СВІТОВА ЕКОНОМІКА ТА МІЖНАРОДНІ ВІДНОСИНИ

УДК 321.6/8:316.3
DOI: https://doi.org/10.32782/2415-8801/2023-4.1

Алексєєва Т.І.
кандидат економічних наук, доцент,
доцент кафедри міжнародних відносин, міжнародної інформації та безпеки,
Харківський національний університет імені В.Н. Каразіна

ВПЛИВ ГЛОБАЛІЗАЦІЙНИХ ПРОЦЕСІВ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ УКРАЇНИ В УМОВАХ ВІЙНИ

У статті проведено аналіз впливу глобалізаційних процесів на інформаційну безпеку України в умовах війни. Визначено роль та значення міжнародних та регіональних організацій в сфері інформаційної безпеки. Досліджено основні світові тренди глобалізації та причини їх загострення. Доведено необхідність реагування на виклики та загрози глобалізації, до яких відносяться: кібератаки; використання меметичної зброї; поширення фейків; проблема війни та миру; використання технологій штучного інтелекту тощо. Проаналізовано загрози інформаційній безпеці України в умовах повномасштабної військової агресії рф. Практичне забезпечення інформаційної безпеки України визначається необхідністю створення міжнародних механізмів протидії військовим та іншим загрозам світового масштабу. Це стосується, насамперед проблем підтримання миру і стабільності в світі; застосування колективних заходів для припинення актів агресії; забезпечення міжнародної інформаційної безпеки шляхом використання технологій штучного інтелекту для прогнозування і протидії загрозам.

Ключові слова: *глобалізаційні процеси, глобальні тренди; інформаційна безпека, кібербезпека, фейки, меметична зброя, інформаційні загрози, міжнародні організації.*

THE IMPACT OF GLOBALIZATION PROCESSES ON THE INFORMATION SECURITY OF UKRAINE DURING THE CONDITIONS OF WAR

Alekseeva Tetiana
V.N. Karazin Kharkiv National University

Large-scale changes that took place during the 20th and early 21st centuries. in international relations were caused by a number of global problems, the solution of which should be directed to the activities of the state and international organizations. Global trends, which have become a planetary factor, have introduced such processes as information wars, information weapons, information terrorism, information crime, and information security into the system of social relations. In this regard, the issue of developing and implementing a qualitatively new system of international security is urgent, which is explained not only by its unconditional importance for the preservation of human civilization, but also by its importance for the stable functioning of the world community as a whole. More and more countries are paying attention to the problem of information security and are developing national strategies to counter these threats. With the establishment of a monopolar world system, the issue of growing threats to regional and global security from international terrorism and organized crime arose. For Ukraine, ensuring international security remains the main problem today. In the conditions of a full-scale invasion of the Russian Federation on the territory of Ukraine, the importance of the ability to navigate in the ever-growing flow of information, effectively working with it, increases. In the conditions of the war in Ukraine and the tense situation in other countries of the world, the increase in the number of global disinformation campaigns is recognized as negative; information policy of the Russian Federation; social networks as subjects of influence in the information space; cyber security (cyberespionage, cybercrime, cyberterrorism. To fight against manifestations of negative trends, developed countries of the world and Ukraine use artificial intelligence, which provides military and intelligence services with new operational solutions for forecasting and countering threats, as well as for conducting offensive operations in cyberspace. Information security is an important function of the state, which must protect the country from the negative impact of globalization processes on information security.

Keywords: *globalization processes, global trends; information security, cyber security, fakes, memetic weapons, information threats, international organizations.*

Постановка проблеми. У системі міжнародної безпеки протягом XX – початку XXI століття відбулися значні зміни, пов'язані з цілою низкою глобальних проблем, на вирішення яких, повинна бути спрямована діяльність держави та міжнародної спільноти. Все більше держав звертають увагу на проблему інформаційної безпеки та розробляють національні стратегії для протидії цим загрозам.

З встановленням монополярного світоустрою постає питання вироблення дієвих механізмів забезпечення міжнародної інформаційної безпеки завдяки розв'язанню глобальних проблем сучасності за рахунок успішного розвитку в науково-технічній, інноваційній сфері та участі в цьому процесі міжнародних організацій. Механізм функціонування глобальних трендів і тенденцій на сьогодні став планетарним фактором, породивши цілий ряд соціальних трансформацій, ввівши в систему соціальних відносин такі процеси, як інформаційні війни, інформаційна зброя, інформаційний тероризм, інформаційна злочинність та інформаційна безпека [1].

У зв'язку з цим, проблематика становлення якісно нової системи міжнародної інформаційної безпеки є актуальною, і процес регулювання з боку держав та міжнародних організацій відіграє значну роль для економічного та соціально-політичного розвитку як кожної країни окремо, так і людства в цілому.

Аналіз останніх досліджень і публікацій. Серед фундаментальних досліджень у напрямі визначення впливу глобальних проблем на сферу інформаційної безпеки слід визначити праці А. Голікова, О. Довгаль, І. Матюшенко, В. Лужицького, А. Кожухівського, М. Згуровського, О. Захарової, Н. Тарханової, Ю. Внучко, Е. Лібанової, В. Тураєва та багато інших. Серед зарубіжних вчених проблемою впливу глобалізаційних процесів на інформаційну безпеку займались: Зб. Бжезинський, М. Дженіс, Б. Гейтс, Е. Бредлі, Г. Анхейер, К. Хагаі, З. Тофлер, У. Шрамм тощо.

Постановка завдання. Метою дослідження є виявлення причин виникнення та загострення глобальних проблем людства та їх вплив на інформаційну безпеку України.

Виклад основного матеріалу дослідження. В теперішній час процеси глобалізації все більш охоплюють сучасну систему міжнародних відносин. До основних проблем сучасності відносяться: вичерпання запасів стратегічних мінеральних ресурсів, пошук нових джерел енергії, бідність, тероризм, загрози кібербезпеці, територіальні суперечки, проксі-війни, розповсюдження ядерної зброї, міграція та біженці, інформаційні війни тощо.

В цих умовах подолання глобальних проблем людства залежить перед усім від підвищення ролі та відповідальності усіх суб'єктів господарювання, координації їх зусиль щодо формування та реалізації на національному та світовому рівнях загальних стандартів життя населення. Основним процесом світового розвитку, що визначають еволюцію світової системи виступають глобальні тренди, за допомогою яких можливо визначити шляхи вирішення глобальних проблем [2].

Необхідність реагування на виклики та загрози глобалізації пов'язана з визначенням та дією глобальних трендів розвитку у провідних країнах світу, до яких відносяться: розробка та впровадження технологічних інновацій; перехід глобальної економіки на новий етап технологічного розвитку; екологізація економіки і «зелене зростання»; процес старіння населення; вичерпання запасів стратегічних мінеральних ресурсів, пошук нових джерел енергії; застосування NBIC-технологій; проблема війни та миру; використання технологій штучного інтелекту тощо.

Динаміка майбутнього Європи буде залежати від якості її науки і технологічних інновацій. Разом зі Сполученими Штатами Америки і Японією, Європейський Союз в даний час є провідним гравцем в області інновацій і наукових досліджень, на які припадає 24% світових досліджень і 32% патентів. Щодо США, то пріоритети науково-технологічної та інноваційної політики цієї країни спрямовані на утримання лідерства у світовій політиці. Розробка NBIC-технологій є для цієї країни вкрай актуальним завданням [3].

Китай, як країна з високим рівнем демократичного дефіциту до 2030 року буде прагнути до більшої демократії, що матиме величезні наслідки. Зростання обсягів регіональної торгівлі призведе до порушень торговельного балансу у світі, де обсяг експорту Китаю значно буде перевищувати імпорт. Це означає, що успішний перехід Китаю до демократизації може посилити тиск на інші авторитарні держави, а також підправити подальшу модель економічного розвитку Китаю до тих пір, поки демократизація надовго не зупинить економічне зростання Китаю [4].

Україна, яка опинилась перед викликами зовнішньої агресії зі сторони рф, особливо гостро відчуває проблему у галузі забезпечення безпеки. Ефективність інформаційної безпеки будь-якої держави насамперед залежить від досконалості нормативно-правового регулювання діяльності інформаційної системи державних і громадських органів. Так, 28 грудня 2021 року було затверджено Стратегію інформаційної безпеки України.

Головна мета документа – забезпечення інформаційної безпеки держави та її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України.

Під час воєнного стану інформаційна зброя є достатньо потужним засобом ведення війни. Соціальні мережі виступають як канали поширення недостовірної інформації, застосовуя акаунти відомих політиків, повідомлення Viber, WhatsApp, Telegram та інших месенджерах.

Особливостями російсько-української війни виступає використання меметичного забезпечення. Війна, що ведеться за допомогою «меметичної зброї», є окремим випадком новітньої кібертехнології – «Memetic Warfare» («меметична війна»). У часи повномасштабної війни українці використовують меми для таких основних функцій: висміювання й деморалізація ворога; підтримка морального духу «своїх»; ідеалізація особистості. Кожна із цих функцій «б'є по ворогу, підриває його, дратує, ослаблює». Загалом меми повноцінно воюють на полі смислової битви і для протидії агресії терористичної федерації, а також для посилення єдності «смислів» українців [5].

В умовах війни особлива увага приділяється поширенню фейків, які являють собою навмисно сфабриковану інформацію, яка не має під собою ніяких підстав. Фейки ґрунтуються на брехні, маніпуляціях та перекручуваннях фактів. Така дезінформація поширюється через Інтернет, в основному для таких цілей використовуються месенджери (Whatsapp, Viber, Telegram), соцмережі (Facebook, Twitter, Instagram), онлайн-платформи (Reddit). Це робиться для того, щоб під виглядом фактів виростати плітки для зіпсування репутації конкуренту [6, с. 860].

В теперішній час особливого значення та актуальності набуває використання штучного інтелекту в системі забезпечення інформаційної безпеки. В сучасних умовах глобалізації інформаційна безпека виступає одним з найголовніших чинників забезпечення умов реалізації національних інтересів, спроможності держави долати кризові явища при зовнішній агресії. Це дає змогу провести аналіз інформаційних загроз та здійснити практичне застосування штучного інтелекту в контексті інформаційного опору.

Штучний інтелект (ШІ) може бути використаний для створення систем розвідки та контролю, які можуть виявляти загрози національній безпеці та вживати заходів для їх запобігання. Він також може бути застосований для автоматизації та оптимізації військових операцій, що дає змогу зменшити ризики для життя військових та підвищити ефективність дій, у військовій логістиці, військовій медицині, аєророзвідці тощо.

Однак, разом з перевагами, ШІ може становити загрозу національній безпеці. Наприклад, країна-агресор може використовувати ШІ для здійснення кібератак та інших злочинів, що можуть негативно впливати на національну безпеку. Також існує ризик, що інші держави можуть використовувати ШІ для проведення кібершпигунства та кібератак на інфраструктуру країни. При цьому не слід забувати й те, що системи на базі штучного інтелекту використовують і кіберзлочинці: відомі шахрайські прийоми використання Deep fake (створення реалістичного віртуального образу людини) для обману анти-фрод систем, підробки голосів для шахрайських дзвінків.

В умовах війни Україна застосовує технології штучного інтелекту для забезпечення обороноздатності країни. Розпорядженням Кабінету Міністрів України № 1556-р в Україні 2 грудня 2020 року було схвалено Концепцію розвитку штучного інтелекту, яка передбачає визначення основних напрямів та пріоритетних завдань розвитку технологій штучного інтелекту з метою захисту технологічних інформаційно-комунікаційних систем [7].

Сьогодні ШІ в сфері інформаційної безпеки використовується у таких напрямах: виявлення та аналітика загроз, безпека даних і додатків, управління ідентифікацією, безпека мереж та систем, управління інформаційною безпекою. Наприклад, такі технології ШІ, як обробка природної мови, квантові обчислення, нейронні мережі і глибоке навчання надають військовим і розвідувальним службам нові оперативні рішення для прогнозування і протидії загрозам, а також для проведення наступальних операцій в кіберпросторі.

Україна поступово переходить в онлайн простір з використанням сучасних технологій, що спонукають до розвитку економіки. На основі цього, серед інших суспільних проблем суттєво загострюються питання кібербезпеки, коли кризові ситуації традиційно викликають активізацію різноманітних хакерських угрупувань. В кіберпросторі конфлікту між Росією та Україною відбуваються значущі події та трансформації, які віддзеркалюють сучасні підходи до ведення війни та протистояння в кібернетичній сфері. На сучасному етапі війни Росії проти України велика увага приділяється кібератакам, а саме: хакерські атаки на урядові системи, енергетичні інфраструктури та спроби шпигунства через кібернетичні канали.

Так, 12 грудня 2023 року російські хакери під назвою угруповування «Сонцепік» здійснили масовану кібератаку на мобільну мережу України «Київстар» та на національний банк України «Монобанк», який зміг протистояти даній кібератаці. Проте «Київстар» зазнав великих втрат – безпосередньо більша частина інфраструктури була знищена та 27 мільйонів користувачів втратили змогу користуватися мобільним зв'язком та Інтернетом. Станом на сучасний момент Служба безпеки України вже відкрила кримінальне провадження за фактом кібератаки на «Київстар».

Характер військового конфлікту між Росією та Україною в сучасний час характеризується впли-

вом на інформаційну безпеку України з застосуванням традиційних і нетрадиційних елементів. Інформаційна війна формує динаміку конфлікту, яка відкриває перед міжнародною спільнотою нові глобалізаційні загрози на інформаційну безпеку України.

Висновки з проведеного дослідження. Значний вплив глобальних викликів на інформаційну безпеку в Україні зумовлений тим, що країна здобула державну незалежність у період, коли процеси неоліберальної глобалізації досягли у світі свого апогею. За таких умов процес відродження національної свідомості, формування внутрішніх національних символів та життєвих цінностей з самого початку обумовлювався значною роллю трендів глобального впливу. Незважаючи на те, що інституційна складова державної інформаційної політики в Україні представлена доволі широко, але враховуючи приклад більш розвинених країн, необхідно зосередитись на вдосконаленні цієї системи.

В теперішній час російська агресія та підвищена активність в кіберпросторі є головним викликом для України у сфері забезпечення інформаційної безпеки. Тому Україні доцільно застосовувати світовий досвід забезпечення інформаційної кібербезпеки та боротьби з інформаційними злочинами. Необхідно посилити співпрацю між країнами, розвивати міжнародні стандарти та спільні стратегії, а також підвищувати кіберсвідомість серед громадян та підприємств. Боротьба з кіберзагрозами та інформаційними злочинами вимагає комплексного та постійного підходу для забезпечення стабільності та безпеки сучасного суспільства.

Список використаних джерел:

1. Лужецький В.А., Войтович Р.П., Кожухівський А.Д. та ін. Основи інформаційної безпеки : посібник. Черкас. держ. технол. ун-т. Черкаси : ЧДТУ, 2008. 243 с. URL: http://voytovych.vk.vntu.edu.ua/file/329641c3933b8b8cbe161af0c43785ee.pdf (дата звернення: 08.12.2023).

2. Декларація тисячоліття ООН. URL: http://www.un.org/ru/documents/decl_conv/declarations/summitdecl.shtml (дата звернення: 10.12.2023).

3. AAAS American Association for the Advancement of Science. Science for all Americans: Project 2061. Oxford University Press, New York, 1989. URL: http://www.project2061.org/publications/sfaa/online/sfaatoc.htm (дата звернення: 10.12.2023).

4. Global trends 2030: alternative worlds a publication of the National Intelligence Council. December 2012. NIC 2012-001. P. 35–44. (дата звернення: 11.12.2023).

5. Золотухін Д. Меметична зброя як інструмент смислової війни РФ проти України. URL: https://matrix-info.com/memetychna-zbroya-yak-instrument-smyslovoyi-vijny-rf-proty-ukrayiny (дата звернення: 12.12.2023).

6. Писаренко Л. М. Фейки як інструменти інформаційної війни. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття* : матеріали міжнар. наук.-практ. конф. Одеса, 17 червня 2022 р. Одеса : Видавничий дім «Гельветика», 2022. Т. 1. С. 859–861.

7. Концепція розвитку штучного інтелекту в Україні : Розпорядження Кабінету міністрів України від 02.12.2020 р. № 1556-р URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 12.12.2023).

References:

1. Luzhetskyi V. A., Voitovych R.P., Kozhukhivskyi A. D. ta in. (2008) Osnovy informatsiinoi bezpeky: posibnyk. Cherkas. derzh. tekhnol. un-t. Cherkasy: ChDTU, 243 p. (accessed December 8, 2023). (in Ukrainian)

2. Deklaratsiia tysiacholittia OON. Available at: http://www.un.org/ru/documents/decl_conv/declarations/summitdecl.shtml (accessed December 10, 2023).

3. AAAS American Association for the Advancement of Science (1989) Science for all Americans: Project 2061. Oxford University Press, New York. Available at: http://www.project2061.org/publications/sfaa/online/sfaatoc.htm (accessed December 10, 2023).

4. Global trends 2030: alternative worlds (December, 2012) a publication of the National Intelligence Council. NIC 2012-001. Pp. 35–44. (accessed December 11, 2023).

5. Zolotukhin D. (2022) Memetychna zbroia yak instrument smyslovoi viiny RF proty Ukrainy. Available at: https://matrix-info.com/memetychna-zbroya-yak-instrument-smyslovoyi-vijny-rf-proty-ukrayiny (accessed December 12, 2023).

6. Pysarenko L. M. (June 17, 2022) Feiky yak instrumenty informatsiinoi viiny. *Yevropeiskyi vybir Ukrainy, rozvytok nauky ta natsionalna bezpeka v realiiakh masshtabnoi viiskovoi ahresii ta hlobalnykh vyklykiv XXI stolittia*: materialy mizhnar. nauk.-prakt. konf. Odesa: Vydavnychyi dim "Helvetyka", vol. 1, pp. 859–861.

7. Kontseptsiia rozvytku shtuchnoho intelektu v Ukraini (2020). Rozporiadzhennia Kabinetu ministriv Ukrainy vid 02.12.2020 r. No. 1556-r. Available at: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (accessed December 12, 2023).

E-mail: t.i.alekseeva@gmail.com