фішель та ін.

Метою статті є проведення аналізу сучасних європейських тенденцій та оновленої парадигми перспективного високотехнологічного розвитку інтелектуальних мереж, щоб знайти шляхи подолання розриву, який існує між суб'єктами господарювання при переході на нові моделі виробництва та споживання в цифрових енергетичних системах, а також визначення ролі та значення в цьому процесі окремих ризикових та безпекових аспектів створення відповідної мережевої інфраструктури.

Виклад основного матеріалу дослідження. Світ нині переходить до нової ери цифрової глобалізації, до більш цілісних перетворень, від цифрових продуктів та інфраструктури до цифрового розподілу та веб-стратегій, які засновані на цифровій технології самоконтролю, аналізу та звітування (*Self Monitoring Analysis and Reporting Technology*) у мережевій інфраструктурі. У розвинених країнах управління промисловістю здійснюється за допомогою цифрових технологій, Інтернету енергії, систем доповненої реальності, штучного інтелекту (*Artificial Intelligence, AI*), розпізнавання голосу, віртуальної реальності (*Virtual Reality, VR*) тощо.

У міжнародній практиці проактивне управління інноваціями є основним рушієм стабільної довгострокової конкурентоспроможності економіки держав. Воно включає всі фази: від візуалізації контекстного сценарію до реалізації конкретних бізнес-моделей і вимагає системного підходу до інтеграції суб'єктів господарювання у задекларований світовою спільнотою екосистемний простір у тих галузях, де існує потенціал для створення нових ринків на основі Інтернету речей та економіки спільного споживання, що функціонують як нові економічні геополітичні формування інтеграції різноманітних складних технологій. Ці технології з'єднані в національні інноваційні системи (*National System of Innovation*, *NSI*), а в планетарному масштабі – у мережеву інфраструктуру на основі цифрових активів.

Модернізація мережевої інфраструктури на основі стійких енергетичних систем відповідно до національних обставин, потреб та пріоритетів, з урахуванням міжнародних зобов'язань щодо пом'якшення наслідків зміни клімату та досягнення цілей сталого розвитку сприяє припливу значних інвестицій і є важливим напрямом у моделюванні економічного розвитку на основі апробованих міжнародною практикою сценарних досліджень формування сучасної інноваційної мережевої інфраструктури, яка змінює динаміку виробництва та починає трансформувати енергетичну мережу в *3Ds*-систему – оцифровану, декарбонізовану та децентралізовану (*Digitization, Decarbonization and Decentralization*) на значно вищому рівні. Нинішні та майбутні ініціативи в межах ринку цифрових технологій стосуються перш за все кібербезпеки, формату *5G*, регуляторних норм для досягнення цілей сталого розвитку з урахуванням специфіки національного розвитку.

Високотехнологічний економічний розвиток XXI ст. нині формують дві технологічні революції: розвиток Інтернету та перехід до глобальної енергетичної системи, що не містить вуглецю. У цій децентралізованій системі інноваційні технології стають все більш важливими в мережевій інфраструктурі, виступають центральними елементами сучасної енергетичної революції у промисловості та є ключовим елементом нової інфраструктури, яка змінює динаміку виробництва енергії та трансформує енергетичну мережу в *3Ds*-систему. З розвитком інноваційних технологій і високотехнологічних можливостей мережевої інфраструктури зростають і ризики, які суттєво впливають на суб'єкти господарювання.

Необхідність запровадження цілісного системного підходу до цифрових перетворень у промисловості нині зумовлюється використанням можливостей, що виникають із початком Четвертої промислової революції. Про це свідчить і впровадження у ЄС законодавства, яке передбачає регуляторне середовище для забезпечення електронної взаємодії на внутрішньому ринку між підприємствами, громадянами та державними органами [16]. *Європейська стратегія інтелектуального, сталого та інклюзивного розвитку до 2020 року* [13] *декларує реалізацію своїх*

цілей як спільний інтерес *на основі трьох взаємодоповнюючих пріоритетів* економічної політики*:*

- «розумного» зростання: розвиток економіки на основі знань та інновацій;
- сталого розвитку: сприяння більш ресурсозберігальній, зеленій та конкурентоспроможній економіці;
- інклюзивного зростання: стимулювання економіки зайнятості населення, забезпечення соціальної і територіальної єдності.

Зазначені пріоритети реалізуються через проголошені у ЄС ініціативи щодо клімату, енергії та мобільності (ефективне використання ресурсів); цифрового суспільства; інновацій (поліпшення рамкових угод та доступу до фінансування досліджень); зайнятості та навичок; освіти; конкурентоспроможності та боротьби з бідністю, де промислове виробництво та взаємодія з послугами відіграють провідну роль у відновленні економіки. Планування такої системи у *3D*-форматі потребує системних інфраструктурних рішень для сталого економічного й соціального розвитку та розбудови інфраструктурних мереж на основі поширення для споживачів програмних продуктів як послуг (*Software-as-a-Service, SaaS*).

Однак, як засвідчив досвід, оцифрування промислового виробництва формує нові виклики, що пов'язані з даними, створеними безліччю нових інтелектуальних продуктів та взаємодією між людьми й розумними пристроями, і вимагає встановлення балансу між законними бізнес-інтересами та основними правами, що забезпечують захист персональних даних і конфіденційність.

Прийнятий у 1991 р. закон Нанна–Лугара було покладено в основу програми спільного зменшення загроз і допомоги країнам, які мали у своєму розпорядженні ядерну зброю, – Білорусі, Україні та Казахстану. Однак світ упродовж наступних років не став більш безпечним, а ймовірність загроз в Україні через кібервтручання в системи управління, війни через ескалацію напруженості між США та Росією – зросла багатократно. І, звичайно ж, підвищилися небезпека тероризму, ймовірності загроз щодо управління системами промислового виробництва. Програмно-апаратні та інші технічні й технологічні засоби, які є складниками мережевої інфраструктури, є вразливими до кібератак, що спричиняє порушення надійного та стійкого режиму функціонування технологічних систем, а також погіршення енергоспоживання.

Експерти з безпеки характеризують кібератаки як форми асиметричної війни, що еквівалентні знищенню суспільства шляхом відмови від постачання продуктів харчування та води. Тим часом в Україні один інцидент за іншим підкреслює нагальність заходів щодо кібербезпеки. Так, у грудні 2015 р. атака на енергосистему довела вразливість суб'єктів господарювання не лише в нашій країні, а й у розвинених країнах світу. У грудні 2016 р. вітчизняна мережа знову була атакована складною кіберзброєю «*Crash Override*», яка, імовірно, може бути модифікована з метою ураження широкого спектра промислових об'єктів у всьому світі. За повідомленням Департаменту внутрішньої безпеки США, через місяць Україна пережила іншу кібератаку, основу якої становили маніпулювання тональними кодами та скоординоване віддалене кібервтручання хакерських угруповань. Однак великі розподілені системи спостереження та керування (*Supervisory Control and Data Acquisition, SCADA*), які використовуються впродовж останніх десятиліть, на сучасному етапі не розраховані на розпізнання кібератак.

З метою формування заходів безпеки існуючих систем військовими відомствами США впроваджено демонстраційний проект надійності та безпеки для інтелектуальної енергетичної інфраструктури (*Smart Power Infrastructure Demonstration for Energy Reliability and Security, SPIDERS*), який широко використовується як у промисловості, так і органами виконавчої влади, місцевого самоврядування на основі аналізу статичного коду виявлення та усунення завад [18]. Виступаючи в лондонському дослідницькому центрі «*Policy Exchange*», радник президента з національної безпеки США Герберт Макмастер заявив, що головними загрозами, на думку Білого дому, є «ревізіоністські» сили, такі, як Росія та Китай, які намагаються підірвати глобальний порядок і стабільність» [4]. Кібератака на Україну в 2017 р., відома як *NotPetya*, була частиною зусиль РФ щодо дестабілізації нашої країни та порушення договору європейської безпеки від 1997 р. [2].

Згідно з результатами останнього дослідження загроз, оприлюдненого підрозділом «*Forti Guard Labs*» американської транснаціональної корпорації *Fortinet*, у 2017 р. кількість загроз у глобальному, регіональному та секторальному вимірах не тільки значно зросла кількісно, а й поширилися завдяки масованим атакам на екс-

плойт-додатки, програмне забезпечення та ботнети. Метою зростання активності експлойтів є порушення саме системи контролю за виробничими процесами (*Industrial Control System*, *ICS*) та інструментальних систем безпеки з використанням нових *IoT-ботнетів*, наприклад *Reaper* та *Hajime*, які здатні одночасно вражати декілька промислових об'єктів.

Концепція інноваційних перетворень «розумних» мереж (*Smart Grid*) передбачає побудову інтегрованої, саморегулівної та самовідтворювальної системи на основі мережевої топології. Планування такої системи в *3D*-форматі потребує наборів мікросхем для підтримки нової бізнес-моделі та системних інфраструктурних рішень для великих підприємств, виробників хмарних технологій та користувачів у створенні та управлінні величезною кількістю підключених *4G*-пристроїв (а швидше, *5G*) у надійному та масштабованому вигляді.

Визначення *Smart Grid* у широкому розумінні стосується сімейства взаємопов'язаних технологій, які використовують широкий спектр датчиків та джерел даних для збирання інформації про роботу електричної мережі щодо зондування та моніторингу, координації та управління технологіями. Процес створення «розумної» системи переважно розглядається як інтеграція інформаційно-комунікаційних технологій (*Information Technology*, *IT*) в енергетичну інфраструктуру.

Більш достовірне трактування інтелектуальної мережі полягає в тому, що, як концепція і як соціотехнічна система, вона перебуває на ранній стадії розвитку, і, отже, її визначення може стабілізуватися лише тоді, коли система буде стандартизована для конкретних цілей. В інтелектуальну енергетичну систему залучено нині різні суб'єкти господарювання, одні з яких виконують чисто технологічну роль, а інші – гібридні, або ринкові ролі. Суб'єкти господарювання, які мають інтерес до ринку, включають постачальників, операторів системи передачі (*Transmission System Operator, TSOs*) та системи розподілу (*Distribution System Operator, DSOs*), споживачів, уряд, регуляторів, аналітичні центри тощо і формують простір для діяльності нових підприємств та організацій на новій інноваційній платформі. Підприємства, що розвиваються на базовій технології *Smart Grids*, варіюються від великих інфраструктурних компаній, таких як *GE* та *Siemens*, спеціалістів виробників «розумних» вимірювальних приладів (*Elster, Landys + Gyr*) та інших до малих стартапів, якот *Smarter Grid Solutions.*

Створення й адаптація цифрових промислових платформ до ринкових реалій має важливе значення для забезпечення необхідного масштабу та охоплення національних і регіональних ініціатив щодо оцифрування промисловості та ініціатив суб'єктів господарювання. При цьому у ЄС, наприклад, з одного боку, ініціативи з побудови цифрових промислових платформ майбутнього спрямовані на об'єднання цифрових технологій, зокрема великих даних і хмарних обчислень, автономних систем, штучного інтелекту й *3D*-друку в інтеграційні платформи, що вирішують міжгалузеві проблеми, а з другого – на інтеграцію конвергентних цифрових інновацій у такі галузеві платформи, як інвестиції у фабрики майбутнього (*Factories of the Future*, *FoF*), сталого розвитку промисловості за рахунок використання ресурсів та енергоефективності (*Sustainable Process Industries through Resource and Energy, SPIRE*) та біологічні галузі (*Bio-based Industries, BBI*). У зазначеному контексті *ініціатива оцифрування європейської промисловості* (*Digitizing European Industry*, *DEI*) спрямована на об'єднання зусиль спільних інтересів на економічній платформі («*Platform Economy*») та забезпечення майбутніх *глобальних стандартів* для підключення «розумних» підприємств (*Connected Smart Factory*) і передбачає інвестування цифрових інноваційних можливостей на основі стандартів інформаційно-комунікаційних технологій та адаптацію робочої сили шляхом підготовки людського капіталу для набуття необхідних навичок для цифрових перетворень.

З метою надійного забезпечення, підключення та управління довгими життєвими циклами мільярдів інтелектуальних пристроїв через їхні хмарні платформи вже нині світовими компаніями, наприклад, *Qualcomm* (*NASDAQ QCOM*), *Ericsson*, *Telstra*, *Netgear* та іншими, розроблені абсолютно нові набори послуг програмного забезпечення на відповідність вимогам нових виробників та клієнтів промислового Інтернету речей (*Industrial IoT*, *IIoT*) [15]. Такі набори послуг переважно спрямовані на забезпечення надійного захисту від мережевих атак та прискорення трансформаційних можливостей безпеки, інтелекту та бездротового з'єднання за допомогою апаратного забезпечення цілісності пристроїв для широкого спектра інноваційних додатків *IoT* на основі зв'язку *5G*, який стане не лише новим поколінням, а й новою мережею. Саме вона об'єднає нові галузі, і в ній надаватимуться нові послуги та розширюватимуться нові можливості для користувачів, а також формуватимуться нові ринки вартості та енергоефективності.

Основною проблемою, яка потребує підвищення довіри до продуктів та послуг *IoT*, розміщених на ринку, є розширення обміну та співпраці з міжнародними й регіональними організаціями, промисловістю на основі уніфікованих стандартів у таких ключових сферах, як *Smart City*, *Smart Grid*, *IoT*, кібербезпека, штучний інтелект, розпізнавання голосу, віртуальна реальність та цифровізація в цілому. Різноманітність технологій, котрі пов'язані з великомасштабною мережевою інфраструктурою, вимагають вертикального підходу до стандартизації, починаючи з архітектури, дорожніх карт, планування та організації діяльності системи в таких секторах, як електроенергетика, охорона навколишнього середовища, безпека для систем і процесів оцінки відповідності.

Оперативна сумісність є важливою для розгортання *IoT* та безперешкодного потоку даних у різних секторах і регіонах. Однак, як зазначалось, поточна фрагментація платформ *IoT* створює проблеми, які потребують адресної взаємодії між комерційними або некомерційними платформами, наприклад, зосереджуючись на семантиці та онтології, і вимагає співпраці на загальних інтерфейсах. Широкомасштабні пілотні проекти допомагають перевірити чинні стандарти та підтримувати діяльність із стандартизації на міжнародному рівні. До прикладу, глобальні ініціативи із стандартизації міжмашинної взаємодії та *IoT* (*Standards for M2M and the Internet of Things*, *oneM2M*) або з розробки та впровадження технологічних стандартів для Всесвітньої мережі (*World Wide Web Consortium*, *W3C*) у випадку визначення семантичної сумісності, особливо коли це стосується конвергенції чинних стандартів, а не створення нових платформ і нових стандартів *IoT*.

Відкриті стандарти із справедливими, обґрунтованими й недискримінаційними економічними та правовими умовами (*Fair*, *Reasonable and Non-Discriminatory*, *FRAND*) є необхідними для надання суб'єктам господарювання доступу до нових технологій і нових способів ведення бізнесу. Крім того, вони слугують ключовими елементами платформ. Потреба в їхньому застосуванні полягає в тому, щоб забезпечити сумісні рішення для глобальної ініціативи щодо стандартів, таких як *oneM2M*, *W3C* та ін., що охоплюють вимоги, архітектуру, специфікації різнотипного програмного забезпечення (*Application Programming Interface*, *API*), безпеку та сумісність технологій міжмашинної взаємодії (*M2M)* та *IoT* і формують основу для підтримки додатків та послуг, як-от: інтелектуальна мережа, підключена машина, домашня автоматизація, громадська безпека, здоров'я тощо. Стандартизація цифрових технологій має вирішальне значення для оцифрування промисловості та є ключовим аспектом для функціонування єдиного ринку цифрових технологій, які дозволяють пристроям і службам спілкуватися між кордонами й технологіями.

У Стратегії єдиного цифрового європейського ринку передбачені заходи, спрямовані на покращення стандартного встановлення технологій *IKT*, зокрема щодо п'яти пріоритетних напрямів – *5G*, *Cloud Computing*, *Internet of Things*, технології передачі даних та кібербезпеки. Цей стратегічний курс підтримується регулярним моніторингом, тривалим політичним діалогом з усіма зацікавленими сторонами, поглибленою співпрацею з організаціями стандартизації та зміцненням міжнародної участі. Окрім того, стандартизація *IKT* спирається на збалансовану політику захисту прав інтелектуальної власності для доступу до основних стандартних патентів (*Standard-Essential Patent*, *SEPs*) на основі чесних, розумних та недискримінаційних умов [6].

У світовій практиці ініціативу щодо запровадження системного підходу в електроенергетиці та електроніці на основі міжнародних стандартів узяла на себе Міжнародна електротехнічна комісія (*International Electrotechnical Commission*, *IEC*), у структурі якої функціонують групи з оцінювання систем «розумних» енергетичних мереж (*Smartenergygrids*, *SEGs*), системні комітети з електротехнічних аспектів «розумних» міст (*Electrotechnical Aspects of Smart Cities*, *SyC*), групи системних ресурсів (*Systems Resource Group*), роботу яких забезпечує секретаріат *ISO/IEC JTC 1/SC 41,* Інтернет речей та суміжних технологій (*Internet of Things and Related Technologies*). Окрім того, *IEC* запровадила унікальний стандартизований підхід до тестування та сертифікації обладнання для застосування поновлюваних джерел енергії (*IEC System for Certification to Standards Relating to Equipment for Usein Renewable Energy Applications, IECRE*), у т. ч. пов'язаних із кібербезпекою в секторі промислової автоматизації. Всесвітня система сертифікації *IEC* (*IEC Quality Assessment System for Electronic Components*, *IECQ*) використовує специфікації оцінки якості системи електронних компонентів *IEC*, допомагає забезпечити безпеку та надійність багатьох компонентів, що є невід'ємною частиною *IoT* та розумних пристроїв [14]. Наприклад, асоціація груп телекомунікаційних компаній (*Generation Partnership Project*, *3GPP*), головною метою якої є розроб-

лення та затвердження стандартів для мережевих технологій, архітектури мереж та сервісів, у 2018 р. оголосила про чергову комунікаційну революцію, завершивши розробку першої серії радіостандарту п'ятого покоління – *5G NR*.

На цьому етапі формування децентралізованих розподілених систем та розробки платформ, які покликані забезпечити нові форми участі споживачів, для України надзвичайно важливим є саме формування власної концептуальної та логічної інноваційної моделі промислового розвитку. Відповідно модель життєвого циклу такої системи повинна включати розробку концептуальних підходів, вимог із безпеки (*Safety Requirements Specification*, *SRS*), архітектурних проектів системи (*System Architecture Design*, *SAD*), апаратних засобів (*Hardware Design*, *HD*) та кодів програмного забезпечення (*Software Coding*). Оригінальність концептуальних підходів полягатиме у побудові платформи стандартизованої сумісності роботи телекомунікаційної індустрії на основі відкритого коду (*Open Source*) для розробки якісних послуг з високою пропускною спроможністю та низькою затримкою мережевих функцій віртуалізації (*Network Functions Virtualization*, *NFV*). У деякому сенсі така концепція звучить дещо утопічно, однак розробка такої глобальної розподіленої архітектури, яка здатна підключати хмарні сервіси та пристрої, уже сьогодні активно впроваджується на основі сучасних технологій компаніями *MWC 2107*, *Ericsson* та *Intel* [5]. Крім того, некомерційною організацією *Media Development Investment Fund* здійснено запуск супутників у тестовому режимі, втілюється в життя проект Ілона Маска «*Starlink*» зі створення «Глобального широкосмугового зв'язку». Усе це – реальні кроки щодо забезпечення доступу до бездротового Інтернету мешканцям усієї планети [17].

Відповідно до опублікованого Міжнародним інститутом управлінського розвитку (*International Institute for Management Development*, *IMD*) рейтингу конкурентоспроможності країн *IMD* – 2017 [10] Україна в глобальному та цифровому рейтингу посіла 60-те місце. Проте в рейтингу цифрової конкурентоспроможності щодо впровадження та вивчення цифрових технологій, котрі зумовлюють трансформації в урядовій практиці, бізнес-моделях та суспільстві в цілому, Україна перебуває на останніх позиціях поряд з Індонезією, Монголією, Перу та Венесуелою. Наприкінці 2017 р. Уряд схвалив Концепцію розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердив план заходів щодо її реалізації [3]. Основною метою Концепції є реалізація «Цифрового порядку денного України 2020» (цифрова стратегія) для усунення бар'єрів на шляху цифрової трансформації України у найбільш перспективних сферах [1]. Однак про результати подолання цифрової нерівності, розбудови інноваційної інфраструктури країни, цифрових перетворень і формування умов для підприємств та бізнесу говорити ще зарано. На тлі зростаючих зовнішніх загроз кібервтручання в управління енергетичною системою, її стійкість, а також ядерна безпека, кібербезпека, блокчейн, високошвидкісний Інтернет, он-лайн розрахунки тощо розглядаються суб'єктами господарювання як складові світової інтелектуальної енергетичної системи, де одним із пріоритетних напрямів розвитку в новій промисловій стратегії є місцеві системи інтелектуальної енергетики.

Зближення різних технологій приводить до цифрових змін, зокрема використовуються *IoT*, великі дані, хмарні обчислення, робототехніка, штучний інтелект і *3D*-друк, що допомагає промисловості реагувати на основні прагнення сучасних клієнтів: персоналізація, підвищення безпеки та комфорту, а також енергоефективність та збереження ресурсів. Платформи промислового *IoT*, широкомасштабні пілотні проекти й тест-майданчики, які впроваджуються нині у ЄС (*див. Додаток, с. 98*), визнані нині найкращими практиками в промисловому середовищі і виконують роль платформи з активації додатків (*Platform Activation Applications*, *AEP*). Яскравим прикладом цифрової платформи з'єднаних підприємств на сьогодні є платформа розумного, безпечного захисту (*Smart*, *Safe & Secure*, *S3P*) *«Nouvelle France Industrielle»*, розроблена за підтримки французького уряду та спрямована на забезпечення швидкого розвитку та експлуатації пристроїв і прикладних програм, що підтримують *IoT* безпеку, оперативність та портативність промислового виробництва [11].

Такі інновації стають основою тіснішої взаємозалежності між прогресом цифрових технологій та їх використанням у різних галузях і потребують створення високоінноваційних цифрових секторів та оновлення цифрової інноваційної спроможності всіх галузей. З цією метою для використання можливостей, що пропонуються в галузі цифрових інновацій, у Європі було запущено кілька національних та регіональних ініціатив, таких як *Industrie 4.0* (*DE*), *Smart Industry* (*NL*), *Catapults* (*UK*) та *Industrie du Futur* (*FR*) [8]. Так, наприклад, для *Industrie 4.0* у Німеччині створена модель довідкової архітектури для промисловості (*Reference Architectural*

Model Industrie 4.0, *RAMI 4.0*) на основі стандарту *IEC 62264* щодо інтеграції систем управління підприємствами, яка сприяє розумінню того, які стандарти необхідні для впровадження *Industry 4.0*. Зокрема, стандарт *IEC 62264* [12] деталізує такі моделі: об'єктів та атрибутів виробничих операцій; інтеграції та управління виробничими операціями; обслуговування повідомлень та бізнесу тощо. Окрім того, асоціація *ProSTEPiViP* у Німеччині розробила каталог критеріїв сумісності інфраструктури, інтерфейсів, стандартів, архітектур тощо (*Product Life Cycle Management*, *PLM*) у вигляді кодексу відкритості управління життєвим циклом продукту (*Code for PLM Openness*, *CPO*) [7].

Прикладами національних та регіональних програм покращення оцифрування промислового виробництва можуть слугувати ініціативи, започатковані в різних країнах: «*Produktion 2030*» – у Швеції; «*Industry 4.0*» – в Іспанії; промисловий альянс «*Industrie du Futur*» – у Франції; національний промисловий план «*Italy's National Industrial Plan*» – в Італії та ін. У США оцифрування промисловості значною мірою залежить від великих компаній, таких як *AT&T*, *Cisco*, *IBM*, *GE* та *Intel,* які зосереджуються у конкретних галузях застосування на тестових сейфах, на відміну від більш загальних стандартів налаштування. Виробничі компанії Китаю теж демонструють зацікавленість у цифровізації підприємств, однак увагу зосереджують на іншому підході, покладаючись на прямі інвестиції у європейські компанії, серед них, зокрема, такі: *Krauss-Maffei*, *Stoll*, *ManzGroup*, *Kuka*, які мають для КНР вагоме значення. Рівень інвестицій Китаю у відповідних технологіях перевищує рівень інвестицій у ЄС. Поширеною є програма «Зроблено в Китаї 2025» («*Made in China 2025*»), яка вважається китайським еквівалентом *Industry 4.0*, та *Internet Plus* (*IP*).

З метою впровадження та реалізації ініціативи оцифрування промисловості системи управління промисловим виробництвом в Україні у процесі трансформації мають бути націлені, перш за все, на розробку механізмів адаптації господарської системи країни до загальноєвропейського простору й реалізації проектів, що представляють спільний інтерес (*Projects of Common Interest*, *PCIs*) і вимагають колективних зусиль із залученням громадських та приватних заінтересованих сторін на регіональному та національному рівнях. З цією метою в міжнародній практиці визначені рамки для ідентифікації, планування та реалізації *PCIs* на основі забезпечення єдиної послідовної нормативно-правової бази.

Особливого значення для сприяння великомасштабним інвестиціям в інноваційні сфери має використання проектів спільного європейського інтересу (*Important Projects of Common European Interest*, *IPCEI*) у виробничих потужностях і створення цифрових промислових платформ майбутнього, які вимагають розробки еталонних екосистемних архітектур і стандартизації [9]. При цьому одна група ініціатив з побудови платформ має бути спрямована на об'єднання цифрових технологій, зокрема формування інноваційного та технологічного тарифу (*Innovation and Technology Tariff*, *ITT*) великих даних і хмарних обчислень, автономних систем і штучного інтелекту, *3D*-друку, в інтеграційні платформи, що вирішують міжгалузеві проблеми, а друга – на інтеграцію конвергентних цифрових інновацій у такі галузеві платформи, як-от: інвестиції у фабрики майбутнього (*Factories of the Future*, *FoF*), сталий процес промисловості за рахунок ресурсів та енергоефективності (*Sustainable Process Industries through Resource and Energy, SPIRE*) та біологічних галузей (*Bio-based Industries*, *BBI*).

У контексті зазначеного важливими є зусилля урядів, зосереджені на координації національних і регіональних ініціатив з оцифрування промисловості. Однак проблемними нині є питання стосовно стандартизації, регулюючих заходів та інвестицій, які регламентуються рамковими угодами щодо таких ініціатив, як:

- європейська хмарна ініціатива щодо плану побудови високопродуктивних хмарних обчислень інфраструктури даних (віртуальне середовище);
- пріоритети стандартизації *IKT*, які визначають основні стандарти *IKT* для підтримки цифрових інновацій в економіці;
- план дій з електронного урядування;
- підготовка персоналу до роботи з Інтернетом речей.

Цифрові технології фінансового сектору, котрі є підґрунтям «розумних» систем*/IoT* (*Smart System/IoT*), формують інформаційну «розумну» мережеву інфраструктуру на основі технології розподіленої (*Peer-To-Peer*) мережі, що отримала назву *Blockchain*, у якій зберігається інформація про кожну транзакцію. Поєднання інноваційних технологій та новітніх методів капіталізації використання електричної енергії у виробничих процесах нині є *революційним підходом до формування локалізованого енергетичного ринку на основі ексергії термодинамічної*

системи при переході від поточного стану до стану термодинамічної рівноваги.

Упродовж останніх років саме технологія *Blockchain* отримала статус «гейм-чейнджера» як така, що змінює правила гри для інвестування мережевої інфраструктури. У грудні 2017 р. консалтингова компанія *LO3 Energy*, діяльність якої орієнтована на формування нових децентралізованих бізнес-моделей, та європейська енергетична біржа *EPEX Spot* оголосили про впровадження рівноправних енергетичних торговельних і транзакційних систем *Blockchain*. Окреслення такої багаторівневої перспективи (*Multi-Level Perspective*, *MLP*) теоретизує уявлення про технології та фінансові, економічні й політичні тенденції, що сприяють формуванню глобального набору даних про потоки цифрових активів для фінансів нової енергії (*Bloomberg New Energy Finance*, *BNEF*), кращого розуміння взаємозв'язку між різними суб'єктами господарювання та розробки надійних майбутніх сценаріїв.

Висновки та напрями подальших досліджень. Сформована інтегрована модель системи управління інноваційним розвитком підприємств забезпечує синергетичний ефект управління через реалізацію відповідних функцій, а також надає цілісне уявлення про процеси, ресурси, об'єкти (інфраструктуру) інноваційної діяльності, що формують інноваційний базис для розроблення відповідних стратегій розвитку та вдосконалення організаційно-економічних засад інноваційного розвитку суб'єктів господарювання в Україні відповідно до потреб національної економіки, суспільства. Проведений аналіз дозволяє зробити висновок про те, що саме нові моделі бізнесу та оцифрування визначають імпульс на шляху до інноваційного розвитку, який змінює спосіб виробництва та використання енергії в промисловості, та можливість активізації поступальних процесів переходу суб'єктів господарювання до високотехнологічного економічного розвитку через упровадження інновацій, пов'язаних з електрифікацією, децентралізацією та цифровізацією.

У зв'язку з цим виникає необхідність комплексного підходу до формування інноваційної мережевої інфраструктури з урахуванням цифрових технологій та фінансових, економічних і політичних тенденцій, що сприяють формуванню набору цифрових активів для фінансів нової енергії та кращого розуміння взаємозв'язку між різними суб'єктами господарювання, а також розробці надійних майбутніх сценаріїв. З точки зору дотримання безпекових аспектів переходу підприємств до високотехнологічного економічного розвитку, цей підхід повинен містити складові, пов'язані із забезпеченням стабільної правової та нормативної бази функціонування суб'єктів господарювання, її гармонізацією із європейським законодавством, що регулює господарські відносини.

Водночас потребують подальшого наукового дослідження питання, пов'язані з децентралізацією, декарбонізацією, цифровізацією, зберіганням електроенергії, ринковим дизайном та поновлюваними джерелами енергії. Також варто окремо вивчати ключові фактори ризику щодо технологічних інновацій, які вже нині спричинили переорієнтацію промисловості з мейнфреймів на персональні комп'ютери, Інтернету – на смартфони, глобального з'єднання (сумісності) – на об'єднання цифрового та фізичного світів на основі цифрових платформ та екосистем, де виникає потреба у забезпеченні цифрової та мережевої інфраструктури з урахуванням пристроїв і платформ.

Україні важливо не відставати від мейнстриму цих тенденцій. Гіпотетичне осмислення та передбачення кардинальних змін у суспільстві щодо можливості подальшого розвитку держави й уникнення загроз внаслідок цифрової глобалізації вимагає розроблення та впровадження єдиної національної стратегії розвитку та відповідного інструментарію моделювання майбутнього розвитку промисловості як системи на підставі висунення гіпотез із технологічно-концептуальної точки зору.

Таким чином, вирішення нагальних проблем соціально-економічного характеру та подальший розвиток економіки України повинні відбуватися на основі побудови конкурентоспроможної в глобальному просторі соціально-орієнтованої ринкової економіки, де моделювання майбутнього розвитку промисловості як системи повинно здійснюватися на інноваційно спрямованій основі, органічно поєднаній з міжнародними інституціями, науковими центрами, і носити випереджальний, а не адаптивний характер. Визначення шляхів удосконалення організаційно-економічних засад переходу суб'єктів господарювання до високотехнологічного економічного та інноваційного розвитку держави повинно базуватися на глибокому аналізі стану та тенденцій функціонування мережевої інфраструктури в Україні як у контексті міжнародних порівнянь, так і на державному й регіональному рівнях.

Додаток

Перелік платформ, широкомасштабних пілотних проектів і тест-майданчиків, які впроваджуються у ЄС до 2020 року

Платформи	Широкомасштабні пілотні проекти	Тест-майданчики
З'єднані «розумні» підприємства *(Connected Smart Factories)*		
• *Smart, Safe & Secure Platform – S3P;* • *Optician 2020ICT;* • *Unmanned Systems Industrial Robotic Platform (USIRP);* • *Sense & React;* • *MAGINE – Innovative End-to-end Management of Dynamic Manufacturing Networks;* • *SeRoNet;* • *Industrial Communication for Factories (IC4F);* • *ROS-Industrial*	• *Vendor-independent Industry 4.0 production line;* • *Large 4.0 investments initiative;* • *PressNozz: AI-based modelling for production optimization based on an enriched data acquisition method;* • *Anella Industrial 4.0 (AI4.0);* • *Pilot Digital and Virtual Factory integrating planning and simulation into operative environment;* • *The Advanced Sustainable Surface & Coating Manufacturing Technologies on Polymer materials;* • *ERICA: Establishing Regional Cluster Agreement for sharing good practices in Advanced Manufacturing;* • *PREVIEW: PREdictiVe system to recommend Injection mold sEtup in Wireless sensor networks*	• *Testbed for cognitive autonomous work systems for human centered manufacturing in Industry 4.0;* • *SmartFactoryKL;* • *FactoryLab;* • *FFLOR: Future – Factory@LORraine;* • *VIRTUREAL;* • *Plataforma Industrial 4.0*
«Розумне» сільське господарство *(Smart Agriculture)*		
• *FIspace;* • *Robot-assisted movement;* • *PRIMARE;* • *Tracciabilita e Big Data (Traceability and big data);* • *HortiCube*	• *Internet of Food and Farm 2020 (IoF2020);* • *AgriTech Big Data Platform;* • *Fruit 4.0;* • *DATA-FAIR;* • *Pilot Project of Fraunhofer Society Germany in cooperation with State Country of Saxony developing digital technologies in Smart Farming*	• *Dutch National Testbed; Precision Agriculture (Nationale Proeftuin Precisielandbouw);* • *Simulareg*
Цифрова трансформація охорони здоров'я та допомоги *(Digital Transformation of Health and Care)*		
• *CONNECARE: Self-management system for complex chronic patients;* • *eKauri;* • *eKenku;* • *MyVitalink;* • *Health Suite Digital Platform;* • *Luxembourg national eHealth digital platform*	• *VINCLES*	• *The Experiment'HAAL Living Lab*
Платформи промислових даних *(Industrial Data Platforms)*		
• *Industrial Data Space (IDS);* • *CIMEC: New generation of Cyber Physical Systems for productivity increase in high added value industrial sectors;* • *openEASE*	• *Exploiting mobile phone data for statistical and commercial purposes;* • *TeraLab;* • *Mo3Dlling: Intelligent monitoring and visualization of injection process and smart moulds;* • *Piloting Industrial Data Space in Smart Industry Fieldlabs*	• *IPCEI on HPC and Big Data enabled applications;* • *Big Data Centre of Excellence Barcelona (Big Data CoE BCN)*
Інтернет речей *(Internet of Things)*		
	• *Large-scale Pilots under the 2016 Internet of Things Focus Area;* • *SmartGrids_CTM: Integration of renewable energy sources to smart grids*	• *FIT;* • *Smart Objects & IoT Platform Lab*

Джерело: складено за даними звітів *Working Group 2 – Digital Industrial Platforms.*

Список використаних джерел

1. Вице-президент Всемирного банка Сирил Муллер: «Экономика начала расти. Это важно. Но достаточно ли этого?» [Електронний ресурс]. – Режим доступу : https://zn.ua/macrolevel/vice-prezident-vsemirnogo-banka-siril-muller-ekonomika-nachala-rasti-eto-vazhno-no-dostatochno-li-etogo-275580_.html
2. Договор между СССР и США о ликвидации их ракет средней дальности и меньшей дальности (РСМД) [Електронний ресурс]. – Режим доступу : http://www.un.org/ru/documents/decl_conv/conventions/pdf/treaty.pdf
3. Кабмін затвердив Стратегію розвитку цифрової економіки до 2020 р. [Електронний ресурс]. – Режим доступу : http://ua.interfax.com.ua/news/economic/477494.html
4. Трамп впервые представит стратегию национальной безопасности [Електронний ресурс]. – Режим доступу : https://www.golos-ameriki.ru/a/us-national-security-strategy/4166811.html
5. A global distributed architecture connecting all clouds and all devices [Електронний ресурс]. – Режим доступу : http://www.telecomtv.com/articles/ericsson-intel-channel/a-global-distributed-architecture-connecting-all-clouds-and-all-devices-science-fiction-or-science-fact-14464/
6. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All Електронний ресурс]. – Режим доступу : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A228%3AFIN
7. Code of PLM Openness [Електронний ресурс]. – Режим доступу: https://www.techniatranscat.com/about-techniatranscat/about-techniatranscat/code-of-plm-openness
8. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Digitising European Industry Reaping the full benefits of a Digital Single Market{SWD(2016) 110 final} [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0180
9. January 2018 setting up the Strategic Forum for Important Projects of Common European Interest [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2018_039_R_0003
10. Украина опустилась в рейтинге самых конкурентоспособных экономик [Електронний ресурс]. – Режим доступу : http://www.liga.net/infografica/336825_ukraina-opustilas-v-reytinge-samykh-konkurentosposobnykh-ekonomik.htm
11. Digitising European Industry: Working Group 2 – Digital Industrial Platforms [Електронний ресурс]. – Режим доступу : https://ec.europa.eu/futurium/en/system/files/ged/dei_wg2_final_report.pdf
12. IEC 62264-5:2016 Enterprise-control system integration – Part 5: Business to manufacturing transactions [Електронний ресурс]. – Режим доступу : https://www.iso.org/standard/57308.html
13. EUROPE 2020 A strategy for smart, sustainable and inclusive growth /* COM/2010/2020 final */ [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52010DC2020
14. ETSI and partners gather over 200 Cyber security experts and policy makers in Brussels [Електронний ресурс]. – Режим доступу : https://www.telecomtvtracker.com/insights/etsi-and-partners-gather-over-200-cybersecurity-experts-and-policy-makers-in-brussels-13295/
15. Qualcomm Announces a New LTE IoT Software Development Kit in Support of the Commercialization of Internet of Things Solutions Using Cellular Connectivity [Електронний ресурс]. – Режим доступу : https://www.qualcomm.com/news/releases/2018/02/14/qualcomm-announces-new-lte-iot-software-development-kit-support
16. Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic identification and trust services for electronic transactions in the internal market, eIDAS and repealing Directive 1999/93/EC [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
17. SpaceX fires up rocket that will carry the first two 'global internet' Starlink satellites [Електронний ресурс]. – Режим доступу : http://www.ibtimes.co.uk/spacex-fires-rocket-that-will-carry-first-two-global-internet-starlink-satellites-1660579
18. Technology Transition Final Public Report Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) [Електронний ресурс]. – Режим доступу : https://energy.gov/sites/prod/files/2016/03/f30/spiders_final_report.pdf

References

1. Vitse-prezident Vsemirnogo banka Siril Muller: «Ekonomika nachala rasti. Eto vazhno. No dostatochno li etogo?» [Vice President of the World Bank Cyril Muller: "The economy has started to grow. This is important. But is this enough?"]. (n.d.). *zn.ua.* Retrieved from https://zn.ua/macrolevel/vice-prezident-vsemirnogo-banka-siril-muller-ekonomika-nachala-rasti-eto-vazhno-no-dostatochno-li-etogo-275580_.html [in Russian].
2. Dogovor mezhdu SSSR i SSHA o likvidacii ih raket srednei dalnosti i menshei dalnosti (RSMD) [The USSR–USA Agreement on the Elimination of their Medium-range and Short-range Missiles]. (n.d.). *www.un.org.* Retrieved from http://www.un.org/ru/documents/decl_conv/conventions/pdf/treaty.pdf [in Russian].
3. Kabmin zatverdyv Stratehiu rozvytku tsyfrovoi ekonomiky do 2020 r. [The Cabinet of Ministers of Ukraine approved the Strategy for the Development of the Digital Economy by 2020]. (n.d.). *ua.interfax.com.ua.* Retrieved from http://ua.interfax.com.ua/news/economic/477494.html [in Ukrainian].
4. Tramp vpervie predstavit strategiu natsionalnoi bezopasnosti [Trump will present for the first time a national security strategy]. (n.d.). *www.golos-ameriki.ru.* Retrieved from https://www.golos-ameriki.ru/a/us-national-security-strategy/4166811.html [in Russian].
5. A global distributed architecture connecting all clouds and all devices. (n.d.). *www.telecomtv.com.* Retrieved from http://www.telecomtv.com/articles/ericsson-intel-channel/a-global-distributed-architecture-connecting-all-clouds-and-all-devices-science-fiction-or-science-fact-14464/ [in English].
6. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All. (n.d.). *eur-lex.europa.eu.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A228%3AFIN [in English].
7. Code of PLM Openness. (n.d.). *www.techniatranscat.com.* Retrieved from https://www.techniatranscat.com/about-techniatranscat/about-techniatranscat/code-of-plm-openness [in English].
8. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Digitising European Industry Reaping the full benefits of a Digital Single Market{SWD(2016) 110 final}. (n.d.). *eur-lex.europa.eu.* Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0180 [in English].
9. Commission Decision of 30 January 2018 setting up the Strategic Forum for Important Projects of Common European Interest. (n.d.). *eur-lex.europa.eu.* Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2018_039_R_0003 [in English].
10. Ukraina opustilas v reitinge samykh konkurentosposobnykh ekonomik [Ukraine fell in the ranking of the most competitive economies]. (n.d.). *www.liga.net.* Retrieved from http://www.liga.net/infografica/336825_ukraina-opustilas-v-reytinge-samykh-konkurentosposobnykh-ekonomik.htm[in Russian].
11. Digitising European Industry: Working Group 2 – Digital Industrial Platforms. (n.d.). *ec.europa.eu.* Retrieved from https://ec.europa.eu/futurium/en/system/files/ged/dei_wg2_final_report.pdf [in English].
12. IEC 62264-5:2016 Enterprise-control system integration – Part 5: Business to manufacturing transactions. (n.d.). *www.iso.org.* Retrieved from https://www.iso.org/standard/57308.html[in English].
13. EUROPE 2020 A strategy for smart, sustainable and inclusive growth /* COM/2010/2020 final*/. (n.d.). *eur-lex.europa.eu.* Retrieved from http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52010DC2020 [in English].
14. ETSI and partners gather over 200 Cybersecurity experts and policy makers in Brussels. (n.d.). *telecomtvtracker.com.* Retrieved from https://www.telecomtvtracker.com/insights/etsi-and-partners-gather-over-200-cybersecurity-experts-and-policy-makers-in-brussels-13295/ [in English].
15. Qualcomm Announces a New LTE IoT Software Development Kit in Support of the Commercialization of Internet of Things Solutions Using Cellular Connectivity. (n.d.). *www.qualcomm.com.* Retrieved from https://www.qualcomm.com/news/releases/2018/02/14/qualcomm-announces-new-lte-iot-software-development-kit-support [in English].
16. Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. (n.d.). *eur-lex.europa.eu.* Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG [in English].
17. SpaceX fires up rocket that will carry the first two 'global internet' Starlink satellites. (n.d.). *www.ibtimes.co.uk.* Retrieved from http://www.ibtimes.co.uk/spacex-fires-rocket-that-will-carry-first-two-global-internet-starlink-satellites-1660579 [in English].
18. Technology Transition Final Public Report Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS). (n.d.). *energy.gov.* Retrieved from https://energy.gov/sites/prod/files/2016/03/f30/spiders_final_report.pdf [in English].