УДК 336.1:339.7+351.86 https://doi.org/10.33763/npndfi2021.03.058

Клименко К. В.
кандидат економічних наук, завідувач відділу бюджетної системи НДФІ ДННУ "Академія фінансового управління", Київ, Україна, klymenko_kateryna@ukr.net
ORCID ID: https://orcid.org/0000-0001-8295-1333

Павлюк К. В.
доктор економічних наук, професор, завідувач відділення бюджетної політики та розвитку бюджетної системи НДФІ ДННУ "Академія фінансового управління", Київ, Україна, cllav@ukr.net
ORCID ID: https://orcid.org/0000-0002-9495-6630

Савостьяненко М. В.
старший науковий співробітник відділу міжнародних фінансів та фінансової безпеки НДФІ ДННУ "Академія фінансового управління", Київ, Україна, savomax@ukr.net
ORCID ID: https://orcid.org/0000-0002-6712-5831

СВІТОВА ПРАКТИКА ФІНАНСУВАННЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. *Досліджено проблематику фінансового забезпечення реалізації захисту критичної інфраструктури в міжнародних аспектах. Виокремлено та проаналізовано основні типи фінансування інфраструктурних проєктів і проєктів захисту критичної інфраструктури за рахунок: бюджетних коштів; кредитних ресурсів; приватних коштів; коштів міжнародних фінансово-кредитних організацій. Визначено роль міжнародних фінансових організацій у процесах фінансування інфраструктурних проєктів. Досліджено основні аспекти та особливості системи фінансового захисту фізичних активів. Окреслено та проаналізовано головні складники цієї системи – страхування державного майна, бюджетні механізми, такі як спеціальні фонди на випадок стихійних лих. Виявлено, що інвестування у фінансову стійкість має ключове значення для забезпечення більшої готовності суспільства до нових та несподіваних ризиків. Зроблено висновок, що фінансова готовність є найважливішою передумовою безперервності обслуговування як для забезпечення належного фінансування систематичного ремонту і технічного обслуговування об'єктів критичної інфраструктури після неістотних подій, так і для реалізації планів на випадок надзвичайних ситуацій зі швидкого відновлення критичної інфраструктури. Проаналізовано проєкти критичної інфраструктури в деяких зарубіжних країнах.*

Ключові слова: критична інфраструктура, захист критичної інфраструктури, фінансування інфраструктурних проєктів, Світовий банк, міжнародні фінансові організації, державно-приватне партнерство, кібербезпека, стратегія національної безпеки.

Рис. 1. Табл. 1. Літ. 25.

Kateryna Klymenko
Ph. D. (Economics), SESE "The Academy of Financial Management", Kyiv, Ukraine, klymenko_kateryna@ukr.net
ORCID ID: https://orcid.org/0000-0001-8295-1333

Klaudia Pavliuk
Dr. Sc. (Economics), Professor, SESE "The Academy of Financial Management", Kyiv, Ukraine, cllav@ukr.net
ORCID ID: https://orcid.org/0000-0002-9495-6630

Maksym Savostianenko
SESE "The Academy of Financial Management", Kyiv, Ukraine, savomax@ukr.net
ORCID ID: https://orcid.org/0000-0002-6712-5831

WORLD PRACTICE OF FINANCING THE PROTECTION OF CRITICAL INFRASTRUCTURE

Abstract. *In the article the authors investigate the issue of financial support for the implementation of critical infrastructure protection in international aspects. The main types of financing of infrastructure projects and projects of critical infrastructure protection at the expense of: budgetary funds, credit resources, private funds, international financial organizations (IFIs) are singled out and analyzed. Features, advantages, disadvantages of each of these types of financing are investigated. The role of key international financial organizations in the processes of financing infrastructure projects is determined. The issue of ensuring proper financial protection of physical assets is considered. The main aspects and features of the system of such protection, which are the availability of finances and plans for the restoration or reconstruction of critical assets after a disaster, damage to critical infrastructure are analyzed. The main mechanisms of the system of financial protection of physical assets – insurance of state property, budgetary mechanisms, such as special funds in case of natural disasters, are also revealed and analyzed. It has been found that investing in financial sustainability is crucial to ensure greater preparedness throughout a society, especially for new and unexpected risks. It is concluded that financial preparedness is an essential part of ensuring continuity of service, both to ensure adequate funding for more frequent repairs and maintenance of critical infrastructure after minor events, and to implement contingency plans for the rapid recovery of critical infrastructure. Critical infrastructure projects in some countries of the world are analyzed. The modern innovative experience of financial protection of owners and operators of infrastructure in some countries and practical steps for integration of provisions on protection of critical infrastructure within the limits of national strategies of financial protection of critical infrastructure are investigated.*

Keywords: critical infrastructure, critical infrastructure protection, financing of infrastructure projects, World Bank, International financial organizations, Public-private partnership, cybersecurity, national security strategy.

JEL classification: F52, H54, H56.

Клименко Е. В.
кандидат экономических наук, заведующая отделом бюджетной системы НИФИ ГУНУ "Академия финансового управления", Киев, Украина

Павлюк К. В.
доктор экономических наук, професор, заведующая отделом бюджетной политики и развития бюджетной системы НИФИ ГУНУ "Академия финансового управления", Киев, Украина

Савостьяненко М. В.
старший научный сотрудник отдела международных финансов и финансовой безопасности НИФИ ГУНУ "Академия финансового управления", Киев, Украина

МИРОВАЯ ПРАКТИКА ФИНАНСИРОВАНИЯ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Аннотация. *Исследована проблематика финансового обеспечения реализации защиты критической инфраструктуры в международных аспектах. Выделены и проанализированы основные типы финансирования инфраструктурных проектов и проектов защиты критической инфраструктуры за счет: бюджетных средств; кредитных ресурсов; частных средств; средств международных финансово-кредитных организаций. Определена роль международных финансовых организаций в процессах финансирования инфраструктурных проектов. Исследованы основные аспекты и особенности системы финансовой защиты физических активов. Определены и проанализированы главные составляющие данной системы – страхование государственного имущества, бюджетные механизмы, такие как специаль-*

ные фонды на случай стихийных бедствий. Установлено, что инвестирование в финансовую устойчивость имеет ключевое значение для обеспечения большей готовности общества к новым и неожиданным рискам. Сделан вывод, что финансовая готовность является важнейшей предпосылкой непрерывности обслуживания как для обеспечения надлежащего финансирования систематического ремонта и технического обслуживания объектов критической инфраструктуры после незначительных событий, так и для реализации планов на случай чрезвычайных ситуаций по быстрому восстановлению критической инфраструктуры. Проанализированы проекты критической инфраструктуры в некоторых зарубежных странах.

Ключевые слова: критическая инфраструктура, защита критической инфраструктуры, финансирование инфраструктурных проектов, Всемирный банк, международные финансовые организации, государственно-частное партнерство, кибербезопасность, стратегия национальной безопасности.

Забезпечення національних економічних інтересів країн потребує формування і реалізації стратегічного курсу у сфері забезпечення економічної безпеки, спрямованого як на стале нарощення конкурентоспроможності економіки держав, так і на поступове зміцнення економічної стійкості та, відповідно, невразливості економіки до зовнішніх і внутрішніх загроз. Незадовільний технічний стан та рівень захисту об'єктів критичної інфраструктури, брак інвестицій в її оновлення і розвиток, потенційна загроза несанкціонованих втручань фізичного й кіберхарактеру в її функціонування є головними викликами і загрозами у сфері виробничої та фінансової безпеки будь-якої країни.

Тому набуває актуальності вивчення світового досвіду фінансового забезпечення захисту критичної інфраструктури, розбудови якісної інфраструктури, залучення внутрішніх та іноземних інвестицій у модернізацію і розвиток об'єктів критичної (інженерної, інформаційної, енергетичної) інфраструктури; розроблення механізму й реалізації державного супроводу впровадження новітніх технологій у галузях, що мають стратегічне значення для національної безпеки держави та її критичної інфраструктури; обґрунтування стратегічних напрямів з подальшої його імплементації в Україні.

Критична інфраструктура є об'єктом досліджень багатьох науковців, які зробили вагомий внесок у вивчення окресленої проблематики. Серед зарубіжних дослідників виокремимо таких як: Т. Вілбенкс, Д. Білелло, Д. Шмальцер, М. Скотт [1], С. Хасан, Е. Фахім, Дж. Фолінтеа, А. Ель-Зейнц [2] та ін.

Окремі організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України досліджували такі вчені, як Д. Г. Бобро, С. П. Іванюта, С. І. Кондратов, О. М. Суходоля [3]. Автори О. П. Єрменчук та М. Л. Пальчик акцентують увагу на проблемних аспектах правового регулювання державно-приватного партнерства (ДПП) у сфері захисту критичної інфраструктури [4].

Головні тези концепції захисту критичної інфраструктури як елемента загальноєвропейської безпекової політики країн ЄС містяться у дослідженнях Д. С. Бірюкова [5].

В. П. Кудряшов досліджує досвід фінансового забезпечення формування й розвитку критичної інфраструктури у зарубіжних країнах, розкриває механізми фінансового забезпечення критичної інфраструктури, котрі використовуються в цих країнах, а також пов'язані з ним ризики [6]. Утім, ця проблематика потребує подальшого дослідження з урахуванням викликів і загроз, що виникають в сучасних реаліях щодо питання посилення захисту критичної інфраструктури.

Мета статті полягає у визначенні окремих аспектів фінансового забезпечення захисту критичної інфраструктури у світовій практиці та обґрунтуванні стратегічних напрямів з подальшої імплементації такого досвіду в Україні.

Насамперед розглянемо фінансове забезпечення реалізації захисту критичної інфраструктури. Так, фінансове і ресурсне забезпечення захисту об'єктів критичної інфраструктури здійснюють їх власники (розпорядники). Варто окреслити основні типи фінансування інфраструктурних проєктів, які, зокрема, можуть бути застосовані й до проєктів захисту критичної інфраструктури:

1) за рахунок бюджетних коштів;
2) за рахунок кредитних ресурсів;
3) за рахунок приватних коштів. Цю категорію проєктів можна умовно поділити на: а) ті, які фінансуються лише приватним сектором, перебувають у приватній власності та управлінні; б) ті, які виконуються на основі контракту з державою та хоча б частково фінансуються за рахунок різних форм ДПП, у тому числі за допомогою концесійної форми;
4) за рахунок коштів МФО.

Фінансування за рахунок бюджетних коштів. У фінансуванні проєктів захисту критичної інфраструктури можуть бути використані кошти державного та місцевих бюджетів, але на практиці частка таких коштів є вкрай незначною і фактично виконує допоміжну функцію. Як правило, державні органи намагаються забезпечити непряму (опосередковану) фінансову допомогу: у формі державних гарантій, взяття на себе частини ризиків, кредитної підтримки, податкових пільг та інших державних фінансових інструментів. Бюджетні кошти спрямовуються на участь в проєкті у разі, якщо він має велике стратегічне значення або без державної підтримки проєкт не може бути комерційно виправданим.

Фінансування за рахунок кредитних ресурсів. Банківський сектор є ключовим суб'єктом при реалізації інвестиційних проєктів. Слід зауважити, що банки відіграють особливу роль в процесі реалізації проєктного фінансування, яка не обмежується лише роллю кредитора. У цьому процесі банк виконує такі функції: надання банківських кредитів, співінвестування проєктів, підтримка лізингових операцій, комерційного кредитування, ініціативи створення банківських консорціумів, інституційного інвестора, який купує цінні папери проєктних компаній, тощо. Завдання банку під час проєктного фінансування передбачають: 1) оцінювання вартості інвестиційного капіталу; 2) затвердження бюджету та плану фінансування проєкту; 3) надання посередницьких і експертних послуг; 4) здійснення бюджетного контролю.

У світовій практиці достатньо чітко склалися дві схеми проєктного фінансування – з паралельним та послідовним фінансуванням. За схемою паралельного фінансування для реалізації проєкту кредити надають декілька кредитних установ; це дає змогу банкам не перевищувати дозволених сум кредитів та знижувати свої кредитні ризики. Доволі часто в цій групі банків наявний так званий ініціатор – потужний великий комерційний банк або міжнародний фінансовий інститут. За послідовного фінансування також існує великий банк-організатор, але на нього покладено виконання інших функцій. Він є ініціатором договору кредитування, але не як кредитор. У разі надання кредиту підприємству такий банк передає свої права за боргом наступному кредитору (кредиторам) і таким чином знімає дебіторську заборгованість зі свого балансу.

Фінансування за рахунок коштів міжнародних фінансово-кредитних організацій. Метою залучення цієї групи кредиторів є мінімізація фінансових ризиків проєктів та досягнення фінансового завершення інфраструктурних проєктів. Міжнародні фінансово-кредитні організації є найбільшими стабільними партнерами, а їхня участь у фінансуванні підвищує надійність інфраструктурного проєкту та зменшує ризики для інших кредиторів та інвесторів [7].

У групі Світового банку найважливішу роль у фінансуванні інфраструктурних проєктів відіграють такі організації.

1. Міжнародний банк реконструкції та розвитку (МБРР) – надає фінансову допомогу урядам країн на розвиток внутрішньої інфраструктури. Водночас ця організація закликає до посилення позицій приватного сектору в цій галузі. Під час участі у проєктах також може взяти на себе деякі проєктні ризики.
2. Міжнародна фінансова корпорація (МФК) – надає підтримку приватному сектору у випадках відсутності гарантій приймаючої країни;
3. Міжнародна агенція інвестиційних гарантій – надає захист прямим іноземним інвестиціям у країнах, що розвиваються, від настання та дії ризиків політичного та валютного характеру.

При цьому важливо врахувати й виняткову роль Європейського банку реконструкції та розвитку (ЄБРР) у процесі фінансування інфраструктурних проєктів.

Фінансування за рахунок приватних коштів. Критично важливі проєкти також можуть фінансуватися приватним сектором та перебувати у приватній власності або виконуватися на основі контракту з державою і хоча б частково фінансуватися за рахунок форм державно-приватного партнерства, у тому числі концесії. Особливу увагу варто приділити фінансуванню на основі державно-приватного партнерства, оскільки в умовах фінансової кризи ця форма відіграє своєрідну роль. Державно-приватне партнерство реалізується у таких головних формах: концесія; управління майном (виключно за умови передбачення у договорі, укладеному в рамках державно-приватного партнерства, інвестиційних зобов'язань приватного партнера); спільна діяльність; інші договори тощо [7].

Утім, за даними дослідження Booz & Company (Italia) S.r.l. [8], уряд жодної країни – члена ЄС не надає приватним установам фінансову допомогу

для компенсації витрат, пов'язаних із приведенням їхньої діяльності у відповідність із державними програмами захисту критичної інфраструктури. Натомість більша частина державної фінансової допомоги, призначена для управління під час надзвичайних ситуацій та забезпечення безпеки, залишається у розпорядженні урядових установ, які займаються цими питаннями.

Оскільки державні органи, які координують діяльність із захисту критичної інфраструктури, переважно входять до функціональних структур управління вищого рівня, то їм надається перевага при фінансуванні заходів загальнодержавного значення. Водночас приватні власники та керівники об'єктів критичної інфраструктури зобов'язані самостійно виділяти кошти на приведення своєї діяльності з управління внутрішніми ризиками та забезпечення безперервності бізнесу у відповідність з урядовими програмами захисту критичної інфраструктури.

Однак така модель фінансування, на думку експертів Booz & Company [8], має певні недоліки: чисельність спеціально призначеного персоналу для вирішення питань захисту критичної інфраструктури в урядах та на підприємствах є недостатньою; обов'язки, пов'язані із виконанням заходів захисту критичної інфраструктури, є додатковими, позаштатними, що зумовлює низький рівень відповідальності за їх виконання; відсутність фінансової допомоги стає на заваді приведенню діяльності із захисту критичної інфраструктури у відповідність з урядовими програмами; зміщення пріоритетів на фінансування урядових установ ускладнює процес отримання приватними суб'єктами внутрішнього фінансування.

Отже, забезпечення результативної реалізації критично важливих інфраструктурних проєктів відбувається шляхом вдосконалення механізму фінансування таких проєктів за рахунок різних методів та джерел, а саме: бюджетних коштів; кредитних ресурсів; приватних коштів (ДПП та концесія); коштів міжнародних фінансово-кредитних організацій.

Фінансовий захист фізичних активів. Розглянемо проблематику фінансового захисту фізичних активів. Так, у звіті Світового банку "Financial Protection of Critical Infrastructure Services" [9] наголошується на фінансовому захисті фізичних активів об'єктів захисту критичної інфраструктури. Цей захист означає наявність фінансів та планів відновлення або реконструкції критично важливих активів після катастрофи, пошкодження об'єкта критичної інфраструктури. Захист може передбачати, наприклад, страхування державного майна або бюджетні механізми, такі як спеціальні фонди на випадок стихійних лих.

У 2018 р. АТЕС (Азійсько-Тихоокеанське економічне співробітництво, англ. The Asia-Pacific Economic Cooperation; скорочено АТЕС, англ. APEC) та Світовий банк разом працювали над оперативною базою програм страхування від катастроф для державних активів, ґрунтуючись на досвіді Австралії, Колумбії, Японії, Мексики та Нової Зеландії. На думку експертів МФО, підходи до посилення фінансового захисту критично важливих інфраструктурних служб повинні бути інтегровані у поточну роботу зі зміцнення стійкості.

Ця інтеграція, зокрема, охоплює: 1) зусилля з підвищення фізичної стійкості систем критичної інфраструктури та соціальної й економічної стійко-

сті; 2) використання наявних провідних практик щодо стійкості в рамках державно-приватних партнерських відносин в інфраструктурі. Посилений фінансовий захист може забезпечити істотні переваги для більшої стійкості. Впровадження правил, які визначають, хто сплачує збитки в разі катастрофи, не лише допомагає управляти ризиками для державних фінансів, а й створює стимули для власників інфраструктури та операторів інвестувати більше у формування довготривалої стійкості. Дедалі очевиднішим стає той факт, що посилення готовності до катастроф може сприяти кращому відновленню.

За допомогою регулювання та практики закупівель уряд може заохочувати належний фінансовий захист з боку власників критичної інфраструктури і операторів. Більше того, власники інфраструктури та оператори несуть основну відповідальність за захист своїх активів й підтримання безперервності послуг, які вони надають. Однак пріоритети і рівні толерантності до ризику в державному та приватному секторах зазвичай відрізняються. Будучи розробником політики, фінансовим агентом і регулятором, уряд часто відіграє ключову роль у встановленні необхідних рівнів готовності, які забезпечать прийнятний рівень ризику для громадян та національної безпеки.

Цей підхід може передбачати: а) встановлення мінімальних вимог до управління ризиками і механізмів передачі ризиків шляхом регулювання; б) реалізацію заходів з розподілу витрат у рамках державно-приватного партнерства; в) вимогу щодо розкриття інформації про ризики або г) використання контрактів, котрі ґрунтуються на результатах, які стимулюють безперервність надання послуг. Зобов'язуючи операторів встановлювати певну форму страхування, можна оцінити ризики і вимагати належного технічного обслуговування та експлуатації об'єктів як умови виплати, що загалом додатково сприятиме підвищенню стійкості.

Інвестування у фінансову стійкість має ключове значення для забезпечення більшої готовності суспільства до нових та несподіваних ризиків. Світовий досвід переконує, що вигоди від належного управління фінансовими ризиками полягають не лише у ранньому, передбачуваному фінансуванні, отриманому після події, а й у глибшому розумінні ризику, плануванні й попередженні катастроф та використанні новітніх рішень для створення систем, які можуть забезпечити посилення стійкості до катастроф.

Щоб уряди могли бути краще підготовленими до можливих потрясінь у майбутньому, посилення фінансової готовності повинно стати рушієм відновлення після пандемії COVID-19. Фінансовий захист критичної інфраструктури є ще важливішим у контексті періоду відновлення, коли перед країнами постають фіскальні обмеження, а домогосподарства та фірми економічно менше захищені.

Важливо, що економічні та соціальні наслідки порушень критичної інфраструктури походять здебільшого від втрати послуги, яку вони надають, а не від витрат на відновлення пошкоджень самих активів. Наприклад, прямий збиток від катастроф для виробництва електроенергії та транспортної

інфраструктури оцінюється у 18 млрд дол. США на рік у країнах із низьким та середнім рівнями доходу в усьому світі. Проте орієнтовна вартість пов'язаних із цим порушень послуг (енергетики і транспорту) коливається від 391 млрд до 647 млрд дол. США (що принаймні більше в 20 разів) [9].

Крім людського впливу, такі витрати можуть також посилювати тиск на державні бюджети за рахунок зменшення доходів та збільшення видатків; витрати можуть зупинити інвестиції в економіку, що суттєво вплине на довгострокове зростання і добробут. Цей висновок свідчить про необхідність змістити акцент від стійкості активів до надання критично важливих послуг, які є стійкими.

Також експерти Світового банку наголошують на поєднанні фінансової та оперативної готовності для забезпечення безперервності надання критичних послуг [9]. Фінансова готовність є найважливішою частиною забезпечення безперервності обслуговування, як для належного фінансування систематичного ремонту і технічного обслуговування після менших, регулярніших подій (незначні катастрофи та стихійні лиха), так і для реалізації планів на випадок надзвичайних ситуацій для швидкого відновлення критичної інфраструктури після серйозніших катастроф (падіння мосту, дамби).

Фінансова готовність. Для втілення цих планів доступні механізми забезпечення та ефективного доступу до адекватного й своєчасного фінансування. Так, у питанні фінансової готовності можна додатково виокремити два аспекти:

- мобілізація/доступ до фінансування. Наявність належних фінансових інструментів (таких як непередбачені бюджети та страхування) забезпечить економічно ефективний доступ до достатнього фінансування для подолання наслідків потрясінь різної тяжкості, поряд із достатнім фінансуванням для регулярних операцій і технічного обслуговування (O&M);
- забезпечення фінансування. Наявність належних механізмів фінансування забезпечить ефективний потік коштів. Механізми передбачають, наприклад, способи переказу коштів між урядовими відомствами та ефективні процедури запиту, затвердження і розподілу фінансування. Цей аспект є критичним, оскільки досвід показує, що така нестача може бути головною перешкодою для швидких дій. За допомогою якісної аналітики даних про ризики уряди та власники інфраструктури і оператори можуть оцінювати ймовірні наслідки, визначати пріоритети планування, ініціювати ранні дії та координувати заходи з відновлення [9].

Украй важливою є наявність оперативної готовності. Необхідні розроблення якісних планів, стандартних операційних протоколів і забезпечення належних можливостей для швидкого відновлення критично важливих служб та об'єктів (наприклад, людські ресурси, обладнання, технічні ресурси).

Цей інтегрований підхід експерти Світового банку характеризують як систему, що реагує на удари. За наявності таких систем оператори критичної

інфраструктури знають, що вони мають фінансування для впровадження і реалізації планів, обладнання та угод, необхідних для забезпечення швидкого відновлення. Цей підхід також означає, що розподіл фінансування може бути виконаний швидко і відповідно до узгоджених цілей. Ролі уряду у здійсненні оперативної та фінансової готовності на кожному етапі залежатимуть від того, хто володіє критично важливими інфраструктурними активами і послугами та експлуатує їх. У разі повної державної власності кожна з цих дій буде відповідальністю уряду.

Для повністю приватизованого сектору критичної інфраструктури за дії буде відповідати приватний сектор, хоча уряд може встановлювати стандарти шляхом регулювання, стимулювати та надавати публічні блага (наприклад, системи раннього попередження, координаційні форуми). Важливо визнати, що операційні чинники нерідко можуть бути головним обмеженням для швидкого відновлення, особливо в країнах з низьким рівнем доходів. Фінансова готовність необхідна, але недостатня.

Заходи з відновлення можуть уповільнюватися, наприклад, через відсутність можливості контролювати систему для швидкого виявлення: а) джерела відмови послуги; б) браку планування на випадок непередбачених ситуацій або в) дефіциту людей, запасних частин, обладнання. Також можуть бути фізичні причини затримки відновлення (зокрема труднощі при доступі до пошкодженої інфраструктури, спричинені заблокованими дорогами). Якщо уряди хочуть зміцнити стійкість критично важливих служб, то насамперед вони мають оцінити потенційні проблеми (“вузькі місця”) як в операційній, так і у фінансовій готовності для відновлення.

Так, у США оперативна та фінансова готовність до катастроф в енергетичному секторі тісно взаємопов’язані. Передбачається, що всі штати мають юридичну владу над надзвичайними ситуаціями, а забезпечення безперервності й відновлення служб належить до компетенції комунальників та координаторів мереж. Держави використовують заздалегідь узгоджені плани надзвичайних ситуацій, які ґрунтуються на Національній системі реагування, для чіткого визначення обов’язків між різними учасниками.

Також комунальні підприємства повинні розробити власні плани реагування на надзвичайні ситуації, які періодично подаються на затвердження державному регулятору. Електричним комунальним компаніям доступні численні фінансові та регуляторні інструменти для визначення витрат на реагування і відшкодування, зокрема інструменти попереднього фінансування (наприклад, резервні рахунки) та інструменти ex-post (наприклад, сек’юритизація, випуск облігацій для оплати, відстрочки, а також затверджені тарифи для споживачів) [9].

В Японії органи місцевого самоврядування мають спеціальні механізми для швидкого відновлення державної інфраструктури. Стосовно фінансової готовності, то органи місцевого самоврядування повідомляють профільні міністерства про пошкодження інфраструктури та замовляють отримання національної субсидії на відновлювальні роботи протягом декількох днів.

Як захід оперативної готовності, вони можуть укласти спеціальні угоди з приватними компаніями або місцевими галузевими асоціаціями, щоб розпочати відновлювальні роботи негайно після катастроф. Угода охоплює обмін інформацією, надзвичайні інспекції, аварійне відновлення. Одразу після Великого східнояпонського землетрусу такий підхід сприяв швидкій відбудові сильно пошкоджених автострад і доріг. Для допомоги службам відновлення у ліквідації наслідків катастрофи взяли участь приватні компанії. Оцінювання пріоритетних маршрутів було проведене майже одразу, екстрено розпочалися відновлювальні роботи.

Дії щодо фінансової готовності можна розглядати на кожному етапі процесу, починаючи з: а) планування підготовки до катастрофи та вироблення політики; б) раннього попередження і ранніх дій; в) реагування та відновлення; г) реконструкції об'єктів, що зазнали пошкоджень унаслідок катастрофи.

Дії згруповано в чотири компоненти:

1) дані та аналітика;
2) фінансова готовність для забезпечення своєчасності фінансування;
3) розподіл фінансових ризиків для забезпечення ефективності фінансування різних заходів реагування, відновлення;
4) виплата коштів, яка забезпечує їх затвердження, розподіл і використання для ефективного фінансування.

Це може бути підґрунтям для діагностики, визначення пріоритетів для посилення систем, які реагують на надзвичайну подію. Нерідко у багатьох країнах та системах інфраструктури вже є деякі чи багато компонентів. У окремих випадках компонентів може не бути взагалі. Наприклад, існують механізми державних фінансів, що дають змогу профільним міністерствам отримувати доступ до додаткового фінансування в надзвичайних ситуаціях шляхом або перерозподілу бюджетів, або запиту додаткових бюджетних призначень у міністерстві фінансів.

Цей підхід може ефективно працювати, але зазвичай призводить до затримок у фінансуванні та спрямування коштів з іншого планового технічного обслуговування чи інвестицій, зменшуючи тим самим стійкість у довгостроковій перспективі. Вибір фінансової політики на різних рівнях управління (наприклад, централізований та децентралізований підходи) залежатиме від політико-економічного вектора країни та ситуації у країні в цілому.

Інновації у фінансовому захисті власників та операторів інфраструктури [9].

- Гарантія на інфраструктуру катастрофи (CAT) – це фінансовий пакет, який поєднує належне фінансування O&M із заздалегідь підготовленим фінансуванням для відновлення служби критичної інфраструктури після катастроф. Цей пакет забезпечує певний взаємозв'язок між процесами фінансування повсякденного обслуговування у звичайних умовах та фінансування відновлення та продовження послуг під час і після пошкодження об'єкта, аварії, катастрофи.

Фінансовий пакет спрямований на підтримку належного утримання активів у звичайні часи та швидке відновлення критично важливих послуг державної інфраструктури, навіть після катастрофи. Гарантія інфраструк-

тури CAT може бути розроблена для різних секторів економіки, активів та власників. Конкретні види покриття небезпеки можуть бути неоднаковими, що відображає різні фактори, такі як типи активів, власники ризиків, система бухгалтерського обліку і доходи від послуг інфраструктури.

- Гарантія постачальників послуг O&M. Уряди можуть придбати послуги з ліквідації наслідків катастроф у постачальників послуг з технічного обслуговування, сплачуючи авансові або періодичні збори на додаток до звичайних зборів за технічне обслуговування. Наприклад, контракти на основі результативності, які пов'язують оплату за контрактом з показниками ефективності постачальників послуг, можуть передбачати відповідальність за аварійне відновлення як частину ключових показників ефективності (KPI).

За цими показниками (в обмін на оплату) постачальники послуг повинні забезпечувати певний рівень безперервності обслуговування навіть після серйозних катастроф (приміром, надання тимчасових послуг на баржах після обвалення мосту). Для надання таких послуг їх постачальники мають за власний рахунок переносити фінансові ризики, пов'язані з катастрофами, на страхування або ринки капіталу, щоб гарантувати виконання своїх зобов'язань після катастрофи.

- Гарантія, що реагує на шок (Shock-Responsive O&M): продукт, що фінансує ризики, може бути вбудований у наявний фонд оперативного обслуговування, щоб фонд виплат та витрат міг використати його для передачі додаткових ресурсів тому самому або іншим постачальникам послуг для відновлення активних послуг. Страхові продукти можуть бути адаптовані урядами або державними підприємствами до конкретних об'єктів інфраструктури, навіть протягом декількох років, для передачі ризиків катастрофи на страхові ринки або ринки капіталу. Цей підхід також може бути організований за рахунок періодичного бюджетного фінансування та шляхом зв'язку з умовними інструментами передачі кредиту або переказу ризику [9].

Створення систем, які реагують на шоки, перетворює неявну відповідальність на явну, якою уряд може належним чином управляти, інтегруючи її в національну стратегію фінансового захисту держави. Міністерства фінансів відіграють ключову роль у просуванні інтеграції критично важливих інфраструктурних послуг під час фінансового планування на випадок стихійних лих та катастроф, втрати певного з таких об'єктів тощо.

Розглянемо практичні кроки, які міністерства фінансів можуть зробити для інтеграції положень із захисту критичної інфраструктури в рамках відповідних національних стратегій. Необхідно наголосити на двох пріоритетах:

- Підвищення фінансової готовності уряду – щоб забезпечити наявність механізмів для пом'якшення фінансових наслідків, пов'язаних із порушенням надання критично важливих послуг, та своєчасне фінансування для відновлення.
- Захист суспільства – щоб забезпечити безперервність послуг власників та операторів критичної інфраструктури з огляду на відповідні на-

ціональні стратегії, в тому числі за допомогою політики, регулювання і механізмів фінансування, що узгоджують стимули між власниками та операторами інфраструктури.

Ключові кроки у фінансовому захисті систем критичної інфраструктури [9].

А) Оцінювання ризиків, виявлення "вузьких місць" та постановка цілей.

1. Визначення активів критичної інфраструктури.
2. Встановлення непередбачених зобов'язань, покладених на уряд за витратами на відшкодування послуг критичної інфраструктури.
3. Виявлення ризиків та чинників, котрі справляють вплив на роботу критичної інфраструктури, оцінювання умовних зобов'язань. Це передбачає розуміння факторів, що спричинили збої в роботі служб, і визначення ключових "вузьких місць", які слід подолати. Встановлення прогалин у фінансуванні. Уточнення поточних механізмів фінансування. Визначення коротко-, середньо- та довгострокових цілей і стратегії. Розподіл пріоритетів для розв'язання проблемних питань і створення короткострокового плану дій (0–5 років).

Б) Дії уряду щодо підвищення фінансової готовності держави.

1. Уточнення та забезпечення причетності до ризику. Встановлення зобов'язань держави щодо витрат на відновлення й реконструкцію на законодавчому рівні (наскільки це можливо), у тому числі визначення правил розподілу витрат між національними і місцевими урядовими органами, власниками інфраструктури та операторами, користувачами.
2. Розроблення і впровадження національної стратегії фінансування ризиків стихійних лих, яка охоплює послуги критичної інфраструктури, та її поєднання з розширеними системами управління фіскальними і критичними ризиками.
3. Забезпечення негайної ліквідності для бюджетної підтримки швидкого відновлення критично важливих послуг у надзвичайних ситуаціях, включаючи багаторівневі бюджетні та фінансові інструменти, такі як резерви, бюджети для надзвичайних ситуацій і передача ризиків, та їх пов'язаності з планами та протоколами для швидкої виплати й виконання.
4. Довгострокове фінансування реконструкції об'єктів критичної інфраструктури, наприклад, умовні кредитні угоди або державна програма страхування активів.
5. Своєчасні, ефективні механізми виконання бюджету після катастрофи, завдяки чому фінансові ресурси на кожному етапі затверджуються, розподіляються, передаються та ефективно використовуються усіма розпорядниками коштів.
6. Планування і складання протоколів на випадок надзвичайних ситуацій для швидкої виплати коштів, включаючи процедури надзвичайних закупівель, підготовку контрактів на послуги з відшкодування.

В) Дії уряду із захисту суспільства шляхом забезпечення безперервності послуг власниками та операторами критичної інфраструктури.

1. Встановлення вимог до обміну даними та розкриття інформації про ризики, оцінювання ризиків, публічне надання даних.
2. Встановлення нормативів/контрактних вимог та/або стимулів, що забезпечують мінімальну фінансову готовність, у тому числі, приміром, мінімальні стандарти страхового бюджету та бюджету надзвичайних ситуацій.
3. Встановлення регулятивних/контрактних вимог та/або стимулів щодо оперативної готовності до потрясінь, включаючи мінімальні вимоги до планування і координації дій на випадок надзвичайних ситуацій та планування ліквідації наслідків надзвичайних ситуацій і реагування на надзвичайні ситуації, або збори чи штрафи за перебої у роботі критично важливих служб відповідно.
5. Створення позитивних стимулів для довгострокового управління ризиками.

У деяких випадках доцільно зосередитися на конкретних пріоритетних секторах інфраструктури, розширюючись до інших секторів. В інших секторах варто використати наскрізний підхід, що керується централізовано. Різні функції можуть виконуватися різними міністерствами. Наприклад, пункт "Б" належить до повноважень міністерств фінансів, тоді як пункт "В" найчастіше очолюють профільні міністерства або інші державні органи. Міністерствам також слід розглянути відповідний рівень оцінювання ризиків, фінансування тощо, на якому можна зробити певні кроки, котрі залежатимуть від політичної системи країни, її економіки та масштабів, пов'язаних із розгортанням плану для великої кількості інфраструктурних активів і систем.

Тому наступним кроком має стати розроблення положень щодо фінансового захисту критичної інфраструктури в розрізі доступу до інформаційної бази. Ця сфера потребує досліджень, адже обмежена аналітичними інструментами для кількісного оцінювання умовних зобов'язань (в контексті цього положення можемо рекомендувати оприлюднювати інформацію про фінансування захисту критичної інфраструктури, якщо це не заборонено національним законодавством та не є секретною інформацію на рівні служб/міністерств безпеки, правоохоронних органів).

Такі статистичні дані варто оприлюднювати у світових базах даних (ідеться, приміром, про Євростат, сайт МВФ або національні сайти країн, що здійснюють регулювання безпеки та захисту критичної інфраструктури). Ця важлива сфера потребує дослідження для оцінювання потенційного масштабу ризиків, а отже, наслідків для стратегій захисту критичної інфраструктури, в тому числі фінансового захисту. Подальший обмін знаннями серед країн може сприяти обміну провідним досвідом у цій галузі та посиленню підходів до оцінювання фінансування захисту критичної інфраструктури.

Досвід фінансування заходів захисту критичної інфраструктури. Під захистом критичної інфраструктури розуміються заходи із забезпечення безпеки взаємозалежних систем, мереж і активів, що покладені в основу діяльності служб, життєво необхідних для функціонування суспільства.

Як приклад життєво важливої матеріальної інфраструктури можна назвати дороги, мости, аеропорти, споруди зв'язку та електростанції. Всі інші види інфраструктури неможливі без інформаційної інфраструктури, мереж, представлених насамперед системами диспетчерського управління та збору даних (SCADA), взаємопов'язаність яких дає змогу обмінюватися інформацією і проводити аналіз за всіма критично важливими функціями. До інших видів інфраструктури належать банківська сфера, виробництво і розподіл електроенергії, медичні послуги, державні аварійно-рятувальні служби, а також повітряні й наземні перевезення.

Забезпечення надійних та стійких сервісів критичної інфраструктури стає дедалі пріоритетнішим, ключовою частиною планування національної безпеки багатьох країн. У найближче десятиліття очікуються значні інвестиції у критичну інфраструктуру. Наприклад, Азійський банк розвитку підрахував, що лише країнам, які розвиваються, в Азії потрібно буде інвестувати 1,7 трлн дол. США на рік у період між 2016 і 2030 р. для підтримки зростання та зменшення бідності, швидкого будівництва інфраструктури; збільшення економічного взаємозв'язку; зростання залежності від глобальних ланцюгів поставок і телекомунікацій, нових технологій та змін у способах роботи; кліматичні зміни означають, що соціальна, економічна і фіскальна вразливість, пов'язана з критичними послугами, посилюється [9].

За даними Звіту "Global Critical Infrastructure Protection Market Size By Component, By Vertical, By Geographic Scope And Forecast" агентства "Verified market research", у 2019 р. ринок захисту критичної інфраструктури оцінювався у 131,46 млрд дол. США, і, за прогнозами, до 2027 р. досягне 217,56 млрд дол. США (рисунок). CAGR (англ. Compound annual growth rate) – сукупний середньорічний темп зростання, виражається у відсотках і демонструє, на скільки відсотків за рік відбувається приріст досліджуваного параметра (7,01 % з 2020 по 2027 р.).

Далі розглянемо витрати на захист критичної інфраструктури за секторами. Оскільки різні сектори мають свій конкретний досвід, експертні

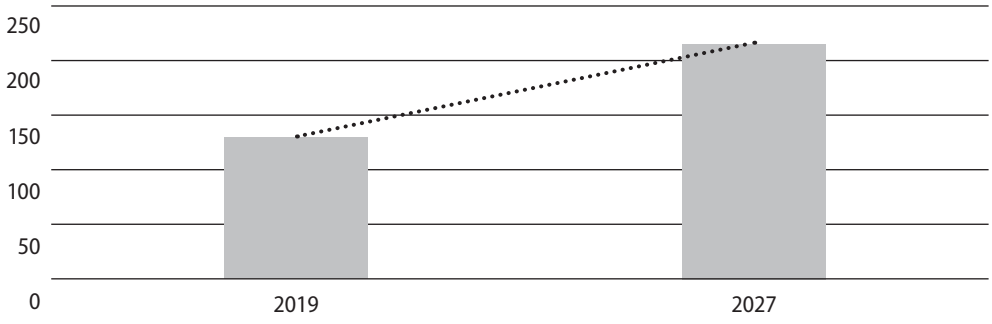

Рисунок. **Світовий ринок захисту критичної інфраструктури у 2019 та 2027 рр.**

Складено за: Critical Infrastructure Protection Market Size And Forecast / VMR. 2021. URL: https://www.verifiedmarketresearch.com/product/global-critical-infrastructure-protection-market-size-and-forecast-to-2025/.

знання і вимоги до охорони та захисту критичних інфраструктур, підхід до охорони і захисту таких інфраструктур необхідно розробляти й упроваджувати з урахуванням секторальної специфіки та наявних секторальних інструментів, зокрема на національних і регіональних рівнях, а також (в окремих випадках) на рівні транскордонних угод про взаємодопомогу між власниками/операторами критичних інфраструктур.

"Охорона та захист" означають всі види діяльності, спрямовані на забезпечення функціональності, безперервності та цілісності критичних інфраструктур з метою недопущення, зменшення наслідків і нейтралізації загрози, ризику або вразливості.

Оскільки в більшості країн критично важлива інформаційна інфраструктура здебільшого належить приватному сектору, що також займається її експлуатацією, необхідна низка динамічних рішень як відображення того факту, що нормативне регулювання не встигає за розвитком як новітніх загроз, так і технологій, необхідних для їх стримування. Тому передусім варто дослідити захист критичної інфраструктури з акцентом на кібербезпеку.

Вагомим елементом безпеки діяльності суб'єктів господарювання є політика інформаційної безпеки та заходи корпоративного або інформаційного комплаєнсу, що впроваджуються суб'єктами господарювання. Зазвичай це певна сукупність правил, вимог, оцінювання ризиків та рекомендацій, що визначають порядок інформаційної діяльності суб'єкта господарювання і особливості забезпечення безпеки його діяльності у кіберпросторі. Вказане питання набуло неабиякої актуальності починаючи з 2020 р., у зв'язку з пандемією, коли в І кварталі минулого року майже всі країни світу запровадили локдаун, внаслідок якого підприємства й бюджетні установи перейшли на дистанційний режим роботи.

Так, забезпечення інформаційної безпеки (критична інформаційна інфраструктура) залишається одним з головних пріоритетів у всьому світі з огляду на те, що спектр загроз розширюється, з'являються нові уразливості, а частота атак не зменшуватиметься. Виходячи з цього, аналітики "Canalys" прогнозують подальше зростання інвестицій у кібербезпеку. Компанія "Canalys" оприлюднила прогноз щодо розвитку ринку засобів кібербезпеки в поточному році: витрати у цій сфері збільшуватимуться на тлі зміненого в умовах пандемії IT-ландшафту. За підсумками 2020 р., витрати у сфері кібербезпеки становлять від 54,2 млрд до 54,7 млрд дол. США [11]. Ці цифри враховують витрати на Endpoint-рішення, рішення для веб-захисту та захисту даних, засоби аналітики систем безпеки і виявлення вразливостей, а також витрати у сфері мережевої безпеки та ідентифікації користувачів. До витрат належать рішення для захисту корпоративних даних, веб-захисту, мережевої безпеки, особистих даних користувачів, Endpoint-рішення та різноманітні засоби аналітики і виявлення вразливостей у системах безпеки.

Компанія "Canalys" дає два варіанти розвитку кібербезпеки – песимістичний і оптимістичний. У песимістичному сценарії витрати зростуть на 6,6 %, або до 57,7 млрд дол. США. В оптимістичному – витрати збільшаться

до 10 %, або до 60,2 млрд дол. США. Проте в будь-якому з цих двох варіантів простежується позитивна динаміка [11]. Зазначається, що в сегменті засобів веб-захисту і забезпечення безпеки електронної пошти зростання може сягнути 12,5 %. Збільшення витрат у секторі аналітики систем безпеки і виявлення вразливостей очікується на рівні 11,0 %. Витрати на Endpoint-рішення та інструменти ідентифікації можуть підвищитися на 10,4 %. Зростання у сфері мережевої безпеки очікується на 8,0 %, захисту даних – на 6,6 %.

Аналіз компанії "Canalys" свідчить, що, попри пандемію, бюджети, котрі виділяються на кібербезпеку, в цілому поки зберігають стійкість. Разом з тим згадані витрати належать до сфери малого і середнього бізнесу, а скорочення персоналу та звільнення позначилися на окремих контрактах, особливо в таких постраждалих від пандемії секторах, як роздрібна торгівля і транспорт. Проблеми в логістичних ланцюжках негативно вплинули на виконання контрактів з постачання обладнання на початку 2020 р., але згодом ситуація нормалізувалася.

Незважаючи на щораз більші витрати на забезпечення інформаційної безпеки, кількість кіберінцидентів, включаючи витоки даних та їх компрометацію, а також атаки вірусів-вимагачів (ransomware), минулого року досягла рекордного рівня. За даними "Canalys", у 2020 р. від витоків постраждали 12 млрд записів, що містять особисту інформацію, а число зареєстрованих ransomware-атак збільшилося майже на 60 %.

Найпоширенішими причинами цього аналітики називають помилки у налаштуваннях хмарних баз даних і фішингові кампанії, націлені на недостатньо захищених і погано підготовлених у плані кібербезпеки співробітників. З огляду на те, що робота й навчання в дистанційному режимі у масових масштабах тривають, а цифровізація набирає обертів, аналітики очікують збереження негативних трендів у цій сфері в 2021 р. [12].

За підсумками опитування "Gartner", проведеного у 2021 р. серед старших ІТ-керівників, головним пріоритетом у нових витратах є кібербезпека: більш ніж 61 % опитаних з 2000 р. ІТ-директорів у цьому році збільшують інвестиції в інформаційну безпеку. Послуги у сфері безпеки, включаючи консалтинг, підтримку обладнання, впровадження та аутсорсинг, являють собою найбільшу категорію витрат у 2021 р., яка оцінюється майже в 72,5 млрд дол. США. На другому місці перебувають витрати на захист інфраструктури, прогнозовані на рівні 23,9 млрд дол. США. Варто зауважити, що в цьому сегменті прогнозується найбільше зростання витрат – на 16,8 %. Третя за розміром витрат стаття – обладнання мережевої безпеки. На неї у світі буде виділено 17,0 млрд дол. США. Очікується, що витрати на обладнання мережевої безпеки порівняно з минулим роком зростуть на 8,9 % (таблиця).

З огляду на актуальність цієї теми для національної безпеки і той факт, що критично важлива інформаційна інфраструктура здебільшого належить приватному сектору, який також займається її експлуатацією, політикам та урядовцям слід допомогти таким організаціям оптимізувати наявні у них можливості щодо забезпечення кібербезпеки, ввівши додаткові

Таблиця

Інформаційна безпека та управління ризиками у світі (витрати кінцевих користувачів за сегментами), *млн дол. США*

Сегмент ринку	2020 р.	2021 р.	Зростання, %
Безпека додатків	3 333	3738	12.2
Хмарна безпека	595	841	41.2
Захист даних	2981	3 505	17.5
Управління доступом до особистих даних	12036	13917	15.6
Захист інфраструктури	20 462	23 903	16.8
Комплексне управління ризиками	4,859	5473	12.6
Обладнання мережевої безпеки	15 626	17020	8.9
Інше програмне забезпечення інформаційної безпеки	2 306	2527	9.6
Служби безпеки	65 070	72 497	11.4
Програмне забезпечення для захисту споживачів	6 507	6990	7.4
Усього	133776	150 409	12.4

Складено за: Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021. Gartner. 2021. May 17. URL: https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem?utm_source=ixbtcom.

стимули. Головними фінансовими стимулами на шляху залучення інвестицій для покращання сектору інформаційної критичної інфраструктури можуть бути:

- податкові пільги: податкові пільги, що заохочують компанії інвестувати в кіберзахист, у тому числі прискорений графік амортизації, та податкові пільги, які за впровадження зарекомендували себе як ефективні технології безпеки;
- страхування: держава могла б стимулювати ринок страхування, розробивши комплекс заходів з його підтримки;
- розсекречення більшої кількості даних про загрози: державним структурам необхідно підвищити якість і кількість даних про загрози, що надаються приватному сектору. Це означає, що державним структурам слід розсекретити більше категорій даних про загрози і активно ділитися такими даними з приватним сектором. Державним структурам варто надавати допуск до найконфіденційніших і потенційно найцінніших масивів та категорій даних про загрози набагато більшій кількості уповноважених представників компаній.

Такі стимули здебільшого призначені для пріоритетних галузей, таких як енергетика, науково-дослідні та дослідно-конструкторські роботи й проєкти з розвитку інфраструктури. Як додаток до цих секторів, стимули надаються для проєктів у різних сферах сталого розвитку або пов'язані з цілями сталого розвитку за допомогою критеріїв ефективності. На додаток до фінансових, фіскальних та регулятивних стимулів уряди можуть залучати інвесторів шляхом створення сприятливої інфраструктури навколишнього

середовища або даючи змогу інвесторам використовувати таку інфраструктуру за низької або нульової вартості.

Інфраструктурні проєкти критичної інфраструктури у 2021 р. у деяких країнах світу.

У США наявний план модернізації інфраструктури на 2 трлн дол., який допоможе створити "найстійкішу інноваційну економіку в світі". План передбачає виділення 621 млрд дол. на модернізацію транспортної інфраструктури, 400 млрд – на підтримку літніх людей та інвалідів, 300 млрд – у промисловий сектор, 213 млрд – на ремонт і будівництво доступного житла і 100 млрд дол. – на розвиток мереж широкосмугового зв'язку. План також передбачає введення нового стандарту для сфери енергогенерації з метою скорочення викидів парникових газів до нульового рівня до 2035 р. [14].

Німецький залізничний перевізник – компанія "Deutsche Bahn" (DB) планує спрямувати 12,7 млрд євро на модернізацію своєї залізничної мережі. Це найбільша сума, інвестована в залізничну інфраструктуру Німеччини, що на півмільярда євро більше, ніж було витрачено за попередній фінансовий рік. Ці інвестиції будуть спрямовані на модернізацію близько 1900 кілометрів шляхів, а також на 140 мостів і близько 2000 стрілочних переводів. Таке збільшення пропускної спроможності залізниць може сприяти мінімізації автомобільних і повітряних перевезень, що допоможе Німеччині досягти цілей із захисту клімату (це, в свою чергу, відповідає цілям сталого розвитку) [15].

Іншим цікавим прикладом може бути корпорація "ArcelorMittal", яка є одним з найбільших світових виробників сталі. Компанія інвестує 4 млн євро в "зелене" виробництво сталі на заводі в м. Айзенхюттенштадт (Німеччина). У планах "ArcelorMittal" – використання природного газу для виробництва сталі в доменній печі на підприємстві, що дасть змогу модернізувати цей завод, знизивши його потреби у вугіллі та витрати на електроенергію. Як наслідок, сталеливарний гігант скоротить викиди CO2 на 5 % на рік, починаючи з 2021 р. "ArcelorMittal" має намір перейти на "зелене" виробництво сталі до 2050 р. Підприємство планує у 2021 р. збільшити обсяги постачання "зеленої" сталі споживачам до 120 тис. т, а в 2022 р. вийти на 600 тис. т [16].

Федеральна асоціація німецьких компаній з перероблення та утилізації сталі (BDSV) виступила зі зверненням до федеральних міністерств внутрішніх справ із закликом оперативно забезпечити загальнонаціональне розширення сектору і галузеву класифікацію критично важливих інфраструктур за рахунок галузі сортування, перероблення та утилізації відходів [17].

Епідемія коронавірусу відобразила різні акценти дискусії в Німеччині щодо проблем розвитку критичної інфраструктури, і насамперед у сфері інформаційної безпеки. Стимулом стала спільна доповідь трьох федеральних відомств, що відповідають за IT-безпеку в Німеччині, в якій містилося попередження про атаки на об'єкти критично важливої інфраструктури. Федеральна розвідувальна служба (BND), Федеральне управління із захисту конституції (BfV) і Федеральне управління з інформаційної безпеки (BSI) дослідили, як діятимуть потенційні хакери [18].

Слід зауважити, що Рада ЄС схвалила висновки щодо стратегії кібербезпеки ЄС, яка окреслює план дій для захисту компаній і пересічних громадян від новітніх кіберзагроз. Стратегію у грудні 2020 р. презентували Європейська комісія та представник ЄС із закордонних справ. У висновках Рада ЄС передбачає такі кроки, як створення мережі безпекових центрів на всій території блоку, які б займалися моніторингом і могли заздалегідь помічати загрозу; визначення спільного центру з кібербезпеки, який був би головним консультаційним органом для розроблення політики.

Ідеться також про впровадження технології зв'язку 5G та заходи для її безпечності; прискорення впровадження базових стандартів інтернет-безпеки; підтримку розвитку надійного шифрування (при цьому залишаються інструменти для роботи правоохоронців); розширення співпраці з міжнародними партнерами у сфері кібербезпеки. Пропонується звернути увагу на попередження і протидію системним кібератакам, які можуть бути спрямовані на критичну інфраструктуру, демократичні інституції та процеси. З-поміж іншого пропонується створити при Розвідувально-ситуаційному центрі ЄС (INTCEN) спеціальну групу кіберрозвідки, яка б поглибила роботу відомства у цій сфері [19].

Епідемія коронавірусу і захист критично важливих інфраструктур стимулювали посилення інвестиційного контролю в зовнішньоторговельному праві Німеччини [20]. У рамках нових правил інвестиційного контролю передбачено обмін інформацією між країнами – членами ЄС та Європейською комісією на додаток до вимоги національного схвалення за 25 % участі в інвестиціях через відповідні транзакції в Європі.

Метою є скоординований контроль прямих іноземних інвестицій на всій території ЄС. Інші країни – члени Співтовариства і Комісії ЄС мають 35 днів, щоб прокоментувати плановане інвестиційне рішення. Таким чином, країни ЄС, формально не перешкоджаючи іноземним інвестиціям як таким, одночасно цілком природно створюють умови для запобігання загрозам безпеці або стимулюванню інвестицій з третіх країн у критично важливі інфраструктури і технології (оборона, енергетика, цифрова інфраструктура, водопостачання, розроблення вакцин, ліків, медичних виробів і засобів індивідуального захисту та ін.).

Розглянемо окремі аспекти захисту критичної інфраструктури, характерні для Великобританії. Британський регулятор енергетичного ринку "Ofgem" схвалив виділення компаніям 30 млрд ф. ст. (40 млрд дол. США) на модернізацію енергетичної інфраструктури в 2021–2026 рр. для переходу до екологічнішої та надійнішої енергосистеми. Регулятор зазначив, що ця сума на 20 % перевищує максимальний обсяг інвестицій, що планувався спочатку. "Ofgem" може інвестувати ще 10 млрд ф. ст. у проєкти відновлюваної енергетики, зокрема підготовку до запуску вітряних установок у Північному морі.

У листопаді було презентовано план підтримки "зелених" галузей і боротьби зі зміною клімату. Оператори енергомереж повинні підготуватися до переходу до низьковуглецевої економіки. Водночас "Ofgem" гарантуватиме, що такий перехід не призведе до зростання витрат споживачів. "Ofgem" увів п'ятирічний ціновий контроль для обмеження прибутку енергетичних компаній [21].

Великобританія виділить 160 млн ф. ст. на модернізацію портів і заводів для будівництва вітряних турбін. Серед пріоритетів – вироблення "зеленої" електроенергії для кожного будинку в країні до 2030 р. У цьому контексті планується створення 2 тис. робочих місць у будівництві та підтримка ще 60 тис. осіб. Як бачимо, модернізація такого об'єкта критичної інфраструктури передбачає й покращання соціальної сфери, адже створення робочих місць – це, відповідно, сплата податків до бюджету, а отже, здійснення належних платежів, у тому числі на соціальні потреби в країні.

У розрізі залізничних інфраструктурних проєктів зауважимо, що англійський оператор інфраструктури залізниць Великобританії "Network Rail" уклав шість рамкових контрактів загальною вартістю 750 млн ф. ст. для модернізації засобів сигналізації й телекомунікації протягом контрольного періоду (2019–2024 рр.). Контракти розподілені по країні за географічним принципом і укладені з компаніями "VolkerRail Special Businesses", "Atkins", "Linbrooke Services", "Babcock Rail", "Colas Rail" і "Siemens Mobility".

Рамкові контракти передбачають реалізацію проєктів трьох рівнів складності – від одиночних залізничних переїздів і окремих телекомунікаційних об'єктів (включаючи загальнобудівельні роботи) до заміни окремих компонентів засобів сигналізації та модернізації систем управління рухом поїздів на цілих ділянках [22].

У Великобританії стане нововведенням освітлювання доріг і вулиць за допомогою спеціального покриття без використання електроенергії. На відміну від ліхтарів та інших елементів електричного освітлення, таке покриття не потребує постійної уваги і витрат на підтримання у робочому стані. Нову технологію під назвою "StarPath", або "Зоряний шлях", розробила компанія "Nevana Designs". Завдяки цій технології також можна освітлити дороги, до яких не підведена електроенергія [23].

Розглянемо окремі приклади інфраструктурних проєктів у Франції. У листопаді 2018 р. у цій країні було оприлюднено довгострокову енергетичну програму (PPE), у рамках якої презентовані головні напрями розвитку для забезпечення енергетичної безпеки. На підтримку розвитку відновлюваних джерел енергії Франція має намір виділити до 7–8 млрд євро замість нинішніх 5 млрд. Субсидії переважно надаватимуться наземній вітроенергетиці, для якої планується потроєння потужності до 2030 р., і сонячній, чиї потужності зростуть у п'ять разів. Передбачено розроблення вітротурбін, що встановлюються на морському дні. Загалом відновлювані джерела повинні забезпечити 40 % виробництва електроенергії до 2030 р. Програма передбачає також закриття решти вугільних електростанцій до 2022 р.

Зазначимо, що в червні 2014 р. на розгляд парламенту Франції було внесено законопроєкт про зниження частки ядерної енергетики в електрогенерації із 75 до 50 % до 2025 р. і обмеження сумарної потужності діючих в країні АЕС до 63,2 ГВт. До 2035 р. повинні бути виведені з експлуатації 14 із 58 діючих ядерних енергоблоків.

У рамках розвитку та уточнення нової енергетичної програми 28 січня 2019 р. у Парижі було підписано нову тристоронню угоду між урядом і пред-

ставниками атомної промисловості, що стосується стратегії розвитку ядерної енергетики Франції на середньостроковий період 2019–2022 рр. Учасники угоди взяли на себе низку взаємних зобов'язань щодо підтримки атомної галузі країни за такими напрямами: забезпечення і збереження зайнятості в ядерному секторі; збереження навичок та забезпечення професійної підготовки персоналу; цифрова і екологічна трансформація галузі, а також питання, пов'язані з підтримкою атомної індустрії країни на міжнародному ринку. На сьогодні атомна галузь Франції охоплює 2600 підприємств (зокрема 85 % – малі та середні), які прямо або побічно забезпечують 220 тис. робочих місць, річний обіг у галузі становить близько 50 млрд євро, з яких 22 % припадає на експортні операції.

Однак, на думку багатьох експертів, значного скорочення атомних потужностей у Франції очікувати не варто, оскільки збереження високої частки АЕС в енергетиці країни необхідно для забезпечення енергетичної незалежності та безпеки об'єктів критичної інфраструктури.

Варто зауважити, як атомна енергетика може сприяти досягненню Францією кліматичних цілей, намічених у Паризькій угоді. Французька електроенергетична система на 97 % низьковуглецева. Саме завдяки ядерній енергетиці Франція має низькі викиди CO2 (5,5 т CO2/осіб/рік). Цей показник нижчий, ніж у середньому по Європі (7,4 т CO2/осіб/рік), і вдвічі нижчий, ніж у Німеччині. Це дає змогу Франції успішно боротися з глобальним потеплінням.

Франція посідає перше місце у світі за своєю енергетичною системою, що забезпечує стійкий захист довкілля. Вона вже виконує рекомендації Міжурядової групи експертів зі зміни клімату (ЮНЕП). Згідно з ЮНЕП низьковуглецева електрична група на 80 % допоможе стримати і стабілізувати глобальне потепління [24].

Одним із негативних прикладів впливу згортання фінансування на об'єкти критичної інфраструктури може бути польська державна енергетична компанія "Polish Energy Group" (PGE), яка оголосила про закриття блоків найбільшої в Європі вугільної електростанції у місті Белхатув [25]. За даними міністерства держмайна, Белхатувська ТЕС буде поступово виводитися з експлуатації з 2030 по 2036 р. Компанія також оголосила про припинення експлуатації родовищ бурого вугілля. Поточна експлуатація родовищ Белхатув і Щерцув завершиться в 2026 і 2038 рр. відповідно. У компанії зазначили, що рішення можна буде реалізувати за умови отримання підтримки ЄС. На наш погляд, компанія не усвідомлює негативних соціальних та економічних наслідків цього рішення, адже йдеться про втрату робочих місць, надходжень до бюджету тощо.

На підставі викладеного доходимо таких висновків. Захист інфраструктури життєдіяльності суспільства стає одним з ключових пріоритетів держави. Важливість безпечного функціонування критичної інфраструктури і, зокрема, її належне фінансування є чинником національної безпеки, сталого функціонування економіки, добробуту та захисту населення країни. Загалом проблему впровадження цілісної концепції та формування дієвої системи захисту критичної інфраструктури потрібно вирішувати з огляду

на загальні процеси модернізації системи забезпечення національної безпеки держави та перспективної системи адміністративного і політичного устрою держави.

Захист критичної інфраструктури розглядається в країнах ЄС як необхідна передумова розвитку масштабних інфраструктурних проєктів, залучення інвестицій для їх здійснення. І хоча зазвичай одні органи державної влади реалізують економічну політику, а інші – відповідають за забезпечення безпеки і стійкості інфраструктури, на рівні національних планів розвитку інфраструктури питання безпеки враховуються. Для України імплементація загальноєвропейських положень про захист критичної інфраструктури є важливим питанням, поряд із зобов'язаннями щодо раннього попередження надзвичайних ситуацій (пов'язаних із припиненням постачання енергоносіїв, здійсненням кібератак, стихійними лихами), які Україна вже взяла на себе в рамках Угоди про асоціацію.

У захисті критичної інфраструктури представники уряду багатьох країн вбачають інструмент, за допомогою якого можна істотно впливати на стан національної безпеки, у розрізі таких її сегментів, як кібербезпека, фінансова, енергетична безпека, наголошуючи на важливому прикладному значенні захисту критичної інфраструктури, яка дає змогу операціоналізувати національні інтереси, тобто відстежувати вплив зміни стану такої інфраструктури на ступінь досягнення цілей, що визначаються національними інтересами, а також створювати необхідні резерви фінансових та матеріальних ресурсів для реагування на кризові ситуації та ліквідації їх наслідків у державі.

Список використаних джерел

1. Climate change and energy supply and use : Technical report for the US Department of Energy in support of the national climate assessment / T. Wilbanks, D. Bilello, D. Schmalzer, M. Scott. Washington, DC : Island Press , 2013. 65 p.

2. Modelling infrastructure interdependency at a local scale: value, methodologies and challenges / S. Hasan, T. Fahim, G. Folientea, A. El-Zeinc. 21st International Congress on Modelling and Simulation (Gold Coast, Australia, 29 November to 4 December 2015). URL: https://www.mssanz.org.au/modsim2015/M4/hasan.pdf.

3. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналіт. доп. / [Д. Г. Бобро, С. П. Іванюта, С. І. Кондратов, О. М. Суходоля] / за заг. ред. О. М. Суходолі. Київ : НІСД, 2019. 224 с.

4. *Єрменчук О. П., Пальчик М. Л.* Проблемні аспекти правового регулювання державно-приватного партнерства у сфері захисту критичної інфраструктури. *Інформаційна безпека людини, суспільства, держави.* 2019. № 2 (26). С. 40–50. URL: https://doi.org/10.51369/2707-7276-2019-2-5.

5. *Бірюков Д.* Концепція захисту критичної інфраструктури як елемент загальноєвропейської безпекової політики. *ІПІЕНД ім. І.Ф. Кураса НАН України. Наукові записки.* 2013. № 6 (68). С. 106–115. URL: https://ipiend.gov.ua/wp-content/uploads/2018/07/birukov_kontseptsia.pdf.

6. *Кудряшов В. П.* Фінансове забезпечення критичної інфраструктури. *Фінанси України.* 2021. № 5. С. 111–128. URL: https://doi.org/10.33763/finukr2021.05.111.

7. *Нагорна О. В., Плаксун В. П.* Особливості фінансування інфраструктурних проектів в Україні: теорія та практика. *Молодий вчений.* 2016. № 12. С. 796–801. URL: http://molodyvcheny.in.ua/files/journal/2016/12/190.pdf.

8. Study: stock-taking of existing critical infrastructure protection activities : final report JLS/2007/D1/037 / European Commission. 2009. 492. p. URL: https://vdocuments.mx/study-stock-taking-of-existing-critical-infrastructure-protection-activities.html.

9. Financial Protection of Critical Infrastructure Services / International Bank for Reconstruction and Development, International Development Association of The World Bank. 2021. March 22. URL: https://www.financialprotectionforum.org/publication/financial-protection-of-critical-infrastructure-services.

10. Critical Infrastructure Protection Market Size And Forecast / VMR. 2021. URL: https://www.verifiedmarketresearch.com/product/global-critical-infrastructure-protection-market-size-and-forecast-to-2025/.

11. Canalys. URL: https://www.canalys.com/.

12. Инвестиции в кибербезопасность продолжат ощутимо расти. *DailyComm.* 2021. 21 янв. URL: http://www.dailycomm.ru/m/52044/.

13. Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021. *Gartner.* 2021. May 17. URL: https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem?utm_source=ixbtcom.

14. *Pramuk J.* President Biden unveils his $2 trillion infrastructure plan – here are the details. *CNBC.* 2021. March 31. URL: https://www.cnbc.com/2021/03/31/biden-infrastructure-plan-includes-corporate-tax-hike-transportation-spending.html.

15. Deutsche Bahn to spend €12.7 billion on infrastructure and digitalization. *Deutsche Welle.* 2021. March 5. URL: https://www.dw.com/en/deutsche-bahn-to-spend-127-billion-on-infrastructure-and-digitalization/a-56790038.

16. *Левчук М.* ArcelorMittal вложит €4 млн в "зеленое" производство стали в Германии. *GMK Center.* 2021. 13 янв. URL: https://gmk.center/news/arcelormittal-vlozhit-e4-mln-v-zelenoe-proizvodstvo-stali-v-germanii/.

17. Corona: Stahlrecycling als kritische Infrastruktur. *Stahleisen.de.* 2020. April 1. URL: https://www.stahleisen.de/2020/04/01/corona-stahlrecycling-als-kritische-infrastruktur.

18. *Tanriverdi H., Flade F.* Kritische Infrastruktur: Behörden warnen vor Hackerangriffen. *BR24.* 2021. July 14. URL: https://www.br.de/nachrichten/deutschland-welt/bundestagswahl-behoerden-warnen-vor-hackerangriffen,Sd3fYe6.

19. Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy / Council of the EU. 2021. March 22. URL: https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/.

20. *Dietz P., Shen Yu.* Auswirkungen der EU-Screening-Verordnung und verschärften Investitionskontrolle. 2020. November 10. URL: https://www.investmentplattformchina.de/die-neue-eu-screening-verordnung-und-verschaerfte-investitionskontrollen.

21. Ofgem gives go-ahead to a £40 billion+ investment programme for a stronger, greener and fairer GB energy system / Ofgem. 2020. December 8. URL: https://www.ofgem.gov.uk/publications/ofgem-gives-go-ahead-ps40-billion-investment-programme-stronger-greener-and-fairer-gb-energy-system.

22. Network Rail announces signalling and telecoms framework deals worth £750m. *Rail Business UK.* 2019. April 29. URL: https://www.railwaygazette.com/uk/network-rail-announces-signalling-and-telecoms-framework-deals-worth-750m/48440.article.

23. В Британии разработали технологию освещения дорог без электричества. *Центр транспортных стратегий.* 2021. 23 июня. URL: https://cfts.org.ua/news/2021/06/23/v_britanii_razrabotali_tekhnologiyu_osvescheniya_dorog_i_ulits_bez_elektrichestva_65433.

24. Франция начинает пересматривать планы по развитию энергетики. *НГ.* 2019. 11 февр. URL: https://www.ng.ru/ng_energiya/2019-02-11/9_7504_france.html.

25. EURACTIV. URL: https://www.euractiv.com/.

References

1. Wilbanks, T., Bilello, D., Schmalzer, D., & Scott, M. (2013). *Climate change and energy supply and use* (Technical report for the US Department of Energy in support of the national climate assessment). Washington, DC: Island Press.

2. Hasan, S., Fahim, T., Folientea, G., & El-Zeinc, A. (2015). Modelling infrastructure interdependency at a local scale: value, methodologies and challenges. In *21st International Congress on Modelling and Simulation* (Gold Coast, Australia, 29 November to 4 December 2015). Retrieved from https://www.mssanz.org.au/modsim2015/M4/hasan.pdf.

3. Sukhodolia, O. M. (Ed.). (2019). *Organizational and legal aspects of ensuring the security and sustainability of Ukraine's critical infrastructure.* Kyiv: NISS [in Ukrainian].

4. Iermenchuk, O. P., & Palchyk, M. L. (2019). Problematic aspects of legal regulation of public-private partnership in the field of critical infrastructure protection. *Information security of man, society, state*, 2 (26), 40–50. DOI: 10.51369/2707-7276-2019-2-5 [in Ukrainian].

5. Biriukov, D. (2013). The concept of critical infrastructure protection as an element of European security policy. *Kuras Institute of Political and Ethnic Studies of the National Academy of Sciences of Ukraine. Scientific notes*, 6 (68), 106–115. Retrieved from https://ipiend.gov.ua/wp-content/uploads/2018/07/birukov_kontseptsia.pdf [in Ukrainian].

6. Kudrjashov, V. (2021). Financial support of critical infrastructure. *Finance of Ukraine,* 5, 111–128. DOI: 10.33763/finukr2021.05.111 [in Ukrainian].

7. Nagorna, O. V., & Plaksun, V. P. (2016). Features of infrastructure projects financing in Ukraine: theory and practice. *Young Scientist,* 12, 796–801. Retrieved from http://molodyvcheny.in.ua/files/journal/2016/12/190.pdf [in Ukrainian].

8. European Commission. (2009). *Study: stock-taking of existing critical infrastructure protection activities* (final report JLS/2007/D1/037). Retrieved from https://vdocuments.mx/study-stock-taking-of-existing-critical-infrastructure-protection-activities.html.

9. International Bank for Reconstruction and Development, & International Development Association of The World Bank. (2021, March 22). *Financial Protection of Critical Infrastructure Services.* Retrieved from https://www.financialprotectionforum.org/publication/financial-protection-of-critical-infrastructure-services.

10. VMR. (2021). *Critical Infrastructure Protection Market Size and Forecast.* Retrieved from https://www.verifiedmarketresearch.com/product/global-critical-infrastructure-protection-market-size-and-forecast-to-2025/.

11. Canalys. (n. d.). Retrieved from https://www.canalys.com/.

12. DailyComm. (2021, January 21). *Cybersecurity investment will continue to grow significantly.* Retrieved from http://www.dailycomm.ru/m/52044/ [in Russian].

13. Gartner. (2021, May 17). *Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021*. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem?utm_source=ixbtcom.

14. Pramuk, J. (2021, March 31). President Biden unveils his $2 trillion infrastructure plan – here are the details. CNBC. Retrieved from https://www.cnbc.com/2021/03/31/biden-infrastructure-plan-includes-corporate-tax-hike-transportation-spending.html.

15. Deutsche Welle. (2021, March 5). *Deutsche Bahn to spend €12.7 billion on infrastructure and digitalization.* Retrieved from https://www.dw.com/en/deutsche-bahn-to-spend-127-billion-on-infrastructure-and-digitalization/a-56790038.

16. Levchuk, M. (2021, January 13). ArcelorMittal will invest € 4 million in green steel production in Germany. *GMK Center.* Retrieved from https://gmk.center/news/arcelormittal-vlozhit-e4-mln-v-zelenoe-proizvodstvo-stali-v-germanii/ [in Russian].

17. Stahleisen.de. (2020, April 1). *Corona: Stahlrecycling als kritische Infrastruktur.* Retrieved from https://www.stahleisen.de/2020/04/01/corona-stahlrecycling-als-kritische-infrastruktur.

18. Tanriverdi, H., & Flade, F. (2021, July 14). Kritische Infrastruktur: Behörden warnen vor Hackerangriffen. *BR24.* Retrieved from https://www.br.de/nachrichten/deutschland-welt/bundestagswahl-behoerden-warnen-vor-hackerangriffen,Sd3fYe6.

19. Council of the EU. (2021, March 22). *Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy.* Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/.

20. Dietz, P., & Shen, Yu. (2020, November 10). *Auswirkungen der EU-Screening-Verordnung und verschärften Investitionskontrolle*. Retrieved from https://www.investmentplattformchina.de/die-neue-eu-screening-verordnung-und-verschaerfte-investitionskontrollen.

21. Ofgem. (2020, December 8). *Ofgem gives go-ahead to a £40 billion+ investment programme for a stronger, greener and fairer GB energy system.* Retrieved from https://www.ofgem.gov.uk/publications/ofgem-gives-go-ahead-ps40-billion-investment-programme-stronger-greener-and-fairer-gb-energy-system.

22. Rail Business UK. (2019, April 29). *Network Rail announces signalling and telecoms framework deals worth £750m*. Retrieved from https://www.railwaygazette.com/uk/network-rail-announces-signalling-and-telecoms-framework-deals-worth-750m/48440.article.

23. Center for Transport Strategies. (2021, June 23). *Britain has developed a technology for lighting roads without electricity.* Retrieved from https://cfts.org.ua/news/2021/06/23/v_britanii_razrabotali_tekhnologiyu_osvescheniya_dorog_i_ulits_bez_elektrichestva_65433 [in Russian].

24. NG. (2019, February 11). *France begins to revise plans for energy development.* Retrieved from https://www.ng.ru/ng_energiya/2019-02-11/9_7504_france.html [in Russian].

25. EURACTIV. (n. d.). Retrieved from https://www.euractiv.com/.