Зінченко Олександра Ігорівна

Вплив політичної ситуації в Україні на проблеми кібербезпеки Європейського Регіону

УДК 351.86:004.056](4)-042.3:32(477)
DOI https://doi.org/10.24195/2414-9616.2024-5.21

Зінченко Олександра Ігорівна
аспірантка кафедри політології
Харківського національного
університету імені В. Н. Каразіна
майдан Свободи, 4, Харків, Україна
ORCID: 0000-0003-1623-957X

У статті досліджується вплив політичної ситуації в Україні на проблеми кібербезпеки Європейського регіону в умовах сучасних геополітичних викликів. Зокрема, зосереджена увага на тому, як війна в Україні, а також політичні та соціально-економічні процеси, пов'язані з конфліктом, сприяють зміні характеру та інтенсивності кіберзагроз для європейських країн. Важливою темою є вплив агресії росії на стратегії кібербезпеки не тільки в Україні, але й в інших країнах Європи, що, з одного боку, постраждали від хакерських атак, а з іншого – стали свідками посилення співробітництва в галузі кіберзахисту. У статті розглядаються різноманітні типи кіберзагроз, з якими стикаються європейські держави через політичні події в Україні, серед яких кібератаки на інфраструктуру, інформаційні маніпуляції, викрадення даних, дезінформаційні кампанії, а також зростання кібертероризму.

Особлива увага приділяється аналізу специфічних викликів для кібербезпеки, які виникають унаслідок активізації гібридних загроз та використання кіберпростору як частини військової стратегії. Актуальним є також питання зміцнення кіберзахисту на рівні окремих країн та міжнародних організацій, таких як Європейський Союз та НАТО, які активно сприяють розвитку спільної стратегії боротьби з кіберзлочинністю. У статті висвітлюється важливість створення і підтримки єдиної стратегії для забезпечення кібербезпеки в Європі в умовах посилення глобальної політичної нестабільності. Поряд з цим, розглядаються можливості взаємодії України та ЄС у сфері кібербезпеки, а також роль міжнародних експертів та організацій у наданні підтримки у відбитті кіберзагроз.

Не менш важливим аспектом є оцінка ефективності реагування на кіберзагрози на рівні міжнародних угод та спільних ініціатив, які дозволяють не тільки зміцнювати обороноздатність держав, але й знижувати ризики виникнення кібервійни на глобальному рівні. У статті наголошується, що для ефективної боротьби з кіберзагрозами потрібна не тільки технічна, але й політична координація зусиль між державами, що мають спільні інтереси щодо безпеки кіберпростору.

Ключові слова: *кібербезпека, політична ситуація, Україна, Європейський Союз, кібератаки, інформаційні загрози, кіберзлочинність, Європейський регіон, кібертероризм, кіберзахист, безпека в Інтернеті, кіберпростір, кібероборона.*

Постановка проблеми. Політична ситуація в Україні, особливо в умовах збройного конфлікту з росією, значно впливає на кібербезпеку як в Україні, так і в Європейському регіоні загалом. Зокрема, зміни в геополітичному ландшафті спричиняють зростання кількості кіберзагроз, які можуть мати значний вплив на безпеку держав і міжнародних організацій. Кіберзагрози, що виникають в результаті конфліктів, можуть включати кібератаки на критичну інфраструктуру, викрадення та маніпуляцію даними, а також поширення дезінформації через цифрові канали. Ці загрози не тільки ставлять під загрозу економічну і політичну стабільність, але й можуть мати серйозні наслідки для безпеки громадян.

З огляду на це, постає питання: як політичні зміни в Україні можуть впливати на кібербезпеку Європи та які стратегії необхідно розробляти для забезпечення захисту в умовах нових викликів? Враховуючи високий рівень цифровізації та інтеграції інформаційних систем в усіх сферах життєдіяльності держав, зокрема в економіці, енергетиці, транспорті та медицині, кіберзагрози мають потенціал викликати значні економічні та соціальні наслідки. Тому важливо не тільки виявляти ці загрози на ранніх етапах, а й розробляти ефективні механізми для їх попередження та нейтралізації.

Це питання є критично важливим для теоретичних і практичних досліджень у сферах міжнародної безпеки, правознавства та інформаційних технологій. Науковці мають розробляти нові підходи до оцінки кіберзагроз, пов'язаних із політичними конфліктами, а також удосконалювати методи захисту критичної інфраструктури на рівні держав та об'єднань, як-от ЄС і НАТО. З практичної точки зору, це вимагає створення стратегії кіберзахисту для стійкості до атак як від державних, так і недержавних суб'єктів. У контексті нестабільної ситуації в Україні важливо посилити колективну безпеку Європи, зміцнити співпрацю з Україною, обмін інформацією та спільні навчання для захисту інфраструктури. Загалом, ключовими завданнями є як розвиток технологічних рішень, так і політична координація для ефективного захисту від кіберзагроз та підтримки міжнародного правопорядку в кіберпросторі.

Метою статті є аналіз впливу політичної ситуації в Україні на проблеми кібербезпеки Європейського регіону, зокрема на зростання кіберзагроз, що виникають внаслідок збройного конфлікту та геополітичної нестабільності.

Методи дослідження включають аналіз та узагальнення наукової літератури й документів, порівняльний аналіз політичних рішень. Крім того, застосовувалися методи системного підходу для оцінки взаємозв'язків між політичною ситуацією в Україні та проблемою забезпечення кібербезпеки Європейського Регіону.

Аналіз останніх досліджень та публікацій. Європейський Союз високо оцінює практичний досвід України у впровадженні цифрових технологій, відзначаючи її досягнення в цифровій інтеграції. Україна активно застосовує європейські стандарти та регуляції, прагнучи інтегруватися в Єдиний цифровий ринок ЄС і стати частиною загальноєвропейського цифрового простору. Важливість цифрової інтеграції України досліджували вчені, такі як Н. Є. Скоробогатов, В. П. Потапов, К. І. Ладиченко та інші, що висвітлюють роль цифрової інтеграції у глобальні процеси. Зокрема, питання регулювання кібербезпеки порушували О. Ф. Андрійко, В. Т. Білоус та інші.

У загальному контексті дослідження кібербезпеки в Європейському регіоні вже існує значний обсяг наукових праць, що аналізують вплив політичних криз на безпеку в кіберпросторі. Однак у результаті дослідження ми виявили, що певні аспекти цієї проблеми досі залишаються недостатньо вивченими. Однією з невирішених частин є недостатнє розуміння того, як конкретно війна в Україні та її геополітичні наслідки змінюють характер кіберзагроз для європейських країн, зокрема у контексті нових форм гібридних атак, де кіберпростір виступає одним з основних інструментів.

Дослідження часто зосереджуються на загальних механізмах реагування на кіберзагрози, але бракує спеціалізованих досліджень, що безпосередньо пов'язують політичну ситуацію в Україні з конкретними кіберзагрозами для європейських держав. Ці проблеми не завжди розглядаються в комплексі, коли мова йде про взаємозв'язок між військовими діями, політичною нестабільністю та кібербезпекою в Європі.

Іншою нерозв'язаною проблемою є відсутність узгоджених міжнародних стандартів і стратегії кіберзахисту в умовах поточної політичної ситуації, зокрема в контексті постійної ескалації конфлікту в Україні. Різноманітні підходи до забезпечення кібербезпеки на національному рівні не завжди можуть ефективно працювати в умовах, коли кіберзагрози мають транснаціональний характер, і європейські держави не мають єдиного інструменту для оперативного реагування.

Також не розв'язано питання ефективної взаємодії між Україною та ЄС у сфері кібербезпеки. Спільні ініціативи та програми сприяння розвитку кіберзахисту між країнами-членами ЄС та Україною все ще не достатньо розвинені, а співпраця не завжди реалізується на практиці. Додатково залишається актуальним питання посилення кіберзахисту на рівні ЄС, оскільки багато європейських країн не мають достатнього рівня технічної готовності до реагування на нові види кіберзагроз, спричинених геополітичними подіями.

Результати. Політична ситуація в Україні та її вплив на безпеку Європи є складним і багатогранним питанням, яке набуло особливої актуальності після початку агресії росії проти України у 2014 році та повномасштабного вторгнення в лютому 2022 року. Цей конфлікт не тільки змінив внутрішньополітичну ситуацію в Україні, а й поставив перед європейськими державами низку нових викликів у сфері безпеки, зокрема в контексті кіберзагроз.

З початком війни Україна стала не лише ареною військових дій, але й об'єктом численних кібероперацій з боку Росії, що спричинило значні збої в роботі державних і приватних установ, критичної інфраструктури та національних засобів комунікації. Кіберзагрози, які виникли через конфлікт, мають прямий і непрямий вплив на європейську безпеку, адже Україна, маючи стратегічне розташування, фактично стала буферною зоною між росією та Європейським Союзом. Тобто збої в кібербезпеці України безпосередньо відображаються на стані цифрової безпеки всього європейського регіону.

Одним із найбільших викликів для Європи є загроза енергетичної безпеки. Російські кібероперації спрямовані на підрив енергетичної інфраструктури України, зокрема, на атакування енергетичних мереж і постачання електричної енергії. Ці атаки, окрім безпосередніх наслідків для України, створюють ризики для європейських країн, оскільки система енергетичних мереж Європи тісно взаємопов'язана, і будь-які збої в Україні можуть вплинути на постачання енергії до інших держав.

Наряду з атаками на критичну інфраструктуру, зростає загроза використання кіберзброї як елементу гібридної війни. Росія активно використовує кіберпростір для дестабілізації ситуації не лише всередині України, але й на міжнародному рівні. Особливо це стосується кампаній з дезінформації та маніпулювання громадською думкою, спрямованих на підрив довіри до демократичних інститутів в Європі. У зв'язку з цим, поширення фейкових новин і маніпуляцій в кіберпросторі є прямою загрозою для стабільності та безпеки європейських держав, оскільки може спровокувати соціальні, політичні та економічні кризи.

Крім того, напруга на українському фронті сприяє зростанню геополітичних суперечностей між Європейським Союзом, НАТО та росією, що також має вплив на кібербезпеку. Держави ЄС, намагаючись підтримати Україну у війні, одночасно

стикаються з новими кіберзагрозами з боку Росії, яка активно намагається протестувати на цифровому рівні військові та економічні санкції, що були введені проти неї. Кібероперації, які спрямовані на порушення роботи фінансових систем або вплив на економічну діяльність, можуть призвести до негативних наслідків не лише для України, а й для економік європейських країн.

Слід також зазначити, що геополітична ситуація в Україні впливає на міжнародну співпрацю в області кібербезпеки. Європейські країни змушені посилювати взаємодію з Україною у сфері обміну інформацією щодо кіберзагроз, а також удосконалювати свої стратегії кіберзахисту. Українська влада, своєю чергою, розвиває співпрацю з європейськими державами, сприяючи зростанню кібербезпеки на континенті. Це охоплює спільні навчання з кіберзахисту, обмін досвідом та технологіями у сфері кібербезпеки, а також створення спеціалізованих організацій для боротьби з кіберзагрозами.

Виділимо, що для Європи політична ситуація в Україні створює нові виклики у сфері нормативно-правового забезпечення кібербезпеки. Необхідність модернізації законодавства та адаптації наявних стандартів до нових реалій геополітичної ситуації вимагає посиленої уваги до таких аспектів, як визначення правових рамок для боротьби з кібертероризмом, забезпечення кіберзахисту для критичної інфраструктури, а також створення ефективних механізмів реагування на міжнародні кіберзагрози.

Для обґрунтування вище наведених аргументів ми проаналізували конкретні приклади атак та загроз, що мають вплив і на Європейський регіон. В одному з найбільших інцидентів, що відбулися 13 січня 2022 року, було атаковано близько 70 урядових вебсайтів України, включаючи ресурси Міністерства оборони, Міністерства закордонних справ, інших державних органів. Це порушило доступ до державних послуг, підірвало комунікаційну здатність і спричинило хвилю занепокоєння, оскільки кібератака такого масштабу, спрямована на ключові об'єкти державного управління, могла поширитися на європейську інфраструктуру. Європейський Союз відреагував на цю ситуацію посиленням співпраці з Україною у сфері кібербезпеки, що стало частиною стратегічного кібердіалогу.

Ще одним критичним епізодом стала поява шкідливого програмного забезпечення HermeticWiper, запущеного проти українських державних установ та приватних організацій у лютому 2022 року. Це програмне забезпечення призвело до значних втрат даних у таких секторах, як фінанси, авіація та інформаційні технології, створюючи безпосередню загрозу стабільності державних і комерційних процесів. Існувала реальна небезпека, що атака на Україну могла б мати «каскадний» ефект, уразивши також європейські установи та спричинивши масштабне витікання чутливої інформації, пов'язаної з безпекою, обороною або міжнародними проєктами ЄС. Ця потенційна загроза показала, наскільки вразливими можуть бути інформаційні системи в умовах гібридної війни, а також спонукала країни ЄС до перегляду та посилення власної кібероборони [1; 3].

Кібератаки на енергетичну інфраструктуру України у 2015 та 2016 роках привернули увагу ЄС до вразливості власних енергосистем. У відповідь європейські країни розробили стратегії з посилення кіберзахисту, включаючи покращення моніторингу загроз, удосконалення механізмів швидкого реагування, модернізацію інфраструктури та впровадження резервних систем відновлення енергопостачання. Це сприяло інтеграції українських викликів кібербезпеки в ширшу стратегію європейської безпеки, що особливо актуально на тлі сучасних геополітичних загроз. Паралельно з цим російська сторона активно використовує кібершпигунство та крадіжку даних [2; 5]. Починаючи з 2022 року, напади на українські державні установи супроводжувалися масштабним збором інформації, що могла бути використана для тиску, дискредитації або в контексті інформаційної війни. Європейські держави зіткнулися з аналогічною загрозою, адже викрадені дані з українських державних ресурсів можуть мати значення для міжнародних відносин і потенційно бути використаними для дестабілізації європейських урядів або поширення стратегічно важливої інформації.

Дезінформація як ключовий компонент гібридної війни активно використовується росією для маніпуляції громадською думкою як в Україні, так і в країнах Європейського Союзу. Відомі випадки, коли російські кампанії в соціальних мережах та інших медіаресурсах поширювали неправдиву інформацію з метою підриву довіри до урядів, послаблення єдності ЄС, а також провокування суперечок між країнами. Такий інформаційний вплив є серйозною загрозою для інтеграційних процесів у Європі та створює можливості для подальшої дестабілізації регіону [2].

Європейський регіон активно посилив заходи кіберзахисту, орієнтуючись на загрози, пов'язані з конфліктом в Україні. Серед ключових кроків - ЄС організовує регулярні кібернавчання, такі як Cyber Europe, що дозволяють тестувати захист критичної інфраструктури. З 2022 року посилено співпрацю з НАТО для спільних дій у кіберсфері, а завдяки взаємодії з українськими експертами ЄС удосконалив свої методи протидії гібридним загрозам. Крім цього, ухвалено нову директиву NIS2, яка підвищує стандарти кібербезпеки в країнах-членах. Ці заходи стали відповіддю на нові ризики в кіберпросторі, які вимагають координації та посилення правової бази [4; 5].

З цього випливає, що Європейському Союзу доводиться вирішувати ще одну комплексну проблему – недостатню узгодженість між державами-членами в питаннях кібербезпеки. Хоча існують спільні політики та стратегії в рамках ЄС, наприклад, програма Європейського центру боротьби з кіберзлочинністю, підходи різних країн до протидії кіберзагрозам суттєво відрізняються. Це ускладнює створення єдиної системи захисту, адже успіх таких програм залежить від рівня інтеграції національних політик у загальноєвропейську структуру кібербезпеки. Політичні зміни в Україні стали каталізатором для підсилення таких ініціатив, оскільки тепер європейські країни прагнуть швидше досягти узгоджених підходів для ефективного реагування на загрози [6].

Крім того, існує потреба у постійному оновленні технологічних рішень та інновацій для захисту кіберпростору. Росія використовує дедалі складніші методи кібернападів, зокрема деструктивне шкідливе програмне забезпечення, як-от HermeticWiper та інші подібні програми, які були застосовані проти України. Щоб запобігти проникненню таких загроз в ЄС, країни-члени змушені оновлювати свої кіберзахисні механізми, розробляти нові інструменти для виявлення загроз, а також більше інвестувати у дослідження новітніх технологій.

Врешті-решт, питання кіберзахисту України є невіддільним елементом загальної стратегії ЄС із забезпечення регіональної стабільності. Розвиток кіберспроможностей та їхня інтеграція в європейські структури не лише підвищують рівень кібербезпеки в Україні, але й посилюють безпеку Європи загалом. Це стає очевидним з огляду на те, що Україна фактично стала форпостом у боротьбі з кіберзагрозами з боку росії, і її досвід може бути надзвичайно цінним для європейських партнерів [5].

Висновки та перспективи дослідження. Результати проведеного нашого дослідження вказують на кілька ключових аспектів. По-перше, повномасштабна війна, розпочата росією проти України у 2022 році, показала, наскільки серйозно кіберзагрози можуть впливати на критичну інфраструктуру, економічну стабільність та безпеку громадян. Атаки на енергетичний сектор України, фінансові установи та державні органи продемонстрували ефективність та небезпечність деструктивних кібероперацій, які можуть легко перетнути національні кордони та поширитися на інші країни Європи.

По-друге, кіберпростір виявився потужним засобом для ведення гібридної війни, зокрема через кампанії дезінформації та пропаганди, спрямовані на дестабілізацію суспільств. Прокремлівські інформаційні операції, націлені на європейську аудиторію, посилили політичну напругу, збільшили недовіру до урядів та ускладнили питання прийняття рішень, пов'язаних із підтримкою України. Тобто ситуація в Україні стала чинником, який ускладнює не тільки питання внутрішньої, а й загальноєвропейської безпеки.

На нашу думку, перспективи дослідження цієї теми передбачають кілька напрямів, які важливі для подальшого розуміння й розвитку ефективної кіберстратегії ЄС. По-перше, потрібні додаткові дослідження щодо інтеграції українського досвіду кіберзахисту в загальноєвропейську систему безпеки. Це стосується не лише технологічних рішень, але й розробки спільних механізмів реагування на загрози. По-друге, важливим є аналіз ефективності наявних європейських кіберініціатив, зокрема щодо спільних навчань та інформаційного обміну. У контексті сучасних викликів, ці ініціативи вимагають розширення та оптимізації.

Крім того, перспективи дослідження включають аналіз можливостей співпраці між державами-членами ЄС та країнами-партнерами, зокрема Україною, у питаннях попередження кіберінцидентів та запобігання дезінформаційним атакам. Використання штучного інтелекту та новітніх технологій у кібербезпеці також потребує глибокого вивчення для покращення ефективності та своєчасності реагування на загрози. Розвиток цих дослідницьких напрямів сприятиме зміцненню кібербезпеки не лише в Європейському регіоні, але й у всьому регіоні, створюючи стабільну базу для захисту від кіберзагроз, що виникають через політичну нестабільність у Європі та агресивну кіберполітику росії.

ЛІТЕРАТУРА:

1. Зуй В. В. Актуальні проблеми кібербезпеки в Україні з урахуванням європейської інтеграції. *Правове забезпечення адміністративної реформи*. 2022. Ч.1. №4. С. 231-235.

2. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. К., 2023. №7 (липень). 270 с.

3. Пшетачник Я., Тарпова С., Війна Росії проти України: хронологія кібератак. ДСЄП| Дослідницька служба Європейського парламенту. 8 с.

4. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (дата звернення: 06.11.2024).

5. Kamara I. European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience. *Innovation: The European Journal of Social Science Research.* 2024. Pp. 1-20. https://doi.org/10.1080/13511610.2024.2349626

6. Monnet Chair J.. Cybersecurity in the EU: an introduction. Erasmus+ Programme of the European Union. 25 p.

REFERENCES:

1. Zuy V.V. (2022), «Aktual'ni problemy kiberbezpeky v Ukraini z urakhuvanniam yevropeis'koi intehratsii» [«Current Issues of Cybersecurity in Ukraine Considering European Integration»], Pravove zabezpechennia administratyvnoi reformy, Part 1, No. 4, pp. 231-235.
2. Dovhan O., Lytvynova L., Dorohyh S. (eds.) (2023), Kiberbezpeka v informatsiinomu suspilstvi: Informatsiino-analitychnyi daidzhest [«Cybersecurity in the Information Society: Information-Analytical Digest»], State Research Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"; National Library of Ukraine named after V.I. Vernadsky, Kyiv, No. 7 (July), 270 p.
3. Pshetachnyk Ya., Tarpova S. (2024), «Viina Rosii proty Ukrainy: khronolohiia kiberatak» [«Russia's War Against Ukraine: A Chronology of Cyberattacks»], DSEP | Doslidnytska sluzhba Yevropeiskoho parlamentu [EPRS | European Parliamentary Research Service], 8 p.
4. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (accessed: 06.11.2024).
5. Kamara I. (2024), «European Cybersecurity Standardisation: A Tale of Two Solitudes in View of Europe's Cyber Resilience,» Innovation: The European Journal of Social Science Research, pp. 1-20. https://doi.org/10.1080/13511610.2024.2349626
6. Monnet Chair J. (2024), Cybersecurity in the EU: An Introduction, Erasmus+ Programme of the European Union, 25 p.

The impact of the political situation in Ukraine on cybersecurity issues in the European region

Zinchenko Oleksandra Ihorivna

Postgraduate Student at the Department of Political Science
V. N. Karazin Kharkiv National University
Maidan Svobody, 4, Kharkiv, Ukraine
ORCID: 0000-0003-1623-957X

The article explores the impact of the political situation in Ukraine on cybersecurity issues in the European region amid current geopolitical challenges. It focuses on how the war in Ukraine, as well as the political and socio-economic processes related to the conflict, contribute to the changing nature and intensity of cyber threats to European countries. A key theme is the influence of Russia's aggression on cybersecurity strategies not only in Ukraine but also in other European countries, which, on the one hand, have been affected by cyberattacks, and on the other, have witnessed enhanced cooperation in the field of cyber defense. The article examines various types of cyber threats faced by European states due to political events in Ukraine, including cyberattacks on infrastructure, information manipulation, data theft, disinformation campaigns, and the rise of cyberterrorism. Special attention is paid to the analysis of specific challenges for cybersecurity arising from the intensification of hybrid threats and the use of cyberspace as part of military strategies. The strengthening of cybersecurity at the national level and within international organizations such as the European Union and NATO, which actively support the development of a common strategy to combat cybercrime, is also addressed. The article highlights the importance of creating and maintaining a unified strategy for ensuring cybersecurity in Europe in the context of increasing global political instability. In addition, the possibilities of cooperation between Ukraine and the EU in the field of cybersecurity, as well as the role of international experts and organizations in supporting efforts to counter cyber threats, are considered. An equally important aspect is the evaluation of the effectiveness of responses to cyber threats at the level of international agreements and joint initiatives, which not only strengthen the defense capabilities of states but also reduce the risks of a global cyberwar. The article emphasizes that effective counteraction to cyber threats requires not only technical but also political coordination of efforts between states that share common interests in the security of cyberspace.

Key words: *cybersecurity, political situation, Ukraine, European Union, cyberattacks, information threats, cybercrime, European region, cyberterrorism, cyber defense, internet security, cyberspace, cyber warfare.*