ЕКОНОМІЧНІ НАУКИ

УДК 338.242.4+004.056

ЗАХОДИ ЕКОНОМІЧНОЇ ПОЛІТИКИ: ГАЛУЗЕВІ ПРОБЛЕМИ ТЕПЛОПОСТАЧАННЯ УКРАЇНИ КРІЗЬ ПРИЗМУ ГАРМОНІЗАЦІЇ ВІДНОСИН ВЛАСНОСТІ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Зиза О.О., Григоренко Р.О.
Донецький національний університет економіки і торгівлі
імені Михайла Туган-Барановського

У статті розглядається необхідність формування конкурентного середовища у галузі теплопостачання України. Доводиться існування кризового становища галузі і обґрунтовується зміна відносин власності для його подолання. В межах реформування галузі також розглядається її кібербезпека. Обґрунтовується необхідність оперативного реагування на загрози інформаційній безпеці галузі як об'єкту критичної інфраструктури. Досліджено заходи економічної політики щодо формування інформаційної безпеки та реформування відносин власності галузі теплопостачання.
Ключові слова: теплопостачання, економічна політика, кібербезпека, конкуренція, власність.

Постановка проблеми. Галузь теплової енергетики України перебуває сьогодні у кризовому становищі, що негативно впливає на рівень енергетичної і національної безпеки країни. Основні фактори, котрі мають вагомий вплив на кризову ситуацію у галузі – це зношений стан об'єктів теплової енергетики, застарілий житловий фонд, що спричиняє великі втрати тепла при виробництві, споживанні і транспортуванні. Недосконале законодавство та система ціноутворення значно стримують заходи щодо підвищення енергоефективності. Нестача інвестиційних коштів для модернізації основних фондів теплової енергетики та житлового фонду не дозволяє реалізувати сучасні технології в цій сфері. Як результат якість забезпечення населення і промисловості тепловою енергією є наднизькою, часто зустрічаються відключення споживачів від гарячого водопостачання, температура в житлових приміщеннях знижується нижче встановлених норм, в окремих містах відбуваються навіть системні кризи, які призводять до порушення роботи системи життєдіяльності населення.

Тому назріває необхідність реформування економічних відносин в галузі заходами економічної політики. Зокрема підтримку конкурентних відносин, які можуть встановитися у разі гармонізації прав власності.

Крім того, реалізація економічної політики в галузі теплопостачання відбувається через забезпечення країни, як економічного суб'єкта, тепловою енергією, тим самим опосередковано забезпечення соціально-економічної стабільності і гідного рівня життя населення, тобто національної безпеки загалом. В межах останньої гостро стоїть проблема підтримки інформаційної її складової. Адже сфера теплової енергії належить до об'єктів критичної інфраструктури держави.

Аналіз останніх досліджень і публікацій. Питанням реформування галузі теплопостачання присвячено чимало досліджень, зокрема слід виділити доробок Шевцова А.І., Бараннік В.О., Земляного М.Г., Ряузової Т.В. [1], Гелетухи Г.Г. [3]. Щодо дослідження інформаційної безпеки даної галузі як об'єкту критичної інфраструктури, то вони переважно несуть інформаційний характер.

Виділення невирішених раніше частин загальної проблеми. Галузь теплопостачання вимагає реформування, а також є об'єктом критичної інфраструктури, захист кібербезпеки якого є надзвичайно важливим та актуальним питанням на даному етапі. Тому важливо комплексно дослідити ситуацію у даній галузі.

Формулювання цілей статті. Метою дослідження є провести, оцінити можливість впровадження конкурентних відносин у даній галузі задля покращення рівня ефективності її функціонування, а також проаналізувати стан інформаційної безпеки галузі теплопостачання в Україні.

Виклад основного матеріалу дослідження. Галузь теплопостачання це частина енергетичного сектору економіки України. Наразі в Україні наявні наступні системи теплопостачання:

- об'єкти генерації теплової енергії (ТЕЦ, ТЕС, АЕС, централізовані опалювальні котельні, промислово-опалювальні котельні окремих підприємств, вторинні енергоресурси, нетрадиційні та відновлюваніджерела енергії);
- об'єкти передачі і розподілу теплової енергії споживачам(магістральні теплові мережі, теплові пункти, місцеві розподільчі мережі);
- система управління і регулювання постачання теплової енергії.

Основними споживачами теплової енергії є житлово-комунальний сектор (44%), промисловість (35%) та інші галузі економіки (близько 21%) [1].

Через те, що ринок теплопостачання в Україні весь час свого існування знаходиться в монополістичний системі, це сприяло появі неефективного законодавчого регулювання даної галузі та постановці таких проблемних питань, як:

- відсутність умов для створення конкуренції у сфері теплопостачання;
- високі ціни на теплову енергію;
- зношеність основних фондів, високі втрати, низька ефективність;

Таблиця 1

Особливості функціонування ринку теплової енергії в окремих країнах ЄС

Країна	Ринок теплової енергії без тарифного регулювання		
	Опис ринку	**Орган нагляду**	**Особливості тарифів/цін**
Німеччина	Тарифи на теплову енергію не регулюються, а формуються на конкурентному ринку. Законодавство в секторі: Закон "Про стимулювання ВДЕ в секторі теплової енергії"; Постанова "Про загальні умови постачання тепла".	Загальний нагляд: *Департамент з питань конкуренції*. Федеральне агентство Bundesnetzagentur виконує регулювання *тільки* в секторі електричної енергії та природного газу.	Стандартної методики встановлення тарифів на теплопостачання немає.
Великобританія	Тарифи на теплову енергію встановлюються самими виробниками на конкурентному ринку теплової енергії. При цьому постачальники *не зобов'язані* публікувати дані про ціни або розкривати цю інформацію будь-якій третій стороні.	Загальний нагляд: *Департамент з питань конкуренції та ринків*. Управління ринків газу та електроенергії (неміністерський урядовий підрозділ та незалежний *регуляторний орган*) відповідає за реалізацію державного механізму стимулювання виробництва теплової енергії.	Уряд *стимулює виробництво тепла*.

Джерело: [2]

· недостатність власних фінансових ресурсів підприємств;

· відсутність стимулів для підвищення ефективності виробництва.

· Існування бар'єрів для доступу до тепломереж незалежних виробників.

· відсутність/ недостатність інвестицій, як наслідок недосконалості існуючих механізмів тарифоутворення («собівартість +6%) [3].

Для обґрунтування необхідних, на нашу думку, змін у даній галузі слід звернутися до зарубіжного досвіду.

Аналізуючи таблицю 1 можна зробити висновки, що конкурентний ринок в галузі теплопостачання – досить обґрунтована та перспективна ідея. Котра дає змогу державі повністю або частково відійти від регулювання даної сфери та спрямувати всі свої ресурси в інші напрями.

Вагома кількість країн Європейського Союзу ввели прозорий механізм приєднання незалежних виробників до тепломереж, таким чином зменшивши дискримінаційну політику в даній галузі. Загалом в Європейських країнах можна виділити чотири основні типи власності на об'єкти комунальної теплоенергетики:

· повністю знаходяться у державній власності;

· повністю знаходяться у приватній власності;

· змішана форма власності та управління – державно-приватна;

· неприбуткові кооперативи у комунальній власності.

Аналіз наявних даних свідчить про тенденцію приватизації систем централізованого теплопостачання, як у західноєвропейських країнах, так і у Центральній та Східній Європі. На сьогодні в різних країнах ЄС частка приватних форм власності в цьому секторі складає близько 40% [2].

В Україні цей показник знаходиться близько мінімуму, та об'єкти комунальної теплоенергетики знаходяться повністю у державній власності. І тому тут існує наступна ситуація в сфері теплопостачання: (див. рис. 1).

Як видно з рисунку 1, дана сфера повністю монополізована державою – це забезпечує ефективну політику безпеки, але знижує рівень функціонування підприємств, через недостатню мотивацію до покращення наданих послуг.

На рисунку два можна спостерігати ситуацію, в котрій буде перебувати ринок при переході до конкурентного типу ринку. В такому випадку відбуваються структурні зміни у власності підприємств. З введенням цієї системи у сфері надання послуг теплопостачання з'являється можливість для функціонування приватних підприємств, що сприяє покращенню рівня якості наданих послуг та росту ефективності використання паливно-енергетичних ресурсів.

Опосередковано дану мету переслідує і Концепція реалізації державної політики у сфері теплопостачання, прийнята у серпні 2017 року, а саме «надійне забезпечення споживачів послугами з теплопостачання, забезпечення енергетичної незалежності та безпеки України; зменшення негативного впливу на навколишнє природне середовище, поліпшення фінансово-економічного стану підприємств, запровадження прозорої ефективної системи розрахунків між споживачем та надавачем послуг, створення умов та стимулювання залучення інвестицій у сфері теплопостачання» [4].

Рис. 1. Існуюча ситуація на ринку теплопостачання України [3]

Рис. 2. Ситуація після впровадження конкурентного ринку тепла [3]

Звичайно, наявність приватної власності сприяє розвитку галузі, проте, якщо торкнутися питання інформаційної безпеки галузі теплопостачання, то основна загроза тут криється у кібербезпеці даної галузі як об'єкту критичної інфраструктури держави. Для підтвердження у 1 півріччі 2017 року найбільше атак було здійснено на 43,4% комп'ютерів енергетичних компаній (в той час як в середньому за іншими галузями це співвідношення складає 31,2%). А також на енергетику та комунальні служби здійснювалося відповідно 4,9% і 3,9% усіх атак [5].

Тому ми вважаємо, що повністю передати у приватні руки підприємства галузі небезпечно саме з точки зору інформаційної безпеки. Оскільки саме держава несе відповідальність за безпеку об'єктів критичної інфраструктури і повинна тримати усі важелі впливу особливо у інформаційній частині даного питання.

Тому, на нашу думку, своєчасним є прийнятий у жовтні 2017 року Закону України «Про основні засади забезпечення кібербезпеки України» [6]. У цьому документі зазначається, що «відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог законодавства, за невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об'єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури».

Крім того Розпорядженням Кабінету Міністрів України від 6 грудня 2017 року було схвалено Концепцію створення державної системи захис-

Таблиця 2

Особливості забезпечення інформаційної безпеки критичної інфраструктури в окремих країнах ЄС

Країна	*Інформаційна безпека критичної інфраструктури*		
	Законодавчі акти	**Органи регулювання**	**Випадки загроз і середній збиток**
Німеччина	«Стратегія кібербезпеки для Німеччини» (Cyber Security Strategy for Germany) Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту від 08.12.2008 № 2008/114/ЄС, Європейський Союз Директива ЄС щодо мережі та інформаційних послуг (NIS)	Федеральний офіс інформаційної безпеки Міністерства внутрішніх справ (Bundesamt fьr Sicherheit in der Informationstechnik, BSI) Національнй центр кіберреагуваня (Nationales Cyber-Abwehrzentrum, NCAZ) Національна рада кібербезпеки Федеральної асоціації інформаційних технологій і нових засобів комунікації (BITKOM) Альянс за кібербезпеку (Alliance for Cyber Security)	Влітку 2017 року група хакерів здійснила атаку на компанію «NetCom BW» – регіонального телекомунікаційного провайдера, який надає послуги 43 тис. чоловік у федеральній землі Баден-Вюртемберг на південному заході Німеччини, що є дочірньою компанією «EnBW» – однією з найбільших енергетичних компаній Німеччини. Середній збиток на компанію 7,84 млн. дол.
Великобританія	«Стратегія кібербезпеки для Великобританіїї» (Cyber Security Strategy for Great Britain) Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту від 08.12.2008 № 2008/114/ЄС, Європейський Союз Директива ЄС щодо мережі та інформаційних послуг (NIS)	Управління кібербезпеки (OCS) в структурі Кабінету міністрів Оперативний центр кібербезпеки (CSOC) Центр захисту національної інфраструктури (CPNI) Служба швидкої комп'ютерної допомоги (CERT service) Національний центр кібербезпеки (NCSC) при GCHQ (Government Communications Headquarter; Центр урядового зв'язку)	В травні 2017 року шкідливе ПЗ під назвою WannaCry поширилося по всьому світу. Вірус-вимагач блокував комп'ютери і вимагав за повернення доступу $ 600 в біткоіни. Постраждала зокрема Національна система охорони здоров'я (NHS) Великобританії. Середній збиток на компанію 7,21 млн. дол.

Джерело: [10–16]

ту критичної інфраструктури, що має сприяти забезпеченню позитивних змін у мінімізації зокрема кіберзагроз даним об'єктам [7].

У Законі і у Концепції обґрунтовується і передбачається розробка переліку об'єктів критичної інфраструктури, куди мають ввійти і підприємства теплопостачання. Адже з п'яти груп об'єктів критичної інфраструктури конкретно можна ознайомитися лише із переліком підприємств, що мають стратегічне значення для економіки і безпеки держави (цей перлік затверджений іще у 2004 році, а у 2015 році він перетворився на Перелік об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держав) [8]. А, як відомо, з економічної і правової практики чим глибше розроблено (деталізовано) законодавство, тим краще воно працює.

Оскільки реалізувати Концепцію уряд планує через прийняття законів і нормативно-правових актів у короткостроковій перспективі. А орган, що буде відповідати за координацію захисту даних об'єктів у 3-5 років. Функціонування системи має бути налагодженим до 2027 року. Проте строк цей досить дискусійний, виходячи із поточного стану справ і постійних загроз, що виникають. Тому Міністерство інфраструктури створило генеральний секретаріат цифрової інфраструктури і державне підприємство, що буде займатися питаннями кібербезпеки [7; 9].

Дані тенденції відповідають стану та тенденціям Європейського простору. У таблиці 2 представлено особливості забезпечення інформаційної безпеки критичної інфраструктури в даному регіоні.

У порівнянні із визначеним органами в Україні згідно із Законом «Про основні засади забезпечення кібербезпеки України» суб'єктами забезпечення кібербезпеки є [6]:

- Президент України через очолювану ним Раду національної безпеки і оборони України;
- Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України;
- Кабінет Міністрів України.

А також суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки [6].

Відтак нагальною є проблема створення спеціальних органів, що відповідають за кібербезпеку. Тому дії Мінінфраструктури є своєчасними.

Висновки з даного дослідження і перспективи. Отже, проаналізувавши наявні дані, можна зробити висновок, що сфера теплопостачання в Україні знаходиться в стані занепаду. Причинами цього частково стали відсутність конкуренції та мотивації до покращення своїх послуг. Тому одним із заходів економічної політики держави є впровадження конкурентних відносин в даній галузі. Це стане позитивним чинником як для розвитку послуг теплопостачання, так і ресурсного потенціалу країни в цілому. Та перед докорінною зміною структури ринку необхідно провести низку підготовчих та підтримуючих реформ, зокрема у сфері інформаційної безпеки даної галузі як об'єкту критичної інфраструктури держави. Лише у цьому випадку вони будуть сприяти безболісному переходу до нової практики у всій сучасній історії України.

Список літератури:

1. Стан та перспективи реформування системи теплозабезпечення в Україні / А.І. Шевцов, В.О. Бараннік, М.Г. Земляний, Т.В. Ряузова. – 2010. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.db.niss.gov.ua/docs/energy/Teplozabezpechennya.pdf.
2. Проект USAID муніципальна енергетична реформа в Україні. – 2016.
3. Гелетуха Г.Г. Перспективи впровадження конкурентного ринку теплової енергії в Україні / Г.Г. Гелетуха. – 2016. [Електронний ресурс]. – Режим доступу до ресурсу: http://biomass.kiev.ua/images/projects/general/pdf/2-Geletukha-B4B-3rd-seminar.pdf.
4. Концепція реалізації державної політики у сфері теплопостачання [Електронний ресурс]. – Режим доступу до ресурсу: http://zakon2.rada.gov.ua/laws/show/569-2017-%D1%80.
5. Kaspersky Lab ICS Cert выпустил отчет об угрозах для систем промышленной автоматизации [Електронний ресурс]. – Режим доступу до ресурсу: http://digitalsubstation.com/blog/2017/10/04/kaspersky-lab-ics-cert-vypustil-otchet-ob-nbsp-ugrozah-dlya-sistem-promyshlennoj-avtomatizatsii/.
6. Закон України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – Режим доступу до ресурсу: http://zakon0.rada.gov.ua/laws/show/2163-19.
7. Концепція створення державної системи захисту критичної інфраструктури [Електронний ресурс]. – Режим доступу до ресурсу https://www.kmu.gov.ua/ua/npas/pro-shvalennya-koncepciyi-stvorennya-derzhavnoyi-sistemi-zahistu-kritichnoyi-infrastrukturi.
8. Перелік об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держав [Електронний ресурс]. – Режим доступу до ресурсу: http://zakon2.rada.gov.ua/laws/show/83-2015-%D0%BF.
9. Мининфраструктуры создало предприятие для обеспечения кибербезопасности [Електронний ресурс]. – Режим доступу до ресурсу: https://delo.ua/special/mininfrastruktury-sozdalo-predprijatie-dlja-obespechenija-kiberb-336722/.
10. Киберготовность Германии 2.0: Национальная стратегия [Електронний ресурс]. – Режим доступу до ресурсу: https://digital.report/kibergotovnost-germanii-2-0-natsionalnaya-strategiya.
11. Atlantic: Критическая инфраструктура Германии оказалась под угрозой [Електронний ресурс]. – Режим доступу до ресурсу: https://regnum.ru/news/2426126.html.
12. Инфографика: Самые подготовленные и уязвимые страны к кибератакам [Електронний ресурс]. – Режим доступу до ресурсу: https://bcs-express.ru/novosti-i-analitika/infografika-samye-podgotovlennye-i-uiazvimye-strany-k-kiberatakam.
13. Directive Security of Network and Information Systems (NIS) [Електронний ресурс]. – Режим доступу до ресурсу: https://www.baesystems.com/en/cybersecurity/feature/security-of-network-and-information-systems-directive.
14. Бенджамин С. Бакленд. Демократическое управление и вызовы кибербезопасности / Бенджамин С. Бакленд, Фред Шрайер, Теодор Х. Винклер. – Женева: Женевский центр демократического контроля над вооруженными силами, 2013.

15. Дайджест информационной безопасности – Итоги 2017 [Електронний ресурс]. – Режим доступу до ресурсу: https://rvision.pro/blog-posts/dajdzhest-informatsionnoj-bezopasnosti-itogi-2017.
16. Directive 2008/114/EC – identification and designation of European critical infrastructures and assessment of the need to improve their protection [Електронний ресурс]. – Режим доступу до ресурсу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ajl0013.

Зыза О.О., Григоренко Р.А.
Донецкий национальный университет экономики и торговли
имени Михаила Туган-Барановского

МЕРЫ ЭКОНОМИЧЕСКОЙ ПОЛИТИКИ: ОТРАСЛЕВЫЕ ПРОБЛЕМЫ ТЕПЛОСНАБЖЕНИЯ УКРАИНЫ СКВОЗЬ ПРИЗМУ ГАРМОНИЗАЦИИ ОТНОШЕНИЙ СОБСТВЕННОСТИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация
В статье рассматривается необходимость формирования конкурентной среды в отрасли теплоснабжения Украины. Доказывается существование кризисного состояния отрасли и обосновывается изменение отношений собственности для его преодоления. В рамках реформирования отрасли также рассматривается ее кибербезопасность. Обосновывается необходимость оперативного реагирования на угрозы информационной безопасности отрасли как объекта критической инфраструктуры. Исследованы меры экономической политики по формированию информационной безопасности и реформирования отношений собственности отрасли теплоснабжения.
Ключевые слова: теплоснабжение, экономическая политика, кибербезопасность, конкуренция, собственность.

Zyza O.O., Hrihorenko R.O.
Donetsk National University of Economics and Trade
named after Mykhailo Tugan-Baranovsky

ECONOMIC POLICY MEASURES: INDUSTRIAL PROBLEMS OF HEATING SUPPLYING OF UKRAINE THROUGH THE PRIZM OF PROPERTY RELATIONSHIP HARMONIZATION AND INFORMATION SECURITY

Summary
The article considers the necessity of forming a competitive environment in the heat supply sector of Ukraine. The existence of the crisis in the industry is proved and the property relations changing for its overcoming is substantiated. As part of the industry reform, its cyber security is also considered. The necessity of prompt response to the industry information security threats as the critical infrastructure object is substantiated. The economic policy measures on information security formation and reformation of heat supply sector ownership relations are studied.
Keywords: heat supply, economic policy, cybersecurity, competition, property.