УДК: 94:316.774(061.1ЄС)
http://doi.org/10.46869/2707-6776-2024-26-4

Зернецька О.В.
https://orcid.org/0000 0002 6686 6267

ПІДВОДНІ ТЕЛЕКОМУНІКАЦІЙНІ КАБЕЛІ В КОНТЕКСТІ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

У статті вирішується проблема функціонування підводних телекомунікаційних кабелів в контексті безпеки Європейського Союзу. Стверджується, що важливість підводних кабелів зменшена у масовій свідомості, але зараз підводні телекомунікаційні кабелі несуть 99% інформації і даних, починаючи від дипломатичних, політичних, фінансових до економічних, соціальних, культурних сфер життя.

Метою статті є дослідження проблем безпеки пов'язаних з розвитком і експлуатацією підводних кабелів в ЄС, що константує одну з головних геополітичних проблем.

Доводиться, що Інтернет повністю залежить від підводних кабелів. Глобальна комунікація, яка існує зараз, неможлива без підводних кабелів. Її безпека повністю залежить від них. Тому що кабелі прокладені на дні морів і океанів, пролягають через національні кордони і часто закопані у землю, про них часто забувають і політики, надаючи їм замало уваги.

Увага політиків до безпеки підводних кабелів почала збільшуватися з 2014 р., коли російські підводні човни почали свої розвідки у Північній Атлантиці, де прокладені підводні кабелі. Геополітичні хвилі посилилися у 2022 р., коли розпочалася російсько-українська війна, і уразливість морських інфраструктур почала привертати як громадську увагу, так і увагу політиків. У статті висвітлено важливість підводних кабелів через їх глобальну пов'язаність, роль у диджитальній економіці та воєнних операціях.

Зроблено висновок, що Україна як морська держава після повернення Криму та інших приморських територій матиме доступ до підводних телекомунікаційних кабелів, які будуть покладені по дну Чорного моря. Це ще більше наблизить Україну до співпраці з ЄС та приєднання до цієї регіональної організації.

Ключові слова: *підводні телекомунікаційні кабелі, глобальна мережа, безпека, стійкість, Європейський Союз, Україна.*

Нині передача інформаційних даних на 99% відбувається за допомогою підводних телекомунікаційних кабелів. І лише 1% через супутниковий зв'язок [1]. Трансфер фінансових операцій (приблизно 10 трлн. дол на рік), політична, економічна і подекуди інформація в галузі культури передаються завдяки підводним кабелям. Швидкість, яку забезпечують оптичні волокна, надійність, економічність дає змогу спеціалістам припускати, що пропускна здатність кабелів буде подвоюватись кожних 2 роки. Проте у підводних кабелів є уразлива сторона – це не застрахованість від зовнішнього втручання. Тому науковці, політики експлуатаційники давно працюють над проблемою нормального безпечного функціонування підводних кабелів. Починаючи з 2017 р. особлива увага до цієї роблеми була приділена в статтях Р. Сунака, П. Паганіні, К. Бергера, Т. Лібетрау, Дж. Франкена, К. Фрейзера, П. Менона, Т. Вестбрука, А. Ботті, П. Марчета, В. Персика, А. Пескапе, а також в матеріалах і документах ЄС, підпорядкованих їм організацій та інституцій.

Глобальна комунікація, яка відбувається за допомогою підводних телекомунікаційних кабелів та її безпека, - це не тільки питання техніко-технологічне, а й геополітичне й безпекове. Дослідження історії ровитку перших підводних транснаціональних кабелів - спочатку – трансатлантичних, а згодом транстихоокеанських проведено у нашій статті «До історії розвитку комунікацій: перші міжконтинентальні зв'язки», (2016 р.) [2]. Вперше у вітчизняній науці нами системно було досліджено початок електричного міжконтинентального зв'язку в історії розвитку комунікацій, що охоплює період із середини XIX ст. до початку XX ст. або кінця Першої світової війни. Особлива увага була приділена використанню телеграфу Британською імперією, котра першою у світі проклала трансатлантичний та транстихоокеанський підводні телеграфні кабелі. США були другими у цьому змаганні. Це означало, що ці країни здолали останній бар'єр на шляху до створення світових комунікації у XX ст. Системно дослідивши на міждисциплінарному рівні вплив телеграфу, телефону, радіо на реконфігурацію системи міжнародних відносин на першому етапі міжконтинентальних зв'язків з середини XIX ст., ми дійшли висновку про безперечний вплив означених комунікацій не тільки на розвиток комерції та дипломатії провідних колоніальних держав, але й на перебіг Першої світової війни, де вони були активно задіяні як нові тактичні та стратегічні воєнні ресурси. Вперше у воєнній практиці застосовувалися передача повідомлень телеграфом, телефоном і радіо, перехоплення ворожих повідомлень, злам шифрів та розшифрування, дезінформація ворога тощо, які увійшли у воєнну науку та практику під назвами «телеграфна війна» та «телефонна війна». Проведене дослідження дало змогу концептуалізувати теоретичні положення та висновки про реконфігурацію системи міжнародних відносин в цей період і не тільки про зміну політичної карти Європи, а й зміни світового порядку [2, с. 194-195].

Відтоді минуло 100 років, які були позначені стрімким розвитком підводних телекомунікацій. Вони зараз оперезують всю земну кулю. Змінилися техніко-технологічні властивості підводних кабелів: від коаксіальних кабелів перейшли до використання оптоволоконних, які покращують передачу сигналу, його швидкість, якість і обсяг даних, що ними передається.

Ми вважаємо, що проблему безпеки підводних комунікаційних кабелів необхідно розглядати в контексті розвитку диджитальної (цифрової) економіки і диджитального суверенітету, а, можливо й ширше – в контексті створення штучного інтелекту. Мережа підводних кабелів — центральна критична інфраструктура диджитальної ери. Ця мережа створена з оптоволоконних кабелів, які прокладені на дні морів і океанів і пов'язують країни усього світу. Це кабелі, які часто мають довжину в тисячі кілометрів, передають великі об'єми даних через глобальну кабельну мережу.

Підводні кабелі є основою глобальної економіки. Завдяки ним відбувається майже 10 трилiонів фінансових транзакцій щодня. В світі налічується більше,

ніж 400 активно задіяних підводних кабелів, довжиною майже 1,3 млн кілометрів. Це робить мережу підводних кабелів даних фізичним проявом транснаціональної диджитальної зв'язаності.

Мета статті – дослідити проблеми загроз для безпеки, які пов'язані з поширенням та експлуатацією підводних кабелів у Європейському Союзі, висвітлити основні геополітичні проблеми, властиві глобальній мережі оптоволоконних кабелів та розглянути взаємні кроки назустріч України та ЄС у питаннях безпеки підводних кабелів та кібербезпеки.

Виклад результатів дослідження. Підводні кабелі критичні для міжєвропейської комунікації і пов'язують європейські держави з усім світом. Крім використаннядля цивільних потреб, країни залежать від підводних кабелів в аспекті національної безпеки. Координація воєнних операцій, дипломатичних місій і збирання розвідницької інформації залежить від кабельної мережі. Перерва в передачі даних тільки на декілька хвилин або годин може мати катастрофічні наслідки для будь-яких операцій, призначених на певний час та можуть мати значні фінансові наслідки [3].

У зв'яку з цим 1 вересня 2005 р. було створене Агентство Європейського Союзу з кібербезпеки (European Union Agency for Cybersecurity (ENISA). Воно розташоване в Іракліоні (Греція) та Брюселі. Його роль полягає у досягненні високого загального рівня кібербезпеки у Європі [5].

Увага політиків і вчених щодо безпеки і захисту підводних кабелів за останні п’ять років поступово збільшується. Особливе занепокоєння висловлюють військові щодо уразливості цих кабелів. Разом з тим недостатню увагу до цього питання приділяють політики і державні органи. Частина проблеми полягає в тому, що ця інфраструктура є невидимою. Фізично підводні кабелі лежать під водою у морях та океанах, що робить їх великою мірою невидимими. Є і більш загальна тенденція – приділяється недостатньо уваги до того, що взагалі відбувається у морях. Цей феномен був описаний як колективна морська сліпота. Як і інші типи морської інфраструктури, підводні комунікаційні кабелі часто залишаються непоміченими, доки не станеться аварія [3].

Важливо наголосити на такій проблемі, як складність управління глобальною мережею підводних кабелів. Частка державних і наддержавних структур в управлінні підводними комунікаційними кабелями швидко зменшується, тоді, як збільшується кількість ТНК, у яких кабелі знаходяться у приватній власності. Це такі комунікаційні «бегемоти», як Alcatel Submarine Network (France), Prismian Group (Italy), NKT A/S (Denmark), SubCom (United States), NEC (Japan), Huawei Marine Network (China). Ринкова частка компаній, які належить Китаю, за останні роки суттєво збільшилася. Оператори мережі традиційно були головними інвесторами у підводні кабелі. Разом з тим, такі «BigTech» компанії, як Google, Amazon, Microsoft, Facebook розширюють свої інвестиції у цей сектор, аби забезпечити взаємозв’язок своїх центрів обробки даних.

Підводні комунікаційні кабелі даних в економічній літературі нерідко інтерпретуються як нішовий ринок, але вони є головним вектором впливу компаній глобального Інтернету, забезпечуючи його функціонування, розвиток і надійність.

Як було зазначено, навіть короткостроковий збій у роботі підводних кабелів може бути причиною великомасштабних кіберінцидентів. Слабкими місцями в роботі даної інфраструктури є станції з’єднання кабелів, а також підводні зони з їхньою високою концентрацією [1].

Нині кабельні підводні мережі є стратегічним імперативом розвитку провідних країн. Сигнали, що звідти передаються, спрямовуються від міжнародних кабелів до головних національних та регіональних кабелів. Так само, як морські порти та аеропорти, кабельні станції є вирішальними вузлами, стратегічними геополітичними дислокаціями, в яких різноманітні меседжі затримуються або призупиняються, цензоруються або перехоплюються. Відповідно до однієї з інформацій, наданих Едвардом Сноуденом, розвідувальні агентства, зокрема агентства національної безпеки США і Головне управління урядових комунікацій США, моніторили трафік на кабельних станціях. Це не є сюрпризом для тих, хто знайомий з історією кабелів телеграфної ери. Уряди перевіряли послання, які проходили через їхні береги до підводних кабельних станцій. Тож є місця, де безпека набуває абсолютно критичного значення. І це

кабельні станції, оскільки саме в них електрика може бути відключена, жучки можуть бути поставлені в систему, а трафік може бути спеціально переорієнтований [7, с. 64]. Ми звикли думати про кібербезпеку у термінах хакерських атак, але передача данихтакож піддається нападу на шляхах фізичних ліній їхніх підводнихкабельних мереж.

Ремонт підводних кабелів складний, тривалий та потребує наявності спеціалізованих суден. В акваторії навкруг Європи їх два. Ще одне судно розташоване біля берегів Британії у Портленді. За даними звіту Міжнародного комітету захисту кабелів 2022 р., більшість інцидентів з кабелями випадкові і пов'язані з якоренням і рибальством. Але спостерігається також і тенденція до постійного збільшення обсягу інтернет-трафіку, що проходить цими кабелями. Це викликає зростання навантаження на кабельну систему та періодичні збої. Доступ до даних на станціях приєднання є цілком реальною і актуальною загрозою [6].

Розвиток сучасних оптоволоконних кабельних станцій, які підтримують нинішній трафік даних, відбиває сучаснийландшафт безпеки. Станції захищені від терористичних атак на землі. Кабельні компанії захищають навколишнє середовище навколо станції. Таке убезпечення називається «буферною зоною». Нині кабельні станціїй часто залишаються не позначеними на картах і не мають ніяких спеціальних позначень у місцевості, де вони розташовані. Деякі з них не публікують своїх адрес. Інші - означені у спеціальних урядових документах тільки координатами. Такі стратегії кібербезпеки кабельних станцій аби не було виходу цієї інформацію назовні [7, с. 64].

Вже минули ті часи, коли прокладанням телекомунікаційного підводного кабелю опікувалися імперії і держави. Нині окремі корпорації досягли такого рівня, що можуть дозволити собі робити це самостійно або із компаніями інших держав, які вони самі обирають собі у партнери. Так, пошуковий гігант Google та 5 азійських телекомунікаційних компаній домовилися інвестувати орієнтовно 300 млн. дол. у розвиток транстихоокеанської кабельної мережі, яка з'єднує Сполучені Штати та Японію. Цей кабель назвали «Faster», тобто, - «швидше». Кабель з потужністю 60 терабітів у секунду з'єднав Лос-Анджелес, Портленд, Сан-Франциско, Орегон, Сіетл із такими містами у Японії, як Чікура та Шима. NEC Corp., яка виступає системним постачальником для цієї кабельної мережі, заявила, що будівництво мережі закінчено й введено в експлуатацію у другому кварталі 2016 р. Ця підводна кабельна мережа спроможна також з'єднувати сусідні кабельні системи, щоб вони продовжувалися від Японії до інших азійських держав. Необхідно зазначити, що Google вже оперує своїми надшвидкісними кабельним телебаченням та Інтернетом в районі Канзас Сіті [7, с. 65]. Це є свідченням того, що потреба в Інтернеті у світі зростає й він теж є стратегічним імперативом модернізації провідних країн і глобальних ТНК.

У квітні 2022 р. ЄС оприлюднює доповідь «Безпекові загрози підводним комунікаціям та інфраструктурі – наслідки для ЄС», яку написали на його замовлення три європейські експерти Крістіан Бегер, Тобіас Лібертрау і Джонас Франкен. Доповідь являє собою глибокий аналіз ситуації. З боку Європейського Парламенту координатором цього дослідження виступав Департамент політики зовнішніх зв'язків Головного Директорату зовнішніх зв'язків Союзу PE 702.557. У резюме цієї доповіді, зокрема, зазначалося: «Глобальна підводна кабельна мережа для передачі даних – життєво критична інфраструктура. 99% світових диджитальних комунікацій проходить через цю мережу. Глобальна економіка і диджитальні сервіси цілком залежать від неї. Доповідь надає рекомендації Європейському Парламенту, як він може керувати процесом безпеки кабелів, щоб зменшити їх уразливість» [3].

Щодо зламів та пошкоджень підводних кабелів в Атлантичному океані йдеться не тільки про дії підводних човнів (здебільшого РФ), але й про шпигунські дії окремих російських розвідників в Ірландії. Як повідомила впливова британська газета The Times у статті «Російські агенти занурюються у океанські глибини в Ірландії, щоб зламати трансатлантичні кабелі», «Росія надіслала агентів розвідки до Ірландії для того, щоб встановити місце розташування оптоволоконних кабелів, які з'єднують Європу з Америкою» [8]. Ірландські силовики й розвідка також вважають, що відряджені до Ірландії «туристи», які пірнали з ірландсько пляжу до Північно-атлантичних глибин, – це співробітники ГРУ Росії.

До небезпечних держав, які перешкоджають розвитку глобальної кабельної системи, вчені у зазначеній доповіді для ЄС відносять і КНР. Але з боку КНР спостерігаються дії іншого характеру. Це передовсім швидке нарощування кілометражу кабельних ліній, які вони прокладають. Китайська корпорація HMN Technologies, (колишня Huawei Marine Networks) має ринкову долю більше, ніж 10% глобального ринку підводних кабелів. Вона проклала або полагодила біля 100 кабелів з існуючих 400 (за даними американського дослідника Дж. Шермана – 475 м. [9] – *прим. – О.З.*). Китайські інвестиції в інфраструктуру кабелів інтегровані до проекту «Китайський диджитальний шовковий шлях» (The Chinese Digital Silk Road, (DSR)). Цей проект був доданий у 2015 р. до пекинської офіційної програми під назвою «Китайська ініціатива Пояс і Шлях» (Beijin's Belt and Road Initiative, BRI).

Увага політиків і вчених щодо безпеки і захисту підводних кабелів за останні 5 років поступово набирає силу в громадських дебатах. Особливе занепокоєння висловлюють військові щодо важливості цих кабелів. Але разом з тим політики і державні органи приділяють недостатньо уваги цьому питанню. Частина проблеми полягає в тому, що ця інфраструктура є невидимою. Фізично підводні кабелі лежать під водою у морях та океанах, що робить їх великою мірою невидимими.

Ми вже зазначали, що небезпека для глобальної комунікаційної мережі може надходити від ненавмисних дій (якоріння, риболовскі трали тощо). Але існують загрози для кабелів, які, так би мовити, спонсоруються на державному рівні.

Концепція сірої зони і гібридної війни означає зловмисну діяльність за межами збройного конфлікту. Російські збройні сили, починаючи з 2008 р., пройшли значну модернізацію. Головним елементом в ній була модернізація російського морського флоту. Спеціальний фокус був направлений на розвідувальні кораблі класу «Янтар» і допоміжні підводні човни. Ці два види озброєння здатні пошкоджувати інфраструктуру підводних кабелів. До того ж Росією були створені сучасні потужні човни і фрегати. Відповідно до доповіді НАТО 2019 р. щодо безпеки у Північній Атлантиці, «всі вони мають нові можливості використовувати малі субмарини, вивчати підводні морські кабелі та проводити електронну війну щодо них» [10]. НАТО продовжує підкреслювати, що нині існує безпрецедентний інтерес російських морських сил до розташування кабелів, якого ніколи не було раніше [11; 12].

У січні 2022 р. британський Голова оборони застеріг політиків у своєму інтерв'ю, що російська підводна активність стає безпрецедентною і безпосередньо спрямована на кабельні системи [13]. А у лютому 2022 р., як сповіщала газета The Guardian [14], Росія розгорнула морські навчання на Південний Захід від Ірландії (на території, яка безпосередньо прилягяє до ірландської ексклюзивної економічної зони), що дуже близько до кількох підводних кабелів, які пов'язують Британію, Францію та США

У контексті агресії Росії проти України, цей месидж має бути взятим до уваги. Під час анексії Криму Москва пошкодила головний наземний кабель, що з'єднував цей півострів з рештою світу, щоби отримати контроль над інфраструктурою Інтернету Криму і в такий спосіб, — над потоком інформації. Це надало Кремлю можливість поширювати дезінформацію і провадити ці дії немов легітимні [15].

Думка американського дослідника Дж. Шермана з Атлантичної Ради США є дуже слушною, оскільки, як витікає з неї, Україна не стоїть осторонь глобальних комунікаційних процесів, пов'язаних з функціонуванням підводних морських кабелів. Російські агресори добре розуміють важливість функціонування і підводних, і наземних кабельних мереж, через які передаються величезні масиви данних і зокрема послуги Інтернету. Тому Україні необхідно звернути щонайбільшу увагу функціонуванню наземних комунікаційних кабелів з передачі даних та Інтернету, оскільки це є критичною інфраструктурою для її існування та розвитку.

Як повідомляє «пресслужба РНБО, Україна розвиває співпрацю з Агентством ЄС з мережевої та інформаційної безпеки (ENISA). Керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО, секретар НКЦК Н. Ткачук та заступник Голови Держспецзв'язку В. Жора провели робочу зустріч з директором ENISA Юханом Лепасаром 5 вересня

2022 р. Під час зустрічі було обговорено перспективні напрями взаємодії та необхідність розробки дорожньої карти розвитку співробітництва. Українські фахівці наголосили, що для нашої країни налагодження практичної взаємодії з ENISA та отримання особливого статусу партнера стане надзвичайно важливим кроком на шляху євроінтеграції та необхідності гармонізації вітчизняного законодавства у сфері кібербезпеки з європейським».

Британська газета The Financial Times сповіщає, що Європейський Союз має намір прокласти підводний інтернет-кабель через Чорне море, щоб поліпшити зв'язок з Грузією і зменшити залежність від комунікаційної інфраструктури, яка проходить через Росію. Британська телекомунікаційна корпорація Vodafone також має плани щодо прокладання підводного кабелю в Чорному морі, під назвою Kardessa, який з'єднає Україну з Болгарією, Туреччину з Грузією, а потім піде підземлю до Вірменії, Казахстану і далі в Азію. Про це повідомляє Financial Times. У документі Європейської комісії йдеться про те, що 1100-кілометровий кабель коштуватиме 45 млн. євро. Він призначений для того, щоб з'єднати Європу з Кавказом і зменшити «залежність від наземного оптоволоконного зв'язку, що проходить через Росію» [17].

4 січня 2024 р віцепрем'єр-міністр з інновацій, розвитку освіти, науки та технологій, міністр цифрової трансформації Михайло Федоров повідомив, що Україна і Румунія підписали угоду про співпрацю. Сторони домовилися про перші кроки – підвищення стійкості українських інтернет-мереж, розвиток 5G-коридорів між кордонами України й Румунії. Відповідно до угоди, Україна також братиме участь у програмах фінансової підтримки ЄС. Також Румунія допоможе у відновленні цифрової інфраструктури, пошкодженої через війну. М. Федоров висловив свою подяку румунському міністру Богдану-Груї Івану [18]. Такі кроки в бік зближення України та окремих країн ЄС важко переоцінити. Тим більше, що вони йдуть паралельним курсом зі зближенням з центральними стуктурами ЄС.

Підводні кабелі можуть підпадати під юрисдикцію широкого спектру регулюючих режимів, законів та органів влади. На національному рівні їх захистом можуть займатися телекомунікаційні органи, органи кібербезпеки, прикордонна охорона та військові. У приватному секторі екосистема підводних кабелів забезпечується власниками і операторами кабелів, постачальників і компанії з їх обслуговування [17].

Повертаючись до доповіді експертів щодо ситуації з підводними оптоволоконними кабелями в ЄС, необхідно зазначити, що вони дають низку слушних рекомендацій, які базовані на вивченні ситуації у цій регіональній організації:

- Йдеться про усвідомлення і приорітизацію проблеми безпеки підводних кабелів.
- Оновлення Морської безпекової стратегії.

- Запровадження тренувань і навчань берегової охорони в різних країнах ЄС та низку інших.

Ми вважаємо абсолютно доцільними рекомендації європейських експертів для ЄС.

Висновки. Дослідивши і проаналізувавши матеріали, які безпосередньо пов'язані з проблемами безпеки підводних комунікаційних кабелів і основними загрозами в для них, як на землі, так у морях і океанах у контексті європейської безпекими ми дійшли таких висновків:

- Підводні комунікаційні кабелі є критично важливою інфраструктурою у системі глобальної комунікації першої чверті XXI ст.
- Недооцінка їхньої важливості національними урядами, політиками, політологами може призвести до непоправних регіональних і глобальних криз у всіх галузях життєдіяльності людства: від і економіки і фінансів, державної безпеки і дипломатії, до перебоїв у роботі або зникнення Інтернету, соціальних мереж та інших важливих застосунків у цій сфері.
- З'ясовано, що навіть в межах ЄС є країни, в яких існує більше усвідомлення безпеки підводних кабелів – це країни, в яких є вихід до морів і океанів; і країни, які менш усвідомлюють проблеми безпеки підводних кабелів – це країни, які не мають кордонів виходу до морів і океанів. Але всі вони однаковою мірою залежить від функціонування підводних комунікаційних кабелів. Тож треба посилити роз'яснювальну роботу серед політиків і населення ЄС, аби розуміння проблем безпеки підводних кабелів було таким, як, скажімо, інших важливих інфраструктур: енергосистем, аеропортів, залізниць тощо, тобто інфраструктур видимих і зрозумілих громадянам країн ЄС.
- Не менш важливим є усвідомлення важливості підводних комунікаційних кабелів і для таких країн, як Україна, які прагнуть вступити до ЄС. Проте в українській суспільствознавчій науці майже не існує наукових розвідок щодо цієї проблеми. Про підводні комунікаційні кабелі українці можуть дізнатися тільки з технічної літератури. Українські інформаційні агентства є джерелом повідомлень про перші кроки між ЄС та Україною у цій сфері. Але вони, як і годиться інформаційним повідомленням, вкрай короткі і тільки констатують ті чи інші заходи.
- Тому нагальним є інформування політиків і громадян України, у свідомості переважної більшості яких Інтернет пов'язується тільки з супутниковим зв'язком. Але нині супутниковий зв'язок забезпечує тільки 1% розповсюдження Інтернету, тоді як підводні кабелі – 99%.
- Аналізуючи загрози підводним кабелям, їх можна поділити на природні (виверження вулканів, цунамі тощо), пов'язані з діяльністю людини (рибальство, якоріння тощо) та навмисні дії країн або терористичних

організацій, які призводять до пошкодження кабельних станцій або самих кабелів як у прибережній зоні, так і на глибинах морів та океанів.

До країн, які становлять небезпеку, західноєвропейські та американські політики та науковці відносять Росію та Китай. Виходячи з проаналізованих матеріалів, можна констатувати, що ці країни діють в різні способи. Варто зазначити, що Росію насамперед цікавлять шляхи прокладених кабелів з метою їх пошкодження. Для цього у неї є підводні човни, які оснащені батискафами та іншим обладненням, пристроями для заглиблення у морські та океанські води з метою пошкодження комунікаційних кабелів. Дії Росії в цьому напрямі були зафіксовані як європейськими, так і американськими військовими. В свою чергу КНР послідовно нарощує активність, інвестуючи у підводні кабелі та намагаючись до переваги в цьому питанні над США. Прокладаючи комунікаційні підводні кабелі самостійно або спільно з іншими країнами, Пекін особливо намагається посилити свій вплив у Індо-Тихоокеанському регіоні, що погрожує безпеці низки країн, зокрема Австралії та Новій Зеландії. Китай вже сьогодні має 10% від глобальної кабельної мережі. Ясна річ, що це відкриває доступ до кабелів і надає йому встановлювати на кабельних станціях і в кабелях прослуховуючи пристрої і т. ін.

- Необхідно наголосити, що Україна є морською державою. Тому повернення Криму та інших українських приморських територій, які зараз окуповані російськими загарбниками великою мірою збільшить її можливості в отриманні доступу до підводних телекомунікаційних кабелів, які пролягатимуть по дну Чорного моря. Це ще більше наблизить її до співробітництва з ЄС та входження до цієї регіональної організації.

Список використаних джерел та літератури

1. Frazer K. On Protecting the Underwater Cable. *Lawfare.* January 12. 2023. URL: https://www.lawfaremedia.org/article/protecting-undersea-cable-system
2. Зернецька О.В. До історії розвитку комунікацій: перші міжконтинентальні зв'язки. *Проблеми всесвітньої історії: Науковий журнал*. 2016. № 1. С. 183-197.
3. Bueger C., Liebetrau T., Franken J. Security threats to undersea communications cables and infrastructure – consequences for the EU. *European Parliament.* June 1. 2022. URL: https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557
4. Winseck D. The Geopolitical Economy of the Global Internet Infrastructure. *Journal of Information Policy.* 2017. Vol. 7. P 228–267. URL: https://edisciplinas.usp.br › brics_infra_internet
5. European Union Agency for Cybersecurity (ENISA). URL: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en

6. Інтернет на дні океану:якою є роль підводних кабелів в інфраструктурі глобальної мережі. *Internetua*. 26 вересня 2023. URL: https://internetua.com/internet-na-dni-okeanu-yakoua-ye-rol-pidvodnih-kabeliv-v-infrastrukturi-globalnoyi-mereji
7. Зернецька О.В. Глобальна комунікація як стратегічний імператив модернізації провідних країн. *Історичні та стратегічні імперативи модернізації провідних. і транзитивних країн світу: Збірник наук. праць.* За заг. ред. д. політ.н., проф. О.В. Зернецької. К.: ДУ «Інститут всесвітньої історії НАН України», 2017. С. 61-69.
8. Mooney J. Russian agents plunge to new ocean depths in Ireland to crack transatlanticcables. *The Times.* February 16. 2020. URL: https://www.thetimes.co.uk/article/russian-agents-plunge-to-new-ocean-depths-in-ireland-to-crack-transatlantic-cables-fnqsmgncz
9. Sherman J. Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security. *Atlantic Council.* September 13. 2021. URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/
10. Sanger D.E., Schmitt E. Russian Ships Near DataCables Are Too Close for U.S. Comfort. *The New York Times.* October 25. 2015. URL: https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html
11. Hinck G. Evaluating the Russian Threat to Undersea Cables. *Lawfare.* March 5. 2018. URL: https://www.lawfaremedia.org/article/evaluating-russian-threat-undersea-cables
12. Birnbaum M. Russian submarines are prowling around vital undersea cables. It's making NATO nervous. *The Washington Post.* December22. 2017. URL: https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html
13. Brzozowski A. NATO seeks ways of protecting undersea cables from Russian attacks. *Euractiv*. October 23. 2020. URL: https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/
14. UK military chief warns of Russian threat to vital undersea cables*. The Guardian.* January 8. 2022. URL: https://www.theguardian.com/uk-news/2022/jan/08/uk-military-chief-warns-of-russian-threat-to-vital-undersea-cables
15. Sherman J. Cord-cutting, Russian style: Could the Kremlin sever global internet cables? *The Atlantic Council.* January 31. 2022. URL: https://www.atlanticcouncil.org/blogs/new-atlanticist/cord-cutting-russian-style-could-the-kremlin-sever-global-internet-cables/
16. Богданьок О. Наближають наш вступ до ЄС: Шмигаль розповів про 5 угод, які підписали Україна і Євросоюз. *Суспільне новини.* 5 вересня 2022. URL: https://suspilne.media/278480-ukraina-i-es-pidpisali-5-ugod-aki-nablizaut-ukrainu-do-vstupu-v-evrosouz-smigal/
17. Леськова Ю. Взаємне партнерство. Україна розвиває співробітництво з ENISA. *Новини Live.* 4 жовтня 2022. URL: https://it.novyny.live/vzaimnoe-partnerstvo-ukraina-razvivaet-sotrudnichestvo-s-enisa-57681.html
18. Албул С. Україна та Румунія підписали угоду про співпрацю щодо підвищення стійкості телеком-мереж та 5G. *Lb.ua.* 4 січня 2024. URL: https://lb.ua/society/2024/01/04/592191_ukraina_rumuniya_pidpisali_ugodu.html

References

1. Frazer, K. (2023). On Protecting the Underwater Cable. *Lawfare.* January 12. [Online]. Available from: https://www.lawfaremedia.org/article/protecting-undersea-cable-system [In English].
2. Zernets′ka, O.V. (2016). Do istoriyi rozvytku komunikatsiy: pershi mizhkontynental′ni zv″yazky. *Problemy vsesvitn'oyi istoriyi: Naukovyy zhurnal,* 1, pp. 183-197. [In Ukrainian].
3. Bueger, C., Liebetrau, T., Franken, J. (2022). Security threats to undersea communications cables and infrastructure – consequences for the EU. *European Parliament.* June 1. [Online]. Available

from: https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557 [In English].
4. Winseck, D. (2017). The Geopolitical Economy of the Global Internet Infrastructure. *Journal of Information Policy,*7, pp. 228–267. [Online]. Available from: https://edisciplinas.usp.br › brics_infra_internet [In English].
5. European Union Agency for Cybersecurity (ENISA). [Online]. Available from: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en [In English].
6. Internet na dni okeanu:yakoyu ye rol′ pidvodnykh kabeliv v infrastrukturi hlobal′noyi merezhi. (2023). *Internetua.* September 26. [Online]. Available from: https://internetua.com/internet-na-dni-okeanu-yakoua-ye-rol-pidvodnih-kabeliv-v-infrastrukturi-globalnoyi-mereji [In Ukrainian].
7. Zernets′ka, O.V. (2017). Hlobal′na komunikatsiya yak stratehichnyy imperatyv modernizatsiyi providnykh krayin. *Istorychni ta stratehichni imperatyvy modernizatsiyi providnykh. i tranzytyvnykh krayin svitu: Zbirnyk nauk. prats′.* Za zah. red. d. polit.n., prof. O.V. Zernets′koyi. Kyiv: DU "Instytut vsesvitn′oyi istoriyi NAN Ukrayiny", pp. 61-69. [In Ukrainian].
8. Mooney, J. (2020). Russian agents plunge to new ocean depths in Ireland to crack transatlanticcables. *The Times.* February 16. [Online]. Available from: https://www.thetimes.co.uk/article/russian-agents-plunge-to-new-ocean-depths-in-ireland-to-crack-transatlantic-cables-fnqsmgncz [In English].
9. Sherman, J. (2021). Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security. *Atlantic Council.* September 13. [Online]. Available from: https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/ [In English].
10. Sanger, D.E., Schmitt, E. (2015). Russian Ships Near DataCables Are Too Close for U.S. Comfort. *The New York Times.* October 25. [Online]. Available from: https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html [In English].
11. Hinck, G. (2018). Evaluating the Russian Threat to Undersea Cables. *Lawfare.* March 5. [Online]. Available from: https://www.lawfaremedia.org/article/evaluating-russian-threat-undersea-cables [In English].
12. Birnbaum, M. (2017). Russian submarines are prowling around vital undersea cables. It's making NATO nervous. *The Washington Post.* December22. [Online]. Available from: https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html [In English].
13. Brzozowski, A. (2020). NATO seeks ways of protecting undersea cables from Russian attacks. *Euractiv*. October 23. [Online]. Available from: https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/ [In English].
14. UK military chief warns of Russian threat to vital undersea cables (2022). *The Guardian.* January 8. [Online]. Available from: https://www.theguardian.com/uk-news/2022/jan/08/uk-military-chief-warns-of-russian-threat-to-vital-undersea-cables [In English].
15. Sherman, J. (2022). Cord-cutting, Russian style: Could the Kremlin sever global internet cables? *The Atlantic Council.* January 31. [Online]. Available from: https://www.atlanticcouncil.org/blogs/new-atlanticist/cord-cutting-russian-style-could-the-kremlin-sever-global-internet-cables/ [In English].
16. Bohdan′ok, O. (2022). Nablyzhayut′ nash vstup do ES: Shmyhal′ rozpoviv pro 5 uhod, yaki pidpysaly Ukrayina i Yevrosoyuz. *Suspil′ne novyny.* September 5. [Online]. Available from: https://suspilne.media/278480-ukraina-i-es-pidpisali-5-ugod-aki-nablizaut-ukrainu-do-vstupu-v-evrosouz-smigal/ [In Ukrainian].

17. Les′kova, Yu. Vzayemne partnerstvo. Ukrayina rozvyvaye spivrobitnytstvo z ENISA. *Novyny Live.* October 5. [Online]. Available from: https://it.novyny.live/vzaimnoe-partnerstvo-ukraina-razvivaet-sotrudnichestvo-s-enisa-57681.html [In Ukrainian].
18. Albul, S. (2024). Ukrayina ta Rumuniya pidpysaly uhodu pro spivpratsyu shchodo pidvyshchennya stiykosti telekom-merezh ta 5G. *Lb.ua.* January 4. [Online]. Available from: https://lb.ua/society/2024/01/04/592191_ukraina_rumuniya_pidpisali_ugodu.html [In Ukrainian].

Zernetska O. Underwater Telecommunications Cables in the Context of the Security of the European Union.

Underwater telecommunications cables in the context of the European Union's security is tackled in this article. It is asserted that the importance of the underwater cables is diminished in mass conscience, though nowadays underwater telecommunications cables carry 99% of information and huge amount of data from diplomatic, political, financial to economic, social, cultural spheres of life.

The aim of the article is to investigate the problems of security, which are connected with development and exploitation of the undersea cables in the EU, and constituteone of its central geopolitical problems.

It is substantinated that the Internet is fully dependent on underwater cables. The global communication, which takes place nowadays, is impossible without the network of underwater cables. Its security is wholly dependent on them. Because cables lie at the bottom of seas and oceans, come across national borders and are often hidden in the ground, they have frequently been forgotten and received limited attention from policy makers. Sparked by Russian naval activity since 2014, when its submarines examined the waters of the North Atlantic, just the places where underwater cables have been laid, and geopolitical shockwaves sent by the 2022 by Russian-Ukrainian war, vulnerability of maritime infrastructures, is now receiving growing public and policy attention. The importance of the underwater cable network in global connectivity, the digital economy, and military operations is highlighted.

It is concluded that Ukraine is a maritime state, so the return of the Crimea and other costal territories currently occupied by Russian aggressors will greatly increase Ukrainian opportunities to gain access to underwater telecommunications cables that will run along the bottom of the Black Sea. This will bring it even closer to cooperation with EU and joining this regional organisation.

Keywords: *underwater telecommunications cables, global network, security, resilience, European Union, Urraine.*