

БЕЗПЕКА ЄВРОПЕЙСЬКОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

В. В. Магалаєс

Анотація. У статті проаналізовано сучасні підходи ЄС до забезпечення стійкості енергетичної інфраструктури в умовах гібридних загроз. Розглянуто рекомендації Ради Європи 2023 року та стратегію REPowerEU, що спрямовані на диверсифікацію джерел енергії, розвиток відновлюваних ресурсів та посилення кіберзахисту. Особлива увага приділена використанню РФ енергетики як інструменту гібридної війни проти ЄС. Проаналізовано приклади кібератак та роль політичної солідарності ЄС. Під час написання статті було використано методи контент-аналізу та порівняння, статистичний аналіз і системний підхід. Автор робить висновок, що комплексний, координаційний підхід є ключовим для забезпечення енергетичної безпеки ЄС.

Ключові слова: енергетична інфраструктура, гібридна війна, ЄС, безпека, Україна.

У світлі подій російсько-української війни, розпочатої ще в 2014 році, питання захисту енергетичної інфраструктури в країнах Європейського Союзу від зовнішніх дестабілізуючих чинників набуває особливої актуальності. Зростання складності суспільних процесів, цифровізація надання послуг та інтеграція енергетичних та комунікаційних систем, формують нові виклики для держав і міжнародних організацій у сфері управління ризиками. Особливої актуальності ці проблеми набувають у контексті захисту критичної інфраструктури держав, зокрема на тлі гібридних загроз, спричинених діями РФ, яка відкрито використовує як інформаційний тиск на країни ЄС, так і енергетичний шантаж. Огляд рекомендацій Ради Європи, а також контент-аналіз промов міністра закордонних справ Угорщини Петера Сіярто та віцепрем'єр-міністра Польщі Кшиштофа Гавковського, показали, що енергетичний сектор є стратегічним компонентом безпеки та стабільності існування Європейського Союзу. Метою статті є визначення сучасних підходів ЄС до зміцнення стійкості енергетичної інфраструктури в умовах гібридних загроз. Вивчення досвіду ЄС дозволяє осмислити ефективні практики управління ризиками, оцінити виклики та перспективи інтеграції національних систем у єдину європейську мережу безпеки, а також зробити висновки щодо підвищення стійкості держав у контексті глобальних загроз.

У сучасних умовах енергетична інфраструктура Європейського Союзу стає об'єктом нових та комплексних загроз із боку РФ, що поєднують фізичні, кібернетичні та інформаційні складові. Важливість ефективного управління ризиками для послуг енергетичної інфраструктури визначається тим, що її функціонування є пов'язаним із життєздатністю суспільства, економіки та державних інститутів всередині держав-членів ЄС. З огляду на ці виклики, рекомендації Ради ЄС щодо зміцнення стійкості критичної інфраструктури за 2023 рік відображають принциповий перехід від секторального підходу, який був закріплений у «Директиві про ідентифікацію та визначення критичної інфраструктури Європи та оцінку потреби у підвищенні її захисту № 114» від 2008 року, за якою ЄС має перейти до більш системного та інтегрованого бачення управління ризиками [1]. Документ підкреслює, що будь-яке порушення роботи критичної інфраструктури здатне створювати серйозні наслідки для безпеки громадян, економічної стабільності та політичної стійкості держав-членів ЄС, що, безумовно, у межах сучасної російської гібридної агресії залишається досі актуальним [2]. Серед конкретних заходів виділяються диверсифікація джерел постачання енергоносіїв, розвиток відновлюваних джерел енергії, створення резервних потужностей та проведення регулярних стрес-тестів для оцінки стійкості енергетичних систем. До того ж у документі особлива увага звертається на міждержавну координацію реагування, що передбачає обмін інформацією про ризики, взаємодію у кризових ситуаціях та застосування спільних протоколів управління надзвичайними подіями [3]. Отже, зазначені документи та рекомендації Ради Європи за період 2008–2022 рр., демонструють перехід від традиційної реактивної моделі забезпечення енергетичної безпеки до системного підходу, який інтегрує економічні, технологічні та безпекові аспекти. Збереження цілісності та надійності енергетичної інфраструктури є ключовим фактором підтримання політичної стабільності ЄС у майбутньому, особливо в умовах зростаючих гібридних загроз та геополітичної напруженості [2; 3].

Російська Федерація активно використовує енергетичний сектор як інструмент гібридної війни проти Європейського Союзу. Поєднуючи методи використання політичного тиску на держави-члени ЄС із масштабними ІПСО, РФ проводить пропагандистські кампанії, погрожуючи країнам ЄС можливістю «змерзнути» без їхніх енергоресурсів. Прикладом такої пропагандистської кампанії є неодноразові заяви экс-президента РФ Д. А. Медведєва, що «Європа без російського газу замерзне...» [4]. Ці дії спрямовані на дестабілізацію енергетичних систем ЄС, посилення енергетичної залежності та провокування розбіжностей серед держав-членів. До 2022 року Росія була найбільшим постачальником природного газу та нафти до ЄС, що створювало значну енергетичну залежність та можливість для РФ проводити диверсії. У 2021 році «Газпром» призупинив постачання газу через трубопровід «Ямал–Європа» задля штучного зростання ціни газу в регіоні, створюючи ситуацію енергетичної кризи [5]. Але з початком повномасштабного вторгнення та зменшенням кількості імпорту газу з боку Європи, з березня 2022 р. по березень 2023 р. кількість поставок зменшилася на 74 %, згідно з внутрішнім документом Єврокомісії. Відповідно до заяв українського видання «УНІАН»: «На тлі повномасштабного російського вторгнення в Україну чистий прибуток «Газпрому» за міжнародними стандартами фінансової звітності за 2022 рік знизився на 41 % ...» [6]. Як можна побачити зі статистики внутрішнього документу Єврокомісії за 2022–2023 рр., прибутки «Газпрому» та його вплив на енергетичну залежність Європи від Росії зменшився [6]. Слід не забувати про постійний енергетичний шантаж, що відбувається з боку члена Євросоюзу – Угорщини. До того ж цей енергетичний шантаж охоплює також питання вступу України до ЄС. Міністр закордонних справ Угорщини Петер Сіярто заявив: «Є реальність, є права і є обов'язки... Реальність полягає в тому, що в ЄС країни-члени колективно та одноголосно ухвалюють рішення про прийняття нових членів... Кожна країна має суверенне право вирішувати, звідки і яким шляхом вона купує енергоносії, необхідні їй для роботи. Ніхто ззовні не може впливати на це. Ніхто не має права нав'язувати іншій країні більш дорогі, менш безпечні джерела енергії...» [7]. Отже, з заяви топ-посадовця Угорщини можна зрозуміти: по-перше, відбувається шантаж щодо розширення ЄС, який використовують для розв'язання фінансових питань, або ж, як у цьому випадку, енергетичних. По-друге, у своїй заяві Петер Сіярто виправдовує збереження угорської залежності від російського газу й нафти, аргументуючи це економічною доцільністю та безпекою постачань, допомагаючи російським спецслужбам проводити гібридну інформаційну атаку на країни ЄС, які відмовилися від закупівлі російських енергетичних ресурсів.

Одним із важливих напрямів дестабілізації європейського регіону щодо питання енергоносіїв стало використання кіберзагроз. Росія активно здійснює кібератаки на енергетичну інфраструктуру Європи, що в останні роки проявилось у різкому збільшенні випадків втручання. Згідно з розслідуванням Брюссельської галузевої асоціації Eurelectric, у 2022 році зафіксовано 20 успішних кібератак на енергетичні об'єкти, що вдвічі більше порівняно з 2020 роком [8]. Такі атаки здатні спричинити значні перебої у постачанні енергії, економічні втрати та загрозу безпеці громадян [8]. Дії Росії безпосередньо впливають на енергетичну стійкість ЄС, послаблюючи здатність системи протистояти зовнішнім загрозам і створюючи додаткові ризики для енергетичної безпеки. У відповідь на кібератаки, Єврокомісія у 2022 році розробила стратегію REPowerEU, яка передбачає зменшення залежності від російських енергетичних ресурсів, диверсифікацію джерел енергії, розвиток відновлюваних джерел та вдосконалення інфраструктури [9]. Відповідно до стратегії, представленій Єврокомісією у червні 2025 року, ЄС планує припинити увесь імпорт російського газу та нафти до 2027 року, залучаючи до цього боротьбу з так званим «тіньовим флотом РФ», а також заходи щодо розробки відновлюваної енергії в межах країн Союзу [9]. Важливим кроком стало успішне інтегрування української енергетичної системи до європейської мережі ENTSO-E, що продемонструвало ефективність координації на міждержавному рівні та роль інституційних платформ у забезпеченні стабільності енергопостачання [10]. Як було згадано раніше, досвід окремих країн-членів ЄС, зокрема Угорщини, демонструє, що політична орієнтація держави та історично сформована енергетична залежність можуть посилювати її вразливість перед зовнішнім

тиском. Угорщина, яка довгий час покладалася на постачання російського газу та підтримувала політичний діалог із Москвою, стала прикладом того, як економічна залежність і внутрішньополітичні преференції впливають на реакцію держави у кризових ситуаціях. Цей досвід свідчить про необхідність комплексного підходу до енергетичної безпеки, який поєднує диверсифікацію джерел, розвиток внутрішніх енергетичних потужностей. Паралельно з цим ЄС активно співпрацює з міжнародними партнерами для зміцнення кібербезпеки та захисту інфраструктури від зовнішніх загроз, що дозволяє забезпечувати більш високий рівень енергетичної безпеки та протидіяти гібридним загрозам із боку Російської Федерації.

Надзвичайної актуальності стратегія REPowerEU набула на фоні російської енергетичної агресії проти України. Відповідно до видання «Про Гроші», під час так званих «блекаутів», лише за листопад 2022 року, українська енергетична інфраструктура зазнала значних пошкоджень [11]. Цілеспрямовані атаки на український енергетичний сектор у 2022–2023 роках показали, що енергетична безпека перестала бути виключно економічним або технологічним питанням і перетворилася на ключовий компонент колективної безпеки ЄС [2]. А вже в серпні 2025 року, хакери з РФ почали першу фазу нападів на енергетичну інфраструктуру країн Євросоюзу, завдавши кібератак по польським гідроелектростанціям [12]. Відповідно до видання CyberDefence24, хакери націлилися на невелику гідроелектростанцію в Поморському воєводстві, неподалік Гданська. Як зазначається у виданні: «... події серпня показали маніпуляції з параметрами працюючої електростанції, що викликає тривогу з точки зору енергетичної безпеки» [13]. У серпні віцепрем'єр-міністр Польщі Кшиштоф Гавковський повідомив, що влада запобігла кібератаці на систему водопостачання у великому місті, яка могла б відрізати доступ жителів до води. Раніше у тому ж серпні 2025 року було проведено розслідування, яке з'ясувало, що російське хакерське угруповання Secret Blizzard (підрозділ 16-го Центру ФСБ) заражало шпигунським програмним забезпеченням ApolloShadow, які використовували співробітники посольств та енергетичних підприємств всередині Польщі, що були підключеними до російських інтернет-провайдерів [13].

Підсумовуючи вищесказане, варто зазначити, що проведений аналіз гібридних загроз РФ щодо енергетичної інфраструктури ЄС підтвердив актуальність дослідження наведеного питання. Досвід 2022–2023 років підтвердив, що РФ використовує енергетичні ресурси як інструмент гібридної війни, поєднуючи атаки на енергетичну інфраструктуру України, кіберагресію, політичний тиск та інформаційну війну. Запровадження стратегії REPowerEU та ухвалення нових регламентів щодо стійкості об'єктів європейської енергетичної інфраструктури свідчать, що ЄС майже цілком готовий позбутися енергетичної залежності від РФ. Але водночас на прикладі Угорщини можна побачити, що енергетична залежність та проросійські політичні орієнтації країни можуть створювати вразливості всередині ЄС і ставати інструментом зовнішнього впливу.

Abstract. The article analyzes the European Union's current approaches to ensuring the resilience of energy infrastructure under hybrid threats. It examines the 2023 Council of Europe recommendations and the REPowerEU strategy, which are aimed at diversifying energy sources, developing renewable resources, and strengthening cybersecurity. Particular attention is paid to Russia's use of energy as an instrument of hybrid warfare against the EU. Examples of cyberattacks and the role of EU political solidarity are analyzed. In writing the article, methods of content analysis and comparison, statistical analysis, and a systematic approach were applied. The author concludes that a comprehensive, coordinated approach is key to ensuring the EU's energy security.

Keywords: energy infrastructure, hybrid warfare, EU, security, Ukraine.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance). *EUR-LEX*. URL: <https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng>
2. European Commission. Critical infrastructure resilience at EU-level. *DG HOME – Protection of critical infrastructure and resilience of critical entities*. URL: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en
3. Commission takes first step to strengthen the EU's energy security framework. *European Commission*. 2025. URL: https://commission.europa.eu/topics/preparedness_en

4. Медведев заявил, что Европа замерзнет без российского газа. *Internet Archive*. URL: <https://web.archive.org/web/20241227190750/https://www.gazeta.ru/politics/news/2024/11/23/24453193.shtml>
5. Росія призупинила постачання газу до Європи: ціни знову зросли. *Слово і діло*. 22.12.2021. URL: <https://www.slovoidilo.ua/2021/12/22/novyna/svit/rosiya-pryzupynyla-postachannya-hazu-yevrovy-cziny-znovu-zrosly>
6. В Угорщині шантажують Україну членством у ЄС через зупинку транзиту російського газу. *УНАН*. URL: <https://www.unian.ua/economics/energetics/dohodi-rosiji-vid-eksportu-gazu-do-yevrosoyuzu-obvalilisya-u-visim-raziv-ft-12270540.html>
7. Корж А. Припинення транзиту газу – Угорщина шантажує Україну членством в ЄС. *Телеграф*. 9.01.2025. URL: <https://news.telegraf.com.ua/ukr/politika/2025-01-09/5893447-roznilisya-prorosiyanskiy-uryad-ugorshchini-shantazhue-ukrainu-chlenstvom-v-es-cherez-zupinku-tranzitu-gazu>
8. Eurelectric: A snapshot of Cybersecurity in the EU. *URelectric.org*. URL: urelectric.org/wp-content/uploads/2024/11/A-Eurelectric-snapshot-of-Cybersecurity-2024-11-18-FINAL.pdf
9. REPowerEU – енергетична політика ЄС. *Європейська Комісія*. URL: https://commission.europa.eu/topics/energy/repowereu_en
10. Europe's energy security after the Russia-Ukraine war: a call for pragmatic action. *EIIR*. 04.04.2023. URL: <https://www.eiir.eu/strategic-affairs/energy-security/europes-energy-security-after-the-russia-ukraine-war-a-call-for-pragmatic-action/>
11. Як довго тривав перший блекаут в Україні у 2022 році. *ПроГроші*. URL: <https://progroshi.news/news/industri/2022-vs-2023-yak-dovgo-trivav-pershiy-blekaut-y-do-chogo-gotuvatisya-ukrajincyam-teper-10961.html>
12. Russian Hackers Attack Hydroelectric Power Plant in Poland. *Militaryni*. URL: <https://militaryni.com/en/news/russian-hackers-attack-hydroelectric-power-plant-in-poland/>
13. Russian Security Service Infected Foreign Embassies' Devices With Spy 'Virus'. *Militaryni*. URL: <https://militaryni.com/en/news/russian-security-service-infected-foreign-embassies-devices-with-spy-virus/>

УДК 327:17:316.77

ЕТИЧНІ ДИЛЕМИ ВИКОРИСТАННЯ ГУМОРУ В МІЖНАРОДНІЙ ПОЛІТИЧНІЙ КОМУНІКАЦІЇ

Л. О. Мартинюк, І. Г. Лебідь

Анотація. У статті досліджено значення гумору в міжнародній публічній комунікації. Особливу увагу приділено етичним дилемам, пов'язаним із використанням гумору в глобальних політичних повідомленнях, підкреслюється його подвійна роль як інструменту переконання та потенційного джерела шкоди. Проаналізовано та представлено кейси застосування гумору, зокрема, сатири, іронії та сарказму, політиками та дипломатами. Методологія дослідження має в основі індуктивно-дедуктивний метод, метод кейсів і метод політичного прогнозування.

Ключові слова: гумор, гумор у політиці, міжнародна політична комунікація, етичні дилеми.

Вступ. Гумор стає дедалі популярнішим інструментом у міжнародній політичній комунікації. В епоху домінування цифрових технологій тривалість уваги аудиторії обмежена, а новини миттєво поширюються через кордони. Дипломати й політики використовують сарказм, сатиру та меми, щоб привернути увагу, переосмислити проблеми та вплинути на іноземну аудиторію. Гумор може зробити лідерів більш зрозумілими, спростити складні питання та навіть посилити м'яку силу.

Водночас те, що імпонує одній аудиторії, може образити іншу, а жарти можуть стимулювати діалог і одночасно загострювати напругу або поширювати оманливі наративи. Гумор може бути цінним інструментом переконання та дипломатії, але у разі недоречного використання він може призвести до появи етичних ризиків.

Гумор у політиці є ключовим елементом наукових досліджень С. Баранової, С. Денисюк, В. Ігнатенко, І. Калініченко, С. Косенко, К. Ластовки, З. Осіпової, В. Самохіної. С. Басу та Г. Мальмвіг у своїх роботах приділяють увагу етичним складовим політичного гумору. Г. Браун, А. Лягуша, А. Кулкарні, Х. Магар, З. Махмуд акцентують увагу на гуморі, як на інструменті міжнародної політичної комунікації.

Метою статті є виявити етичні дилеми використання гумору в міжнародній політиці, дослідити найбільш поширені контраверсійні аспекти політичного гумору, можливі негативні наслідки жартів для міждержавних відносин і міжкультурного діалогу.