

ГО «ГРУЗИНСЬКО-УКРАЇНСЬКИЙ ЕКСПЕРТНИЙ ЦЕНТР»

**СУЧАСНІ ЗАГРОЗИ
ГЛОБАЛЬНІЙ ТА РЕГІОНАЛЬНІЙ
БЕЗПЕЦІ**

МАТЕРІАЛИ

Міжнародної науково-практичної інтернет-конференції
(м. Одеса, 29 жовтня 2023 року)

DOI: 10.46340/GUEC2023-10

Одеса
Фенікс
2023

Редакційна колегія:

Гардапхадзе Тамара – доктор юридичних наук, професор, ректор Нового закладу вищої освіти «Newuni» (м. Тбілісі, Грузія);

Донов Олексій – голова Департаменту експертно-аналітичної діяльності щодо взаємовідносин Грузії та України ГО «Грузинсько-український експертний центр» (м. Одеса, Україна);

Полухіна Аліна (укладач) – кандидат політичних наук, засновниця ГО «Грузинсько-український експертний центр» (м. Одеса, Україна);

Польовий Микола – доктор політичних наук, професор, Університет імені Коминського (м. Братислава, Словачія); засновник ГО «Грузинсько-український експертний центр» (м. Одеса, Україна);

Хаджинов Ілля – доктор економічних наук, професор, ректор Донецького національного університету імені Василя Стуса (м. Вінниця, Україна);

Хевцуріані Аміран – кандидат наук з міжнародних відносин, засновник ГО «Грузинсько-український експертний центр» (м. Одеса, Україна); професор академічної кафедри політики та міжнародних відносин Грузинського технічного університету (м. Тбілісі, Грузія);

Цокур Євген – доктор політичних наук, професор, завідувач кафедри політології Запорізького національного університету (м. Запоріжжя, Україна).

Сучасні загрози глобальній та регіональній безпеці : матер. С 89 Міжнар. наук.-практ. інтерн.-конф. (м. Одеса, 29 жовтня 2023 р.) [Електронне видання] / уклад. А. Полухіна ; ГО «ГУЕЦ». – Одеса : Фенікс, 2023. – 394 с. – Укр., англ., груз. мовами.

ISBN 978-617-8395-01-8

Збірник матеріалів містить матеріали доповідей, поданих на Міжнародну науково-практичну інтернет-конференцію «Сучасні загрози глобальній та регіональній безпеці», що відбулася 29 жовтня 2023 року. Подані матеріали були розглянуті під час роботи дев'яти секцій: теоретичні та прикладні аспекти міжнародного співробітництва у сфері безпеки; криза сучасної системи міжнародної безпеки; регіональна безпека в нових геополітичних концепціях; основні стратегічні напрямки кібербезпеки; кіберзахист і національна безпека: український досвід; цифрова дипломатія в умовах трансформації системи міжнародної безпеки; фейки та дідфейки як інструменти негативного впливу на національну безпеку; фактчекінг як інструмент протидії в гібридній війні; державне управління та національна безпека.

Збірник адресовано науковим, науково-педагогічним працівникам, здобувачам закладів вищої освіти, громадським організаціям, журналістам, незалежним експертам і всім, хто цікавиться проблемами загроз глобальній та регіональній безпеці.

УДК 327.7:355.02

© ГО «Грузинсько-український експертний центр», 2023

© Колектив авторів, 2023

ISBN 978-617-8395-01-8

З М І С Т

ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ БЕЗПЕКИ

Чальцева О. М. Новий світопорядок в умовах конфліктного середовища	9
Daviti Khupenia, Omari Lortkipanidze Rethinking the concept of power in contemporary political and international relations.....	13
ლილი ხარჩილავა ამერიკის შეერთებული შტატებისა და ისრაელის სამხედრო-პოლიტიკური თანამშრომლობა	16
Клименко К. В., Ухналь Н. М. Новітні виміри міжнародної безпеки.....	22
Нечипоренко Т. М. Теоретичні та прикладні аспекти міжнародного співробітництва у сфері безпеки.....	28
Чупіс А. Д. «Гібридний мир»: загроза чи панацея?.....	34
სალომე გოგიშვილი კოოპერატიული უსაფრთხოების თეორიული და პრაქტიკული ასპექტები თანამედროვე საერთაშორისო ურთიერთობებში	40
Іваницька О. П., Чальцева О. М. Особливості безпекової політики іспанії у ХХ – ХХІ сторіччях	47
Міщенко І. В. До питання відповідальності за міжнародними договорами про взаємний захист секретної інформації (на прикладі угоди з США)	53
Орленко В. В. Державний контроль як складова міжнародного співробітництва у сфері безпеки.....	57
Рашевська К. Є. Ре-глобалізація як середовище заохочення та розвитку системи прав людини.....	60
Дем'янюк О. Б. М Міжнародне співробітництво з питань енергетичної безпеки.....	65
Фоменко Д. І. Трансформація системи міжнародного співробітництва в умовах російсько-української війни.....	69

Мосієнко О. В., Якобчук В. П. Бренд України у світовому просторі.....	74
გიორგი კლიმაშვილი საერთაშორისო ურთიერთობათა სუბიექტის მნიშვნელობა	78
Козка А. В., Білик А.С. Космічні аномалії як об'єкт наукових досліджень: неоромантика та міжнародний фактор безпеки	81

КРИЗА СУЧАСНОЇ СИСТЕМИ МІЖНАРОДНОЇ БЕЗПЕКИ

Бадер А. В. Російсько-українська війна крізь призму логіки функціонування капіталістичної світ-економіки.....	85
Цокур Є. Г., Чайка І. Ю. Безпекові стратегії в умовах сучасних викликів: новий погляд на симулякр безпеки.....	90
Юлдашев О. Х. Концепція усунення загроз глобальній та регіональній безпеці.....	94
Волторніст О. С. Розмивання традиційних парадигм безпеки: виклики сучасній системі міжнародної безпеки.....	103
Литвин Ю. В., Лакіза В. В. Вплив економічних криз на міжнародну безпеку: шляхи їх подолання.....	107
Швець К. А. Безпека України в міжнародному контексті сучасності.....	111
Фурсай О. В. «Вакцинодемія» як елемент світового гібридного протистояння демократії та автократії.....	115
Прищеп Р. П. REALPOLITIK як практика економічного тиску.....	121

РЕГІОНАЛЬНА БЕЗПЕКА В НОВИХ ГЕОПОЛІТИЧНИХ КОНЦЕПЦІЯХ

Бусленко В. В. Україна в безпековій політиці Республіки Польща...	125
Стець А. М. Безпека Польщі та України.....	131
Тодоров І. Я., Тодорова Н. Ю. Стійкість та опорність України в контексті євроатлантичної інтеграції	136
ქეთი ჯიჯეიშვილი საქართველო ევროპული ინტეგრაციის გზაზე ..	141

გიორგი ჩხიკვიშვილი საქართველოს ევროპული არჩევანი: ისტორიულ -პოლიტიკური ექსკურსი	147
Gvantsa Abesadze Alignment of Georgia's foreign policy with the European union's foreign and security policy on the path of integration.....	151
Вовченко О. В. Контроль за иноземними субсидіями як фактор регіональної економічної безпеки Європейського Союзу	155
Мацишина І. В. До поняття моралі політичного реалізму в умовах війни.....	159
Райков А. Е. Війна в Нагірному Карабаху як чинник геополітичних змін у регіоні Південного Кавказу	164
Ціватий В. Г. Концепт «кризова дипломатія» і регіональна безпека в умовах трансформації системи міжнародних відносин XXI століття: геополітичний, інформаційно-комунікаційний та інституціональний дискурси	169

ОСНОВНІ СТРАТЕГІЧНІ НАПРЯМКИ КІБЕРБЕЗПЕКИ

Завгородня Ю. В. Політична кіберкультура як елемент кіберстабільності.....	174
Климчук Д. О. Кібербезпека процесу проведення виборів	179
Кучмії О. П. Кібербезпека як складова стратегії протидії гібридним викликам і загрозам ЄС	182
Кузьмич В. М. Основні стратегічні напрямки кібербезпеки.....	187
Сімакова С. І. Актуальні питання кібербезпеки в українському суспільстві	191
Суський Г. В. Кібербезпека у проблемному полі гібридної війни.....	195
Гуменюк Н. І., Ангельська В. Ю., Матвійчук М. В., Поляруш В. В. Безпілотні літальні апарати: виклики та перспективи сьогодення... 200	
Крошка Н. В. Діагностування інтернет-залежності у воєнний час в контексті кібербезпеки	205
Кондратенко А. О. Важливість забезпечення безпеки в логістиці	209

КІБЕРЗАХИСТ ТА НАЦІОНАЛЬНА БЕЗПЕКА: УКРАЇНСЬКИЙ ДОСВІД

Гринік А. В., Ярошевська Т. В. Проблемні питання забезпечення кібербезпеки України	213
Дубель М. В. Цифрові віруси як сучасна загроза національній безпеці.....	218
Горошко О. Л. Перспективи навчання кібербезпеки в освітніх інституціях.....	222
Обіход Т. В., Біленчук П. Д. Кібербезпека України: досягнення і перспективи її забезпечення	227
Галюга К. М., Орел О. В. Як захистити свої особисті дані від кібератак	232
Кондратьєва К. А. Місцева електронна демократія України в умовах воєнного стану: питання ефективності.....	237
Хариневич М.-М. С. Протидія загрозам національній безпеці в інформаційному просторі: досвід України.....	241
Снитко В. В. Кіберзахист та національна безпека: український досвід.....	244
Літинська В. А. Актуальність кібербезпеки у маркетинговій аналітиці.....	247

ЦИФРОВА ДИПЛОМАТІЯ В УМОВАХ ТРАНСФОРМАЦІЇ СИСТЕМИ МІЖНАРОДНОЇ БЕЗПЕКИ

Хорішко Л. С. Особливості співпраці України та НАТО у сфері кібербезпеки.....	251
Калашлінська М. В. Роль цифрових технологій у підтримці медіації та переговорів в сучасних політичних процесах	255
Сокоринський В. О. Цифровий тоталітаризм як загроза сучасній цифровій дипломатії	258
Рогозіна А. В. Цифрова дипломатія: інформаційний фронт України в умовах війни з росією	262

ФЕЙКИ ТА ДІПФЕЙКИ ЯК ІНСТРУМЕНТИ НЕГАТИВНОГО ВПЛИВУ НА НАЦІОНАЛЬНУ БЕЗПЕКУ

Вовк С. О. Технологічні аспекти створення дїпфейків та їх наслідки для національної безпеки.....	266
Федорова А. І. Фейки російської пропаганди щодо історії України та способи протистояння їм.....	270
Шеломовська О. М. Фейк-нюз в соціальних мережах: соціологічний аналіз.....	274
Медведська В. Ю. Дїпфейки як загроза розвитку та ефективного функціонування делїберативної демократії в Україні.....	279
Лисичкіна І. О., Лисичкіна О. О. Фейкові новини в сучасному медійному просторі.....	283
Орел О. В. Фейк як інструмент побудови наративу.....	288
Новік А. К. Російські фейки як фактор ризику національної безпеки України.....	294

ФАКТЧЕКІНГ ЯК ІНСТРУМЕНТ ПРОТИДІЇ В ГІБРИДНІЙ ВІЙНІ

Суська О. О. «Образ суспільства» та його трансформації в умовах гібридної війни.....	298
Олексунь Н. О., Седляківська К. Г. Загрози та механізми протидії російській пропаганді в умовах війни.....	304
Сушко В. А. Національна та етнічна ідентичність українців в умовах війни (на прикладі Харківщини).....	308

ПУБЛІЧНЕ УПРАВЛІННЯ ТА НАЦІОНАЛЬНА БЕЗПЕКА

Примуш М. В. Реформи в обмін на зброю.....	312
Сарибаєва Г. М. Митна безпека в системі національної безпеки України: термінологічний дискурс.....	315
Абакіна-Пілявська Л. М. До питання динаміки кримінального закону в умовах воєнного стану.....	320
Гученко К. В. Значення особливості структури особистості суб'єкта злочину дезертирство для національної безпеки.....	323

Бобось О. Л. Вплив глобальних криз на захист прав споживачів та можливості публічного управління в Україні	329
Ніколаєв К. Д. Екологічні виміри гібридної війни: вплив сучасних загроз на національну та регіональну безпеку.....	331
Мерзлюк Л. В. Публічно-громадське партнерство та міжнародна співпраця в управлінні регіональною безпекою в умовах сучасних загроз.....	334
Шевченко Р. П. Загрози глобальної та регіональної безпеки та їх вплив на ветеранів війни і членів їх родини.....	337
Конопля А. І., Лисиця В. В. Цифрова гігієна як засіб формування навичок безпечної роботи в мережі інтернет у дітей дошкільного віку	339
Гуральський Н. Р. Пропозиції державного регулювання засобів масової інформації	343
Ліщук А. О. Публічне управління навчальними закладами на регіональному рівні	347

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ДЕТЕРМІНАНТИ ФОРМУВАННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Милосердна І. М. Основні загрози інформаційній безпеці як елементу забезпечення національної безпеки	350
Варнавська І. В. Емоційне вигорання як психологічний феномен ...	355
Бондаренко С. Ю., Вітомський Ю. Л. Психологічні чинники формування національної безпеки держави	359
Лихотоп І. В. Схильність курсантів до навчання.....	364
Бутко О. М., Загоровська М. В., Савченко Л. Л. Інформаційна безпека під час війни.....	369
Куля І. Ф., Беженар К. Д. Інформаційна безпека підприємства	374
Куля І. Ф., Пирлог О. С. Кібергігієна у інформаційному просторі в умовах воєнного стану	381
Куля І. Ф., Спиридонова В. В. Безпека підприємства як основний вид діяльності менеджера підприємства	385
სამათ შამუგია HR მენეჯერის ინოვაციური სტრატეგია გლობალური პანდემიის გამოწვევის ფონზე	389

ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ БЕЗПЕКИ

Чальцева Олена Михайлівна
доктор політичних наук, професор,
Донецький національний університет імені Василя Стуса,
м. Вінниця, Україна
ORCID: 0000-0003-3922-7619

НОВИЙ СВІТОПОРЯДОК В УМОВАХ КОНФЛІКТНОГО СЕРЕДОВИЩА

Світова система в сучасних турбулентних умовах знаходиться в стані свого оновлення і переформатування. Відбувається деконструкція крихкого міжнародного порядку, який базувався на загальноприйнятих після Другої світової війни «правилах гри», встановлених Організацією Об'єднаних націй (ООН) і прийнятих всіма членами цієї універсальної організації в якості імперативних норм і правил поведінки у зовнішньому середовищі, а також як гарантія недопущення глобальних протистоянь і вирішення існуючих міжнародних конфліктів. Звісно, що це не був ідеальний порядок без конфліктів, війн, порушень міжнародного права і людських втрат, скоріше це був конструкт, який тримався, керуючись певними правилами в умовах протистояння національних інтересів держав.

Яким буде новий світовий порядок поки передбачити вкрай складно, актори міжнародних відносин обрали, або намагаються обрати своє місце в світовій системі координат в умовах сучасного конфліктного середовища і визначити власну позицію по відношенню до війн, які відбуваються в Європі (російсько-українська війна) і на Близькому Сході (Ізраїль – Хамас). Нова архітектура світопорядку багато в чому буде залежати

від результатів цих війн і позиції впливових держав в означених процесах. Політика держав у зовнішньому середовищі є продовженням їх національних інтересів, які на думку класика постмодерністського підходу Дж. Розенау представляють собою систему висновків, що виходять з аналітичної і ціннісної бази політики (Rosenau, 1968).

Питання національних інтересів розроблялося в реалістичній, ідеалістичній та суб'єктивній парадигмах такими зарубіжними авторами як Г. Моргентау, Р. Арон, В. Вільсон, Дж. Кеннан, Р. Нібур, Дж. Розенау, Н. Спайкмен та інші. В кожному підході були спроби пояснення впливу внутрішніх і зовнішніх факторів на формування національних інтересів держав, а також рефлексій стосовно співіснування національних систем в сучасній на той час моделі світу.

Країни, які живуть за законами демократії (умовно віднесемо їх до західного світу) знайшли рецепт співіснування в середині своїх систем різних інтересів, який базується на двох постулатах. По-перше, це наявність регульованого середовища, яке нівелює через різні унормовані правила і процедурні практики нерівність, що в свою чергу формує певну збалансовану сферу взаємодії акторів політичного процесу. По-друге, за період свого існування демократичні держави сформували певні паттерни поведінки влади і суспільства в умовах конфліктів і традиції їх регулювання в своїх системах. Проте, слід зауважити, що у світовому середовищі, яке є анархічним і конфліктним, філософія демократичних держав в своїй зовнішньополітичній діяльності не може в повній мірі керуватись цими постулатами. Фактор сили наразі повертається як обов'язкова умова фізичного існування західного світу, підтвердженням цього є розширення за рахунок нових членів Фінляндії і Швеції воєнно-політичного блоку НАТО, можливість застосування сили у разі територіальної небезпеки для країн НАТО (пункт про колективну оборону статті 5 Північноатлантичного договору), збройна допомога країнам, які знаходяться в стані війни (Україні, Ізраїлю), проведення миротворчих операцій ООН та ін.

Керуючись результатами досліджень проблеми національних інтересів можна зробити висновок, що ресурсна можливість

держав/акторів (економіка, природні, демографічні, воєнні, технологічні, інформаційні ресурси та ін.) відіграє суттєву роль в їх амбіціях у зовнішньому середовищі і формує моделі поведінки на міжнародній арені. На перший погляд це є очевидним і цілком може бути обґрунтованим сучасними теоретичними парадигмами міжнародних відносин (неореалізмом, неолібералізмом, неомарксизмом, постмодернізмом). Проте, є і певний парадокс, держави/актори (умовно ми їх відносимо до незахідного світу) з незначними, або нерівномірними ресурсами можуть виражати себе досить агресивно і формувати «зони нестабільності» в світовій політиці, керуючись своїм світосприйняттям, бажанням встановлювати «історичну справедливість» силовим шляхом. Останнім часом до групи таких держав можна віднести: росію, Іран, Північну Корею. До дестабілізаторів світової системи слід також додати і недержавних акторів, таких як терористичні угруповання (Хамас, ІдІл).

Однією із основних проблем наукового обґрунтування концепції національних інтересів до сих пір залишається проблема співвідношення національних інтересів і домінуючих цінностей в державі. Ціннісно-ідеологічний фактор виступає матрицею національних інтересів держав і основою для екзистенційних конфліктів у світовій політиці. Отже, можна передбачити, що нова конструкція світопорядку буде формуватися навколо ціннісностей акторів західного і незахідного світів.

Отже, в сучасному глобальному просторі зіткнулись різні філософії розуміння буття, які співіснують в екзистенційній конфліктологічній парадигмі, що безальтернативно веде до сприйняття тих, у кого інше уявлення про цей світ як загрозу. Ціннісних антиподів (державних і недержавних акторів) в інформаційному полі (внутрішньому і зовнішньому) представляють відповідно своїй логіці і етноцентристській позиції еліт, демонструючи негативний образ ворога і невідворотність боротьби з ним. Незахідний світ все частіше використовує пропагандистську риторику на основі переважно вигаданих і технічно сфабрикованих фактів як в середині системи, так і в міжнародному інформаційному просторі.

Західний світ не так агресивно веде інформаційну політику, керуючись в цілому певними морально-етичними і юридичними обмеженнями і часто програє, як наприклад розгорнутою після вторгнення Хамасу в Ізраїль з хвилею антисемітизму у світі.

Таким чином, світ перебуваючи в стані екзистенційного конфлікту, формує нову міжнародну систему, яка буде побудована на основі ціннісних протиріч, які в свою чергу будуть відправною крапкою в перманентному протистоянні національних інтересів державних і нових вимог недержавних акторів, що веде до високої вирогідності масштабування збройних міжнародних конфліктів і концентрації зусиль західного світу на стримуванні глобальної катастрофи і проявів абомінації незахідного світу.

Література

Rosenau, J. (1968). National Interest. *International Encyclopedia of the Social Sciences*, 11, 34–40.

Morgenthau, H. J. (1982). *In Defense of the National Interest*. University Press Of America.

Daviti Khupenia

*Doctor of Philosophy (Ph.D.) in International Relations,
Georgian Technical University, Tbilisi, Georgia
ORCID: 0000-0003-3909-5652*

Omari Lortkipanidze

Georgian Technical University, Tbilisi, Georgia

RETHINKING THE CONCEPT OF POWER IN CONTEMPORARY POLITICAL AND INTERNATIONAL RELATIONS

The tragic events of the 20th century had a profound impact on political research, particularly in the study of central concepts within political science, such as power and force. The prevailing aversion to violence, often referred to as the use of force and the avoidance of conflict, significantly impeded research in the field of political science. Consequently, the contemporary concept of "power" has become susceptible to criticism and is frequently considered irrelevant. Nevertheless, certain scholars, like Harar, have shown that reevaluating classical concepts and proposing new theories can lead to more comprehensive and realistic scientific research.

Exploring the term "power" through the lens of contemporary events is a crucial challenge in the study of modern international relations. The phenomenon of power is typically approached in two directions within this context: as a tool wielded by states, involving the unity of material resources, and as a catalyst for the disruption of the international order. These perspectives, we believe, are one-sided as they neglect the dual nature of power and its degree of regularity. In essence, power possesses both a material and a metaphysical facet, encompassing psychological and spiritual dimensions. Furthermore, it serves not only as an instrument for dismantling systems but also as a creative force that establishes and sustains them.

It is our assertion that the contemporary mainstream understanding of the term "power" is not only outdated but also often

leads researchers astray. The inadequacy and analytical frailty of this paradigm are evident in the ongoing Russia-Ukraine conflict. Scholars are still attempting to describe the motivations and objectives behind the Kremlin's actions on February 24, resorting to mathematical formulas and searching for signs of Russia's national interests in this tragic bloodshed. It is essential to note that, as the war progresses, Moscow's proclaimed national interests are evolving. Initially aimed at neutralizing Ukraine and deterring NATO, these interests now extend to policies concerning China. This fluidity suggests that the Russian Federation may not be a purely rational actor driven by its own interests. Instead, it appears to be guided by the ambitions of an authoritarian ruler, making it essential to scrutinize the notion of "state interests of Russia" as a malleable, non-uniform phenomenon, often serving as a facade for propagandized ideals.

In this context, we aim to demonstrate that the concept of power transcends the conventional definition in international relations, where it is perceived as a resource utilized by a nation to safeguard and pursue its interests, or as a means to disrupt the international system. We contend that power has a more profound significance, serving as a natural regularity inherent in human creative and destructive tendencies, both materially and psychologically. Consequently, we propose the need for a more profound exploration of this concept.

We maintain that power is inherently ambivalent. On one hand, it carries the potential for anarchy and chaos, while on the other, it can establish order and create an institutionalized and legitimate coercive system, such as the state.

This theory is applicable to the realm of international relations as well, leading us to conclude that "power" plays a fundamental role in shaping and dismantling the international order. It embodies both creative and destructive potentials simultaneously.

The original concept of "power" was initially conceived as an ontological concept with inherent regularity. However, it has since evolved into a narrow, instrumental interpretation, primarily focused on material aspects. This transformation has been driven by a societal discomfort with acknowledging the inherent inequality and competitive nature of power distribution, which in turn creates elites,

privilege, social hierarchies, and more. In societies that uphold egalitarian values, acknowledging inherent inequality is unpopular. Consequently, the mainstream in social sciences has shifted toward distributive fields, focused on achieving universal well-being and artificial equality. This trend has also infiltrated the study of international relations, where the emphasis has shifted from the fundamental examination of power between states to the analysis of economic and material data.

An illustrative example of the inadequacy of this approach is the recent ranking in a prominent American analytical magazine, U.S. News, which ranked the Russian Federation third in the world in terms of military strength and Ukraine 14th. This ranking, as evident from the ongoing Russia-Ukraine conflict, lacks empirical credibility. Measuring a nation's power based solely on factors such as manpower, military budget, and equipment does not provide an objective assessment of a state's strength. This underlines the need for a new approach.

Consequently, we assert that it is critically important for the fields of political science and international relations to redefine and reassess the concept of "power." This involves clarifying the term, defining the problem, and exploring its characteristics. This becomes even more pressing in light of the Russia-Ukraine conflict, where the analysis of the strength of the Russian and Ukrainian states, their military capabilities, and their instruments of power is currently lacking a coherent and accurate framework.

References

- U.S.News: Power. URL: <https://www.usnews.com/news/best-countries/rankings/power>
- Harari (2018). *21 Lessons for the Twenty-first Century*. New York.
- Barnett, M., Duvall, R. (2005). Power in International Politics. *International Organization*. 59, 1, 39-75;
- Von Vacano, D. A. (2006). *The art of power: Machiavelli, Nietzsche, and the making of aesthetic political theory*. Lexington Books.

ლილი ხარჩილავა
საქართველოს ტექნიკური უნივერსიტეტის
ასოცირებული პროფესორი

ამერიკის შეერთებული შტატებისა და ისრაელის სამხედრო-პოლიტიკური თანამშრომლობა

2023 წლის 7 ოქტომბერს ისრაელში განხორციელებულმა ტერაქტმა კიდევ ერთხელ ცხდჰყო ტერორიზმთან ბრძოლის მნიშვნელობა. რომ ტერორიზმს არ შეიძლება მიეცეს გასაქანი, მითუმეტეს დიდი სახელმწიფოების მხრიდან. არადა ფაქტია, რომ დღემდე არსებული ტერორისტული აქტების უკან დიდი პოლიტიკა იდგა და სამწუხაროდ სწორედ დიდი სახელმწიფოები აფინანსებდნენ გარკვეულ ტერორისტულ ორგანიზაციებს თავიანთი პოლიტიკური მიზნების მისაღწევად. რასაკვირველია ჰამასი თავისით არ შექმნილა. მის უკანაც დიდი სახელმწიფოები იდგნენ, რაც კიდევ უფრო ართულებს ახლო აღმოსავლეთში შექმნილ ისედაც რთულ ვითარებას. ისრაელი იძულებული გახდა დაზის სექტორში სამხედრო მოქმედებები დაეწყო, რასაც ათასობით მშვიდობიანი მოქალაქეც ემსხვერპლა, მათ შორის ბავშვები. საერთაშორისო თანამეგობრობა გასხვაგვებულად აფასებს ისრაელის ქმედებებს. ზოგიერთმა მსხვილმა რეგიონულმა ლიდერმა მაგ. თურქეთმა უაღრესად ხისტი პოზიცია დაიკავა ისრაელის ქმედების მიმართ, მაგრამ ფაქტი ერთია, ისრაელი ვერ შეძლებდა წინ აღდგომოდა ესოდენ ბარბაროსულ თავდასხმებს, მის უკან რომ არ იდგეს მსოფლიოს ზესახელმწიფო – ამერიკის შეერთებული შტატები.

აქამდე, ჩვეულებრივ კონტექსტში, ხშირად გავიგონებდით, რომ ისრაელს ძლიერი დაზვერვა და უმაღლესი დონის შეიარაღებული ძალები გააჩნია. ეს შეიძლება მართლაც ასეა, მაგრამ ნებისმიერ შემთხვევაში ჩვენ მართებულად მივიჩნევთ პოლიტიკური რეალიზმის ერთ-ერთ წამყვან პოსტულატს, რომ საერთაშორისო არენაზე წამყვან როლს თამაშობენ დიდი სახელმწიფოები და პატარა

ქვეყნები ასე თუ ისე იძულებულნი არიან ფეხი აუწყონ დიდ აქტორთა გადაწყვეტილებებს. ისრაელის სიძლიერე, ვფიქრობთ, აშშ-ს სიძლიერეს ეფუძნება.

ამერიკის შეერთებულ შტატებისა და ისრაელის მჭიდრო სამხედრო პოლიტიკური თანამშრომლობა საყოველთაოდ აღიარებული ფაქტია, არა მარტო სამეცნიერო წრეებში, არამედ მსოფლიოს ფართო საზოგადოებრივ სპექტრში. ეს ორი, მსოფლიო არენაზე უმნიშვნელოვანესი სახელწიფო, ერთმანეთს არსებულმა საერთაშორისო გეოპოლიტიკურმა ვითარებამ დაახლოვა.

თავიდან 1948 წელს, როდესაც ისრაელის სახელმწიფო შეიქმნა, ეს იყო უდიდესი მოვლენა ებრაული ხალხის მრავალსაუკუნოვან ისტორიაში და ეს ებრაელი ხალხის უპირველესი დამსახურება იყო, მაგრამ აქვე უნდა ითქვას, რომ ამ ისტორიულ პროცესებს მაშინ ხელი შეუწყო საბჭოთა კავშირმა და პირადად სტალინმა, რომელსაც სურდა ისრაელი საბჭოთა კავშირის დასაყრდენი გამხდარიყო ახლო აღმოსავლეთში. ამავდროულად საბჭოთა პოლიტიკური ხელმძღვანელობა ფიქრობდა, რომ აქ ექნებოდა სმხედრო ბაზები და გარანტირებული ექნებოდა სამხრეთის საზღვრების უსაფრთხოება (ხარჩილავა ლ, 2021, გვ. 111).

საბჭოთა კავშირის პოლიტიკურ ხელმძღვანელთა აზრით, ისრაელის სახელმწიფოს შექმნა ხელს შეუწყობდა საბჭოთა კავშირის პერსპექტივაში გავლენა აღედგინა ირანსა და თურქეთზე. ამან აშშ-ში შემფოთება გამოიწვია, რომელმაც იმთავითვე დაიწყო მოქმედება კრემლის ექსპანსიის შესაჩერებლად. ვაშინგტონში ფიქრობდნენ თურქეთის მიმართულებით გაეგზავნათა სამხედრო ფლოტი, მათ შორის ახალი ავიაბაზიდი „ფრანკლინ რუზველტი“ (ხარჩილავა ლ, 2021, გვ. 111). ისტორიის ამ ეტაპზე კრემლის მესვეურები სიტუაციის გამწვავებას მოერიდნენ, რადგან ეს ყოფილ მოკავშირეებს შორის გლობალურ სამხედრო დაპირისპირებაში შეიძლებოდა გადაზრდილიყო. შემდეგში განვითარებულმა მოვლენებმა კი გვიჩვენა, რომ ისრაელის მიმართ აშშ-ს ინტერესები უფრო გაიზრდებოდა და სწორედ აშშ გახდებოდა ისრაელის სამხედრო-პოლიტიკური მოკავშირე.

ახლო აღმოსავლეთში გართულებული ვითარების ფონზე აშშ-ისრაელის სამხედრო-პოლიტიკური თანამშრომლობა სწორედ

თანამედროვე ვითარებაში იძენს განსაკუთრებულ აქტუალობას. რომ არა აშშ-ისრაელის გონივრული ურთიერთქმედება, აღნიშნულ რეგიონში ვითარება შეიძლება კონტროლიდანაც კი გამოსულიყო, რითაც საერთაშორისო უსაფრთხოება კითხვის ნიშნის ქვეშ დადგებოდა.

აშშ-ისრაელის მჭიდრო თანამშრომლობა ამერიკელებს შესაძლებლობას აძლევს გაიზიარონ და გადაიღონ ისრაელის საბრძოლო გამოცდილება და მასთან დაკავშირებული ტექნოლოგიები, რაც დიდად წაადგება ამერიკული შეარაღების სისტემის მოდერნიზაციას. კერძოდ ამერიკულ ტაქტიკურ ავიაშემავსებელ Boeing KC707 (KC-137) Tanker/Transport-ზე დამონტაჟებულია ისრაელის სპეციალური აღჭურვილობა, რომელიც აუმჯობესებს თვითმფრინავის ტაქტიკურ-ტექნიკურ მახასიათებლებს. გარდა ამისა, ისრაელის უპილოტო თვითმფრინავები და ტანკსაწინააღმდეგო რაკეტები აშშ-ს მიერ წარმატებით იქნა გამოყენებული ერაყსა და ავღანეთში საომარი მოქმედებების დროს. საავიაციო უსაფრთხოების თვალსაზრისით კი ამერიკის შეერთებულმა შტატებმა ისრაელიდან ისესხა მფრინავთა დახურული (დალუქული) კაბინები და ბრონირებული კარები (ამერიკის შეერთებული). ამერიკულ აეროპორტებში აქტუალური ხდება ისრაელის უკანასკნელი ტექნოლოგიური მიღწევების გამოყენება მგზავრთა შემოქმედებისა და მათი ქვევუს მოდელების მიხედვით (ვაშინგტონის ახლო აღმოსავლეთის).

ორმხრივი თანამშრომლობის ფარგლებში ამერიკის შეერთებული შტატები და ისრაელი ერთობლივად ამუშავებენ რაკეტსაწინააღმდეგო თავდაცვის სისტემას „დავითის შურდული“ („Davids`s Sling“), რომელიც განსაზღვრულია დაბალ სიმაღლეზე მფრინავი დიდი სიშორის რაკეტების გასაწეიტრალეზად. ისინი ასევე ამუშავებენ რაკეტსაწინააღმდეგო თავდაცვის „Arrow“ (მოდულირება 2 და 3), რომელიც საშუალო და დიდ რადიუსზე მოქმედებს.

სამხედრო ტექნიკის გარდა აშშ ახლო აღმოსავლეთის რეგიონს ქვეყნებს, კერძოდ ისრაელს, ეგვიპტესა და იორდანის ფინანსურ-სამხედრო დახმარებასაც უწევს. ამერიკული სამხედრო დახმარების მოცულობით ეგვიპტე და იორდანია მეორე და მესამე ადგილებს

ინაწილებენ ისრაელის შემდეგ და ისინიც ამერიკის შეერთებული შტატების ძირითადი მოკავშირეები არიან რეგიონში და რომლებიც ასევე არ არიან ნატოს წევრები. 2015 წლითვის ამ ქვეყნების დაფინანსება შეადგენდა 1.3 მილიარდ აშშ დოლარს ეგვიპტისათვის, ხოლო 300 მილიონი აშშ დოლარს იორდანისათვის (Israel's Qualitative Military). მას შემდეგ რაც ისრაელმა ეგვიპტესა და იორდანისთან მშვიდობიანი თანამშრომლობა დაიწყო და არაერთ ხელშეკრულებას მოაწერა ხელი, არაბულმა სახელმწიფოებმა შეწყვიტეს ეგვიპტისა და იორდანისათვის დახმარების აღმოჩენა. ამ დანაკლისის შევსებას კი ამერიკის შეერთებული შტატები ახორციელებს.

ახლო აღმოსავლეთში სამხედრო საჭიროებისათვის ყველაზე დიდი ფინანსური დახმარების მიმღები სახელმწიფო ისრაელია. ამერიკის შეერთებულ შტატებსა და ისრაელს შორის 2007 წელს ხელი მოეწერა ხელშეკრულებას სამხედრო ურთიერთდახმარების შესახებ 10 წლის ვადით. შეთანხმების თანახმად აღმოჩენილი სამხედრო დახმარება ყოველწლიურად იზრდებოდა და 2018 წლისათვის წელიწადში 3.1 მილიარდ აშშ დოლარს შეადგენდა (აშშ-ისრაელის სტრატეგიული პარტნიორობის 2014 წლის აქტი). ისრაელს ამერიკული დაფინანსება ასევე შეეძლო გამოეყენებინა საკუთარი წარმოების შეიარაღების შესასყიდად. 2016 წელს ამერიკის შეერთებულმა შტატებმა და ისრაელმა ხელი მოაწერეს ისტორიულ შეთანხმებას სახმედრო დახმარების შესახებ, რომელიც იმოქმედებს 2019-2028 წლებში და ამერიკულ ფინანსურ დახმარებას ისრაელი ყოველწლიურად მიიღებს 3.8 მილიარდი ამერიკული დოლარის სახით (Петрова, 2009).

ამერიკის შეერთებული შტატები ითვალისწინებს რა იმ გარემოებას, რომ ისრაელი მისთვის ახლო აღმოსავლეთში ერთ-ერთი უმთავრესი მოკავშირეა, სურს მიაღწიოს რეგიონში ისრაელის ხარისხობრივ და თვისებრივ სამხედრო უპირატესობას, რომელიც ამერიკის შეერთებულ შტატებში საკანონმდებლო დონეზეა აყვანილი. (Qualitative Military Edge) (Воинственный Израиль, 2012). ამ კონცეფციის თანახმად, ისრაელს უნდა შეეძლოს ეფექტურად დაუპირისპირდეს ჩვეულებრივ სამხედრო საფრთხესა თუ მუქარას, რომელიც მოდის ერთი ან რამდენიმე სახელმწიფოსგან

თუ არასახელმწიფოებრივი აქტორებიდან ისე, რომ თავად ჰქონდეს მინიმალური დანაკარგები, ეს იქნება ცოცხალი ძალა, თუ სამხედრო ტექნიკა. ეს შედეგი კი მიიღწევა ძლიერი შეიარაღებით, ბრძანებით, მართვით, კავშირით, დაზვერვითი მონაცემებით, დაკვირვებითა და დაზვერვის შესაძლებლობებით, რომელიც ტექნიკური მახასიათებლებით აშკარად უპირატესია ცალკე აღებული სხვა სახელმწიფოს, სახელმწიფოთა გაერთიანებასა თუ არასახელმწიფოებრივ სუბიექტებთან შედარებით (ფრიდმანი, 2012). 2014 წელს პრეზიდენტმა ბარაკ ობამამ ხაზი გაუსვა ამ პრინციპის ურყევობას და ხელი მოაწერა კანონს სტრატეგიული პარტნიორობის შესახებ (United States-Israel Strategic Partnership act 2014) (Rothkopf, 2015).

ამერიკის შეერთებული შტატების ახლოაღმოსავლურ პოლიტიკაში ისრაელთან სამხედრო-პოლიტიკური თანამშრომლობა ნაწილობრივ ატარებს ფაქტორის როლსაც. აშშ მჭიდრო სამხედრო-ტექნიკურ ურთიერთობებს ავითარებს ახლო აღმოსავლეთის რეგიონის პრაქტიკულად ყველა სახელმწიფოსთან: ყიდის იარაღს, ახორციელებს ერთობლივ პროექტებს, ბევრთან დადებული აქვს ხელშეკრულება ამ სფეროში. ამდენად ამერიკის შეერთებული შტატები ახლო აღმოსავლეთის ყველა თვის პარტნიორთან ურთიერთობებში ითვალისწინებს ისრაელის ფაქტორს, კერძოდ ეს ეხება იარაღის გაყიდვასა და იორდანისა და ეგვიპტესთან ურთიერთობებს. მიუხედავად ამისა, ისრაელი ამერიკის შეერთებული შტატების მყარი სამხედრო პარტნიორია ახლო აღმოსავლეთის რეგიონალურ პოლიტიკაში და მისი სტრატეგიული მოკავშირეა.

ამჟამად ისრაელიომშია ჩართული ჰამასის წინააღმდეგ, მაგრამ ჰამასის გვერდით სერიოზული ძალები დგანან. აშშ და დასავლეთი ერთის მხრივ აღიარებენ, რომ ისრაელს აქვს თავდაცვის უფლება, მაგრამ იმავდროულად ახსენებენ, რომ პალესტინელთა შორის მშვიდობიან მოსახლეობაში დიდ მსხვერპლს ისრაელი უნდა მოერიდოს. პოლიტიკური თვალსაზრით კი აშკარაა, რომ არაბულ სამყაროსა და ისრაელს შორის მშვიდობიანი თანაცხოვრების შესაძლებლობების კუთხით ბოლო დროს პოზიტიური ძვრები ამჟამად მთლიანად წყალში ჩაიყარა. თუ რამდენად მოხდება ომის

შემდეგ ამ მდგომარეობის გამოსწორება, ამას მომავალი გვიჩვენებს, თუმცა ცალსახაა, რომ ეს ძალზე მტკივნეული და წინააღმდეგობრივი პროცესი იქნება.

გამოყენებული ლიტერატურა

ხარჩილავა ლ (2021). ამერიკის შეერთებული შტატების პოლიტიკა ახლო აღმოსავლეთში, სადოქტორო დისერტაცია, საქართველოს ტექნიკური უნივერსიტეტი, თბ., 111.

ამერიკის შეერთებული შტატების მიერ საგარეო სამხედრო დაფინანსების ანგარიში, 2009-2015 წ. URL: <https://2009-2017.state.gov/t/pm/ppa/sat/c14560.htm>

ვაშინგტონის ახლო აღმოსავლეთის პოლიტიკის კვლევის ინსტიტუტი, ეიზენშტადტი მ., პოლოკი დ. მეგობრები ურთიერთსარგებლით: რატომ არის აშშ-ისრაელის ალიანსი კარგი ამერიკისთვის?. URL: <https://www.washingtoninstitute.org/policy-analysis/friends-benefits-why-us-israeli-alliance-good-america>

Israel's Qualitative Military Edge and Possible U.S. Arms Sales to the United Arab Emirates. URL: <https://crsreports.congress.gov/product/pdf/R/R46580>

აშშ-ისრაელის სტრატეგიული პარტნიორობის 2014 წლის აქტი. URL: <https://www.congress.gov/bill/113th-congress/house-bill/938>

Петрова, И. (2009). Новый взгляд на старую дружбу. სამეცნიერო სტატია. URL: www.mignews.com/news/analitic/world/260709_130408_77271.html

Воинственный Израиль (2012). URL: www.iran.ru/news/analytics/78722/Voinstvennyy_Izrail_Obzor_zarubezhnyh_SMI#prettyPhoto

ფრიდმანი, გ. (2012). ომი და ტყუილი: ირანი, ისრაელი და შეერთებული შტატები, სამეცნიერო სტატია. URL: <https://worldview.stratfor.com/article/war-and-bluff-iran-israel-and-united-states>

Rothkopf, D. (2015). Bibipalooza Is a Dangerous Distraction. URL: <https://carnegieendowment.org/2015/03/02/bibipalooza-is-dangerous-distraction-pub-59221>

Клименко Катерина Володимирівна

кандидат економічних наук,

ДННУ «Академія фінансового управління», м. Київ, Україна

ORCID: 0000-0001-8295-1333

Ухналь Наталія Миколаївна

доктор філософії з економіки,

ДННУ «Академія фінансового управління», м. Київ Україна

ORCID: 0000-0002-8562-9355

НОВІТНІ ВИМІРИ МІЖНАРОДНОЇ БЕЗПЕКИ

Загострення світових проблем як комплексу взаємопов'язаних суспільних негативних тенденцій і небезпек проявляється на глобальному, регіональному і національному рівнях, особливої уваги яким було приділено на Всесвітньому саміті зі сталого розвитку (World Summit on Sustainable Development). У результаті роботи саміту прийнято Йоганнесбурзьку декларацію зі сталого розвитку (UN, 2002) та визначено основні напрями протидії впливу дестабілізуючих чинників, що створюють серйозну загрозу сталому розвитку країн, серед яких світове ядерне роззброєння, економічна відсталість, корупція, соціальна несправедливість, екологічні, демографічні, продовольчі проблеми, раціональне використання природних ресурсів, криза в сфері охорони здоров'я тощо. Підкреслюється, що, з одного боку, внаслідок глобалізації відбувається інтенсифікація інвестиційних процесів, інтеграція товарних ринків, прискорення науково-технічного прогресу та поява новітніх ІКТ, з іншого – виникають нові проблеми і протиріччя значного розширення та відтворення світового виробництва.

Однак позитивні наслідки глобалізації розподіляються нерівномірно, а країни, що розвиваються, стикаються з особливими труднощами в ході зусиль щодо вирішення цих проблем. План виконання рішень саміту, затверджуючи необхідність в спільних ефективних діях для досягнення загального добробуту та процвітання через викорінення

злиденності, зміну моделей споживання і виробництва, геополітичну та геоеконімічну безпеку і раціональне використання природної ресурсної бази в інтересах соціально-еконімічного розвитку, обумовив найголовніші цілі та основні потреби стабільного розвитку.

З настанням світової фінансово-еконімічної кризи у 2008 р. світові лідери не раз наголошували на необхідності створення належної глобальної системи фінансового захисту і безпеки. За десять років, що минули з початку світової фінансової кризи, системи фінансового регулювання були удосконалені і рівень стійкості банківської системи став вищим, але виникають нові фактори уразливості та зростають ризики для світової фінансової стабільності у найближчій перспективі. Захисні механізми можуть забезпечити ліквідність під час системної кризи, зменшуючи стимул країн до накопичення надлишкових резервів з метою страхування від несприятливих потрясінь.

В умовах розгортання глобалізаційних процесів і становлення відкритого суспільства пошук шляхів забезпечення безпеки національних еконімічних та фінансових систем необхідно починати з вирішення проблем розвитку (еконімічного, соціального, політичного тощо) і базуватися не лише на захисті об'єктів глобальної безпеки від загроз та інших негативних впливів. Нова концепція забезпечення міждержавної еконімічної та фінансової безпеки повинна поєднувати в одне ціле новий постіндустріальний, ноосферний тип розвитку і забезпечення безпеки світової спільноти, тобто забезпечення гармонізації соціальних і еконімічних відносин, реалізацію принципу справедливості в його глобальному вимірі та безпеки позитивних глобальних процесів через перехід до сталого розвитку. Мова в цьому випадку йде про перехід до створення рівних можливостей і умов для задоволення життєво важливих потреб і раціонально орієнтованих інтересів етнонаціональних груп та корпорацій. Оскільки негативні наслідки закономірностей розвитку глобалізації та нециклічні еконімічні кризи продовжують впливати на рівень еконімічної безпеки держав світу, набуває гострої актуальності пошук шляхів та методів забезпечення фінансової безпеки.

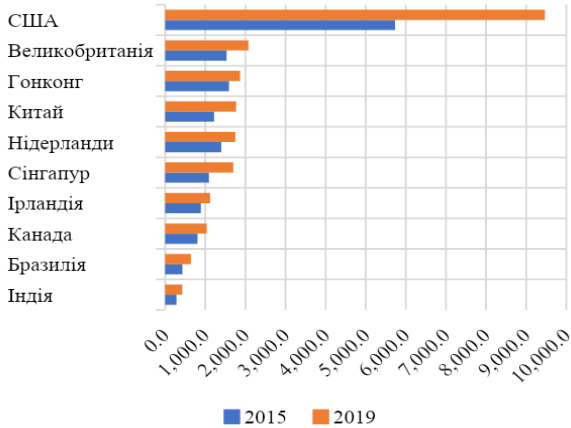
Світова економіка стикається з низкою складних проблем, пов'язаних з технологічним прогресом і глобалізацією, а також з триваючими наслідками фінансової кризи 2008-2009 рр., пандемічного шоку 2020-2021 р., російсько-української війни 2014-2023 рр. За оцінками експертів МВФ, пожвавлення глобальної економіки відбувається повільно, при цьому збільшуються розбіжності між регіонами, з найбільшим падінням світового виробництва в 2020 р. на рівні - 2,8, хоча відновлення зростання у 2021 р. склало 6,3%, у 2022 р. - 3,5% з наступним середньорічним прогнозом у 3,0% на 2023-2025 рр. (IMF, 2023). Визначено, що факторами уповільнення підйому світової економіки виступають зростаючий зовнішній фінансовий тиск на країни з ринком, що формується, помітне посилення проявів напруженості в торговельних відносинах, збільшення державного боргу, стримування інвестиційних потоків.

Існуюча міжнародна система інститутів протягом довгого часу поступово нарощувала потенціал регулюючого впливу на світову економіку. Такі організації як Міжнародний валютний фонд, Світовий банк, G-7, G-20, СОТ та регіональні структури здійснюють активні дії щодо впровадження інструментів фінансово-економічного впливу у міжнародну практику і розроблення принципів і норм функціонування економічних підсистем різного рівня (G-20, 2016). Однак стрімкий розвиток форм міжнародних фінансово-економічних операцій, що знаходиться за межами національного контролю, у просторово-часовому вимірі нівелювала регулюючу та контролюючу функції міжнародних інституцій. Рада з питань фінансової стабільності (Financial Stability Board), утворена як Форум у 1999 р., об'єднала національні органи, відповідальні за забезпечення фінансової стабільності, асоціації регулятивних і наглядових органів, що займаються виробленням стандартів і кращих практик, міжнародні фінансові інститути, а також експертні комітети центральних банків (FSB, n/d). За допомогою цієї установи в інтересах підвищення ефективності та забезпечення стабільності глобального фінансового середовища передбачалося запровадити нові підходи та форми співпраці регуляторно-наглядових органів на міжнародному та національному рівнях.

Забезпечення вільного опосередкованого трансферу фінансових ресурсів є характерною особливістю глобальної фінансової системи (Soros, 2005). Проте глобальний капітал переважно переміщується між розвиненими країнами, а в країнах, що мають менший рівень соціально-економічного розвитку, постійно спостерігається нестача капіталу. Таким чином, останні не мають можливостей для отримання позитивних наслідків фінансової глобалізації, а навпаки, відчують її негативний прояв. Водночас світовий фінансовий ринок функціонує за моделлю «центр-периферія», котра обумовлена концентрацією глобального фінансового капіталу в країнах цивілізаційного «центру», звідки перетікає в «периферійну зону» через фінансові інструменти безпосередньо або транснаціональні корпорації опосередковано. «Глобальним ядром» фінансового ринку, насамперед, виступає англосаксонський кластер (США та Великобританія), обсяги міжнародних фінансових угод котрого досягають 40 млрд дол. США, а також офшорні фінансові центри зони, в яких найбільша концентрація активних і мобільних фінансових капіталів (5 073 трлн дол. США) (WFE, 2019; BIS, 2019), в результаті чого виникла світова фінансова мережа, що об'єднала провідні фінансові центри. У 2019 р. головними реципієнтами глобального фінансового капіталу виступали США і Великобританія, а також тісно пов'язані з ними офшорні юрисдикції, що є підтвердженням функціонування такої моделі (рис. 1). У 2019 р. в 10 країнах концентрація кумулятивного обсягу прямих та портфельних іноземних інвестицій склала 59,9% та 65,1% відповідно.

Таким чином, будучи складним і неоднозначним процесом перерозподілу міжнародних потоків грошового капіталу через національні та світові фінансові ринки, який вкрай складно контролювати, кількісно фінансова глобалізація знаходить своє вираження у випереджальних темпах зростання міжнародного обміну товарами, послугами, технологіями та капіталом у порівнянні з ростом виробництва. Зростає вплив якісної складової наростаючої глобалізації – посилення взаємозалежностей та взаємозв'язків між національними господарствами.

10 найбільших реципієнтів прямих іноземних інвестицій, млрд дол., 2019 р.



10 найбільших реципієнтів портфельних іноземних інвестицій, млрд дол., 2019 р.

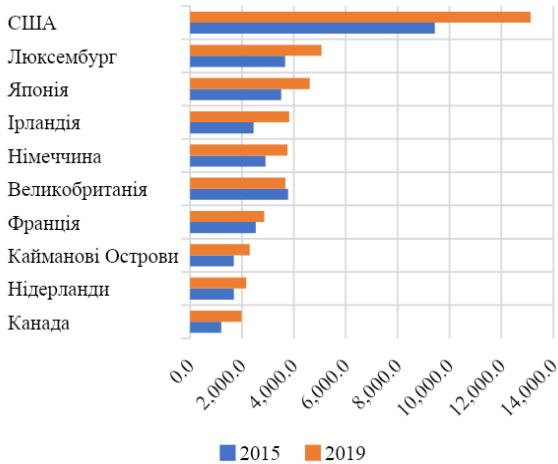


Рис. 1. Централізація глобального капіталу

Складено за: *Foreign direct investment: Inward and outward flows and stock, annual / UNCTAD*. URL: <https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx>; *Total Portfolio Investment Assets – Top 10 Reporting Economies / IMF*. URL: <https://data.imf.org/?sk=B981B4E3-4E58-467E-9B90-9DE0C3367363&slid=1481577897618>

Основними причинами динамічного розвитку фінансової глобалізації слід вважати: кардинальні якісні та кількісні зміни у сучасному світі; лібералізацію міжнародної торгівлі; міжнародну економічну інтеграцію; експансивну діяльність транснаціональних і мультинаціональних корпорацій; транснаціоналізацію потоків робочої сили; динамічний розвиток науки і техніки, розвиток інформаційних технологій та засобів зв'язку, розвиток виробничо-економічних та інформаційних мереж; посилення впливу найбільших міжнародних організацій і фінансових інститутів у міжнародних фінансово-економічних відносинах. Прискорення зеленого переходу, підвищення стійкості до кліматичних потрясень і покращення продовольчої безпеки потребують зміцнення багатосторонніх угод і дотримання заснованих на правилах платформ для міжнародної співпраці.

Література

Financial Stability Board. URL: <https://www.fsb.org/>.

Soros, G. (2005). *On globalization*. Public Affairs.

World Federation of Exchanges (2019). *Annual Statistics Guide*. URL: <https://www.world-exchanges.org/>.

Bank for International Settlements. *Locational banking statistics*. URL: <https://www.bis.org/>.

Johannesburg Declaration on Sustainable Development (2002, September 4). URL: <http://www.un-documents.net/>.

Leaders' Communique Hangzhou Summit (2016, September 4-5). G20. URL: <http://www.g20.org/>.

IMF. *World Economic Outlook: Navigating Global Divergences* (2023, October). IMF. URL: <https://www.imf.org/>.

Нечипоренко Тетяна Дмитрівна
кандидат економічних наук,
Вінницький технічний фаховий коледж, м. Вінниця, Україна
ORCID: 0000-0002-0690-1534

ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ БЕЗПЕКИ

Безпека є однією з найважливіших потреб людини, суспільства та держави. Вона виступає передумовою для розвитку та процвітання держави. У сучасному світі, який характеризується множинністю загроз, міжнародне співробітництво у сфері безпеки є ключовим фактором забезпечення глобального миру та стабільності. Актуальність теми дослідження міжнародного співробітництва у сфері безпеки обумовлена численними факторами, а саме:

- зростанням глобальних загроз і викликів. Світ стрімко змінюється, і з цим змінюються і загрози безпеці. Сьогодні людство стикається з такими глобальними проблемами, як міжнародний тероризм, кіберзлочинність, транснаціональна організована злочинність, незаконна міграція, екологічні катастрофи. Для успішного протистояння цим загрозам необхідне ефективне міжнародне співробітництво;

- розвиток глобальної системи безпеки. У післявоєнний період відбулося значне розширення міжнародної системи безпеки. Були створені численні міжнародні організації та інститути, які займаються питаннями безпеки, зокрема ООН, НАТО, ОБСЄ, СНД. Для ефективного функціонування цієї системи необхідне тісне співробітництво між державами-членами;

- необхідність створення єдиного міжнародного простору безпеки. У сучасному світі країни все більше взаємозалежні. Це вимагає створення єдиного міжнародного простору безпеки, в якому всі держави могли б почуватися в безпеці.

Для цього необхідне всебічне міжнародне співробітництво у сфері безпеки.

Міжнародне співробітництво у сфері безпеки – це форма взаємодії між державами та іншими суб'єктами міжнародного права, спрямована на запобігання та протидію загрозам національній та глобальній безпеці (Гузенко, Саєнко, 2022). Воно може здійснюватися в різних формах, таких як:

- дипломатичні переговори та консультації;
- міжнародні договори та угоди;
- об'єднання та співпраця в рамках міжнародних організацій;
- військова співпраця;
- співпраця в галузі безпеки людини.

Теоретичні основи міжнародного співробітництва у сфері безпеки лежать у таких галузях знань, як міжнародне право, міжнародні відносини, політична філософія та етика. До основних теоретичних основ міжнародного співробітництва у сфері безпеки відносимо:

– принцип суверенної рівності держав. Цей принцип передбачає, що всі держави є рівними незалежно від їхнього розміру, географічного розташування, економічного розвитку чи політичного режиму;

– принцип невтручання у внутрішні справи держав. Даний принцип свідчить про те, що держави не мають права втручатися у внутрішні справи інших держав, якщо це не передбачено міжнародним правом;

– принцип мирного вирішення спорів. Принцип закликає держав вирішувати свої спори мирними засобами, без застосування сили чи загрози її застосування;

– принцип колективної безпеки. Цей принцип має на увазі, що держави повинні співпрацювати в запобіганні та вирішенні конфліктів, щоб забезпечити колективну безпеку (Barry Posen, 2020).

Міжнародне співробітництво у сфері безпеки може здійснюватися в різних формах і напрямках. Основні форми міжнародного співробітництва у сфері безпеки:

– політичні консультації та переговори. Ці форми співробітництва спрямовані на запобігання та вирішення конфліктів шляхом діалогу та домовленостей між державами;

– створення міжнародних організацій та установ. Міжнародні організації та установи відіграють важливу роль у забезпеченні безпеки та стабільності в міжнародному співтоваристві;

– взаємодія в рамках міжнародних договорів та угод. Міжнародні договори та угоди є юридичною основою міжнародного співробітництва у сфері безпеки.

Основні напрями міжнародного співробітництва у сфері безпеки наступні:

– збройна безпека, цей напрям передбачає співробітництво в сфері роззброєння, контролю над озброєннями та нерозповсюдження зброї масового ураження;

– політична безпека, спрямовує співробітництво в сфері запобігання конфліктам, вирішення кризових ситуацій та зміцнення демократичних інститутів;

– економічна безпека, акцентує увагу на співробітництві в сфері забезпечення економічного розвитку, усунення бідності та боротьби з тероризмом;

– соціальна безпека, вбачає співробітництво в сфері захисту прав людини, забезпечення екологічної безпеки та боротьби з транснаціональною злочинністю (Беляков, 2021).

Для прикладу, кількість міжнародних угод та договорів у сфері безпеки збільшилася з 750 у 2020 році до 850 у 2022 році, кількість міжнародних організацій та установ, які займаються питаннями безпеки, підвищилась з 500 у 2020 році до 550 у 2022 році, кількість конфліктів і кризових ситуацій, які вдалося запобігти або вирішити за допомогою міжнародного співробітництва, зросло з 50 у 2020 році до 60 у 2022 році. Відповідно, міжнародне співробітництво у сфері безпеки залишається важливим фактором забезпечення безпеки та стабільності в міжнародному співтоваристві. У 2020-2022 роках спостерігалось зростання міжнародного співробітництва у сфері безпеки, зокрема в таких напрямках, як роззброєння та контроль над озброєннями, боротьба з тероризмом та транснаціональною злочинністю.

За 2020-2022 роки кількість міжнародних організацій та установ, які займаються питаннями безпеки, не змінилася. До їх числа входять: Організація Об'єднаних Націй (ООН), Організація

Північноатлантичного договору (НАТО), Організація Договору про колективну безпеку (ОДКБ), Шанхайська організація співробітництва (ШОС), Африканський союз (АС), Організація Американських держав (ОАД), Організація ісламської співпраці (ОІС), Європейський Союз (ЄС). За аналізовані роки ООН вдалося запобігти або вирішити 15 конфліктів і кризових ситуацій, що свідчить про ефективність міжнародного співробітництва у сфері безпеки.

Однак міжнародне співробітництво у сфері безпеки стикається з низкою проблем, серед яких окреслимо:

- недосконалість міжнародного права, яке не завжди забезпечує ефективне вирішення конфліктів і сприяє забезпеченню безпеки;

- нерівновага сил у світі, що може призводити до конфліктів і дестабілізації;

- посилення тероризму, який є серйозною загрозою для безпеки всього світу;

- зміна клімату, яка може призводити до конфліктів і дестабілізації (Сазонов, 2019).

На нашу думку, для вирішення вищенаведених проблем необхідно:

- удосконалювати міжнародне право, це можна зробити шляхом розробки нових міжнародних договорів і угод, які б забезпечували ефективне вирішення конфліктів і забезпечення безпеки. Крім того, необхідно забезпечити виконання існуючих міжнародних договорів і угод;

- забезпечувати рівновагу сил у світі, шляхом зміцнення міжнародних організацій, таких як ООН, які відіграють важливу роль у підтримці миру і безпеки, сприяти розвитку партнерських відносин між державами, які мають різні інтереси;

- боротьба з тероризмом передбачає посилення міжнародного співробітництва в сфері контртероризму, забезпечення розвитку демократичних інститутів і соціальної справедливості, які є основою для боротьби з тероризмом;

- відповідати на зміни клімату, що можна вирішувати шляхом вжиття заходів щодо скорочення викидів парникових газів і адаптації до наслідків зміни клімату (Mazarr, 2020).

Безперечно вирішенню проблем міжнародного співробітництва у сфері безпеки сприятимуть заходи: підвищення рівня довіри між державами за допомогою активізації політичного діалогу та співробітництва в різних сферах, розвиток міжнародних інститутів та установ, які відіграють важливу роль у забезпеченні безпеки та стабільності в міжнародному співтоваристві та сприяння розвитку демократії та соціальної справедливості, які є основою для забезпечення безпеки.

Отже, можна констатувати, що міжнародне співробітництво у сфері безпеки являє собою процес взаємодії між суб'єктами міжнародних відносин, спрямований на запобігання, попередження та вирішення конфліктів, забезпечення безпеки та стабільності в міжнародному співтоваристві. Міжнародне співробітництво у сфері безпеки є складним і багатограним процесом, який вимагає від держав відповідальності та взаєморозуміння. Для успішного розвитку цього співробітництва необхідно вирішити ряд проблем, які існують на його шляху, таких як відсутність довіри між державами, нестабільність міжнародної системи та інтерес окремих держав до забезпечення власної безпеки за рахунок інших. Для його ефективного розвитку необхідно: зміцнювати міжнародне право та міжнародні організації, розвивати міждержавні відносини та довіру, створювати нові форми міжнародної безпеки. Крім того, держави повинні бути готові до компромісу та співпраці з іншими державами для вирішення спільних проблем безпеки, міжнародні організації мають активізувати свої зусилля щодо запобігання та протидії загрозам національній та глобальній безпеці, а громадськість доречно інформувати про важливість міжнародного співробітництва у сфері безпеки.

Література

Беляков, О. М. (2021). Міжнародне співробітництво у сфері безпеки: теоретичні та прикладні аспекти. *Держава і право*, 10, 60-67.

Гузенко, О. І., Сасенко, А. В. (2022). Міжнародне співробітництво у сфері безпеки: сучасні проблеми та перспективи. *Вісник НУОУ*, 3, 13-21.

Сазонов, В. В. (2019). Міжнародне співробітництво у сфері безпеки: теоретичні та практичні аспекти. *Право та державне управління*, 2 (35), 1, 125-135.

Mahnken, T. J. (2020). The Future of International Security Cooperation: Challenges and Opportunities, *International Security*, 44, 3.

Mazarr, M. J. (2020). The Changing Landscape of International Security Cooperation, *Survival*, 62, 1.

Posen, B. (2020). International Security Cooperation in an Era of Great Power Competition, *Security Studies*, 29, 1.

Чупіс Анастасія Дмитрівна

Запорізький національний університет, м. Запоріжжя, Україна

ORCID: 0000-0002-3091-3332

«ГІБРИДНИЙ МИР»: ЗАГРОЗА ЧИ ПАНАЦЕЯ?

У 21 столітті вченими-політологами під час аналізу сучасних військових конфліктів активно використовується термін «гібридна війна». На початку 2000-х років концепцію «гібридної війни» висунув американський науковець та військовий у відставці Френк Г. Гоффман. Запропонована ним концепція швидко набула популярності та стала предметом чисельних наукових розвідок. У своїй науковій праці «Конфлікт у 21 столітті: розквіт гібридних воєн», що була опублікована у 2007 році Гоффман дав таке визначення: «Розмивання способів війни, розмивання розуміння того, хто воює та які технології застосовуються, що своєю чергою породжує широкий спектр різноманітності та складності, які ми називаємо гібридною війною. Гібридні війни можуть вести як держави, так і різні недержавні актори. Вони включають низку різних способів ведення війни, включаючи звичайні засоби, нерегулярні тактики та формування, терористичні акти, невибіркове насильство та примус, і кримінальні заворушення» (Hoffman, 2007, р. 14).

Тобто у своєму визначенні Гоффман підкреслює процес видозміни традиційного військового зіткнення, або конвенційної війни, де чітко відомі сторони конфлікту, якими є регулярні армії, які мають відповідну військову форму та символи приналежності до певного військового підрозділу та родів військових сил, де застосовується дозволена міжнародним правом зброя відповідно до права Гааги, а ставлення до військовополонених та цивільного населення відповідно до права Женеви. Проте його концепція наголошує на головному аспекті цих змін – всепроникаючому характеру нового типу військових конфліктів, розмитті кордонів між миром та війною.

Аналізуючи доробок українських науковців щодо вивчення концепції «гібридної війни» неможливо не згадати працю наукового колективу під керівництвом Володимира Горбуліна «Світова гібридна війна. Український фронт», що вийшла друком у 2017 році. Ця праця є ґрунтовною та охоплює як теоретичний огляд розвитку концепції «гібридної війни», так і її практичне застосування на прикладі війни РФ проти України. В монографії науковці визначають цей феномен як воєнні дії в ході яких застосовуються комплекс ресурсів, що складаються мілітарних, квазімілітарних, дипломатичних, економічних, інформаційних та інших засобі задля досягнення політичних цілей (Горбулін, 2017, с. 19).

Мабуть, найбільшою дилемою в дослідженні гібридної війни є питання її завершення. Адже безпосереднє завершення військових дій, в контексті гібридного конфлікту, не може гарантувати повного згортання протистояння, а не лише його перехід на інший рівень ведення: інформаційний, дипломатичний, економічний.

Оксфордський науковий словник визначає мир як ситуацію або період часу, коли в країні чи регіоні немає війни, чи насильства (Oxford English Dictionary). Але це визначення не дає нам розуміння чим є мир в умовах гібридної війни, коли де-юре війна не є оголошеною, вона може бути локалізованою, або мати низьку інтенсивність. Чи можемо ми тоді говорити про повний мир у його класичному розумінні? Прослідкувавши взаємозалежність цих феноменів: «війни» та «миру» можна помилково припустити, що протилежною за значенням концепції «гібридної війни» є концепція «гібридного миру». Проте концепція «гібридного миру» що існує на Заході не є протилежною, або розвиненою вслід концепції «гібридної війни» – вона є незалежним підходом в межах дослідження теорії миру.

Концепція гібридного миру була запропонована та розвинена в працях британських дослідників Олівера П. Річмонда та Роджера Мак Гінті в першому десятилітті 21 століття.

Концептуалізуючи цей феномен і Річмонд, і Мак Гінті у своїх наукових працях відштовхуються від теорії ліберального миру,

для якого характерними є сильні демократичні інститути та політичні процеси, економічна взаємодія, сильні міжнародні зв'язки між державами та міжнародні інституції, що їх забезпечують, а також повага до верховенства права та прав людини.

Розвиваючи свої ідеї, на основі відомої концепції норвезького соціолога Йогана Галтунга, який виокремлював «негативний» мир як стан суспільства, що характеризується відсутністю війни як такої та «позитивного» миру, що відрізняється ще й наявністю в суспільстві таких соціальних благ як справедливість, рівність та добробут (Galtung, 1969, p. 170) Річмонд за аналогією виділяє «негативний» гібридний мир та «позитивний» мир як феномени, характерні для постконфліктних суспільств. Ось як він їх визначає: «Негативні гібридні форми миру та пов'язані з цим політики можуть бути структурно насильницькими. З точки зору суб'єкта, ліберальна миротворча система також може бути структурно насильницькою, якщо вона змушує підкорятися чужим нормам, політичним системам або піддана впливу глобального капіталу через своє крихке становище. Позитивна гібридна форма миру не передбачає компромісу щодо потенційної емансипаційної та емпатійної природи миру, що несе з собою як місцеву, так і міжнародну легітимність. Воно ґрунтуватиметься на примиренні, примиренні, емансипації, автономії, соціальній справедливості та почутті звільнення. Інституції, засновані на цих концепціях і адаптовані до місцевого контексту, сприятимуть забезпеченню прав і потреб. Іншими словами, гібридна політика має потенціал каталізувати місцеве примирення, а також міжнародну та місцеву згоду щодо безпеки, культурної, політичної, економічної та соціальної динаміки миру» (Richmond, 2015, p. 60).

Мак Гінті ж аналізує гібридний мир крізь призму вертикалі взаємодії акторів, що беруть участь у його впровадженні, де гібридний мир виступає як результат взаємодії між міжнародними акторами, що здійснюють діяльність з впровадження миру та локальним рівнем реалізації цих підходів, з врахуванням унікальних рис, потреб та особливостей цього регіону. Тобто гібридність він вбачає саме в можливості

застосування іноземного досвіду, без сліпого копіювання або слідування запропонованих моделей, а його критичне осмислення, адаптацію і локалізацію, з врахуванням місцевої експертизи зі знанням регіону, де імплементується цей підхід. Прикладом такої моделі може слугувати впровадження Порядків денних Резолюції ООН 1325 «Жінки, мир, безпека» в країнах, що її імплементують. Країни, які імплементують ці документи розробляють національний план та його локальні робочі версії, які мають враховувати регіональну специфіку.

Аналізуючи ступінь дослідженості концепту гібридного миру українською науковою спільнотою треба зауважити, що він має високу актуальність через свою малодослідженість.

У статті українського дослідника Григорія Перепелиці «Концепція «гібридного миру» для України» у 2016 році було здійснено спробу осмислити воєнні та дипломатичні події на початку війни РФ проти України. Дослідник використовує термін «гібридний мир», але визначає його дещо відмінно від підходів запропонованих британськими вченими. Він осмислює його як «період невизначеності, який не можна визначити як стан відсутності війни, бо в ньому присутні певні елементи війни. Це мир в умовах постійної небезпеки й перманентної загрози застосування зброї та насилля», а також як «Стан невідчутної війни, коли суспільство психологічно та фізично не відчуває її, а продовжує жити мирним життям, не помічаючи втрат і тяжких наслідків. Або коли одна частина суспільства на території країни перебуває в стані війни (у зоні бойових дій), а інша – у стані миру» (Перепелиця, 2016, с. 765). Цей підхід докорінно відрізняється від вищезгаданих. Він описує процес заморожування конфлікту, що відбувалось в момент написання статті автором, в якому автор вбачає потенційну загрозу – через нестійкість цього стану, і його приреченість на постійну ескалацію. Але маючи в арсеналі такі терміни як заморожений конфлікт або сіра зона, чи можемо ми взагалі говорити про концепцію «гібридного» або будь-якого іншого типу миру в цьому випадку? Чи не є описані стани характеристиками притаманними саме гібридній війні? Де-факто, події що аналізує науковець у своїй роботі, по своїй природі були одним з етапів підготовки Росією

до повномасштабної війни. Або якщо подивитися більш глобально – лакмусовим папірцем для Кремля, що як і в прикладі з агресією проти Грузії, мало на меті випробувати характер та масштаб потенційної реакції міжнародної спільноти на свої віроломні дії. Схожу конотацію цього терміну використовував у своїх медіаматеріалах на тему війни РФ проти України й український журналіст Віталій Портніков (Портніков, 2018).

В той час як підхід Річмонда та Мак Гінті пропонують нам побачити перспективу транзиту від «гібридного миру» до його більш стійких форм через реалізацію комплексу зусиль з використанням ресурсів миротворчості, розбудови миру та розвитку і посилення інститутів демократії. Існування подвійної конотації цього концепту, може ускладнювати дослідження феномену «гібридного миру» в Україні, адже потребуватиме уточнення та обґрунтування вживання саме в такому формулюванні. Потенційно це може викликати негативне ставлення як у представників української наукової спільноти так, і у суспільства в цілому через наявний страх «заморожування» поточних воєнних дій, що ведуться РФ на території України.

Саме тому на сучасному етапі активних бойових дій на лінії фронту ми можемо, і маємо говорити про потребу в більш детальному вивченні цього концепту з потенційним використанням результатів цих розвідок у практичному аспекті – як стратегії виходу України з війни, розбудови майбутнього миру та післявоєнного розвитку держави.

Література

Galtung, J. (1969). Violence, Peace, and Peace Research. *Journal of Peace Research*, 6 (3), 167-191. URL: <https://www.jstor.org/stable/422690?seq=4>

Hoffman, F. G. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: *Potomac Institute for Policy Studies*. URL: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Mac Ginty, R. (2010). Hybrid Peace: The Interaction Between Top-Down and Bottom-Up Peace. *Security Dialogue*, 41 (4), 391-412. URL: <https://www.jstor.org/stable/26301105>

Peace. Oxford English Dictionary. URL: <https://www.oed.com/search/dictionary/?scope=Entries&q=peace>

Richmond, O. P. (2015). The dilemmas of a hybrid peace: Negative or Positive? *Cooperation and Conflict*, 50 (1), 50-68.
URL: <https://www.jstor.org/stable/45084282>

Горбулін, В. (ред.) (2017). *Світова гібридна війна: український фронт*. Київ: НІСД.

Перепелиця, Г. (2016). Концепція «гібридного миру» для України. *Україна дипломатична: науковий щорічник*, 17, 762-772.
URL: https://shron1.chtyvo.org.ua/Perepelytsia_Hryhorii/Kontsepsiia_hibrydnoho_myru_dlia_Ukrainy.pdf

Портніков, В. (2018, січень 13). Україна і «гібридний мир» Путіна як пастка Кремля. *Радіо Свобода*. URL: <https://www.radiosvoboda.org/a/28973563.html>

სალომე გოგიშვილი

*საქართველოს თავდაცვის სამინისტროს მთავარი სპეციალისტი
საქართველოს ტექნიკური უნივერსიტეტის საერთაშორისო
ურთიერთობების მაგისტრანტი
სამეცნიერო ხელმძღვანელი: ასისტენტ პროფესორი დავით
ხუფენია,
საქართველოს ტექნიკური უნივერსიტეტი*

კოოპერატიული უსაფრთხოების თეორიული და პრაქტიკული ასპექტები თანამედროვე საერთაშორისო ურთიერთობებში

შესავალი

ისტორიული პრაქტიკა გვიჩვენებს, რომ უსაფრთხოების ტრადიციული კონცეფციები არ იძლევა შესაძლებლობას მოხდეს შიდასახელმწიფოებრივი კონფლიქტის ეფექტიანი გადაწყვეტა და რეგიონული არასტაბილურობის აღმოფხვრა. საერთაშორისო ურთიერთობების ძირითადი სკოლები – რეალიზმი და ლიბერალიზმი – და მათ შორის დებატები ასახავს ეპოქას, როდესაც ომი ითვლებოდა პოლიტიკის ლეგიტიმურ ინსტრუმენტად. დღეს ბევრ სახელმწიფოს, განსაკუთრებით დასავლეთ ევროპაში, ნაკლებად აწუხებს აგრესიის შეკავებისა და თავდაცვის პრობლემატიკა, ისინი უფრო ორიენტირებულნი არიან რეგიონის საერთო სტაბილურობის შენარჩუნებაზე. ასეთ ქვეყნებს ინტერესი გამომდინარეობს თანამშრომლობის გაღრმავების გზით კონფლიქტების აღბათობის შემცირება და ერთობლივი უსაფრთხოების სისტემის შექმნა. ამ ინტერესს სამეცნიერო წრეებში და პოლიტიკოსებშიც ხშირად უწოდებენ „გაერთიანებულ (კოოპერატიულ) უსაფრთხოებას“.

სამწუხაროდ, ბევრი სახელმწიფო მხოლოდ აცხადებს, რომ ჩაერთვება კოოპერატიულ უსაფრთხოების სისტემაში, სინამდვილეში კი, ისინი მიისწრაფვიან მარტივი თანამშრომლობისკენ. მათი რიტორიკაც კარგად ასახავს მათ მიერ

უსაფრთხოების აღქმას: თანამშრომლობა ძირითადი სფეროებში დაცვისა და სტაბილურობის ხელშეწყობისთვის.

ისტორიულად, სახელმწიფოთა მრავალი ჯგუფი ცდილობდა რეგიონული სტაბილურობის ხელშეწყობას. ზუსტად ეს გამოცდილება განსაზღვრავს ამჟამინდელი უსაფრთხოების სისტემის შემქნის მცდელობებს.

დღევანდელი მოცემულობით, სახელმწიფოთა სამი გაერთიანება თავს მიიჩნევს კოოპერატიულ უსაფრთხოებაში ჩართულებად - ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაცია (ნატო), ევროპის უსაფრთხოებისა და თანამშრომლობის ორგანიზაცია (ეუთო) და სამხრეთ-აღმოსავლეთ აზიის ქვეყნების ასოციაცია (ASEAN).

ჩვენი თეზისები წარმოაჩენს კოოპერატიულ უსაფრთხოების ჩამოყალიბებისა და ფუნქციონირების პრობლემატიკას, და თეორიულ ნაწილში, დიდწილად, ეყრდნობა უსაფრთხოების დილემის თეორიას.

ცნება „უსაფრთხოების“ განსაზღვრა

ცივი ომის შემდეგ, დასავლეთეუროპული საზოგადოებები სახელმწიფოს გადარჩენის საზრუნავიდან "მყარი უსაფრთხოების", ეკონომიკური კეთილდღეობის და "რბილი უსაფრთხოების" ინტერესზე გადავიდნენ.

ცივი ომის დასრულების შემდეგ, ტერმინი უსაფრთხოების იმდენი განმარტება გაჩნდა, რომ ზოგიერთმა მეცნიერმა მას უწოდა "არსებითად სადავო კონცეფცია". ჩვენი აზრით, დაბნეულობა უფრო მდგომარეობს იმ ღირებულებებსა და სოციალურ ინსტიტუტებში, რომლებსაც დაცვა სჭირდებათ, ვიდრე თავად კონცეფციასში. ამრიგად, უსაფრთხოება შეიძლება განისაზღვროს, როგორც გარკვეული ღირებულებების დაცვა, ან, როგორც არნოლდ ვოლფერსმა თქვა: უსაფრთხოება შეიძლება შეფასდეს, როგორც „შემენილი ღირებულებებისთვის საფრთხის არარსებობა“. კონცეპტუალური პრობლემა შემდეგ ხდება იმის განმსაზღვრელი, თუ რომელი სოციალური ერთეულები (მაგ., ინდივიდები, სახელმწიფოები, საერთაშორისო ინსტიტუტები და სახელმწიფო სისტემები) და ღირებულებები (მაგ. ფიზიკური უსაფრთხოება, პოლიტიკური სუვერენიტეტი და ეკონომიკური კეთილდღეობა)

გამოიყენება. ამ კითხვებზე პასუხები, როგორც წესი, განსხვავდება იმის მიხედვით, თუ როდის დაისმება კითხვა და რომელი მიდგომაა მიღებული საერთაშორისო ურთიერთობების ინტერპრეტაციისთვის. ამგვარად, ცივი ომის შემდეგ, დასავლეთეუროპული სახელმწიფოს გადარჩენის იტერესიდან გადაიზარდნენ ეკონომიკური კეთილდღეობის ინტერესზე ("რბილ" უსაფრთხოებაზე). ეს ცვლილება ასახავს საბჭოთა კავშირისა და მისი მემკვიდრე სახელმწიფოს, რუსეთის მიერ წარმოქმნილი საფრთხის რეალურ შემცირებას.

ამრიგად, კვლევაში კოოპერატიული უსაფრთხოებას განვმარტავთ შემდეგნაირად:

კოოპერატიული უსაფრთხოება არის აქტივობა სახელმწიფოებს შორის ომის ალბათობის შესამცირებლად, ან მისი შედეგების შესამცირებლად, რომელიც არ არის მიმართული რომელიმე კონკრეტულ სახელმწიფოზე ან სახელმწიფოთა ჯგუფზე.

ეს დეფინიცია განასხვავებს საერთაშორისო ურთიერთობების აქტივობის ორ ძალიან განსხვავებულ სფეროს: 1) აქტი, რომელიც მიმართულია კონკრეტულ სახელმწიფოებზე, ან სახელმწიფოთა ჯგუფებზე, რომლებიც აღიქმება საფრთხეებად; 2) აქტი, რომელიც მიმართულია იმ გარემოს გასაუმჯობესებლად, რომელშიც სახელმწიფოები მოქმედებენ. კოოპერატიული უსაფრთხოება ცდილობს გაუმკლავდეს მეორე პრობლემატიკას: გააუმჯობესოს უსაფრთხოების გარემო.

კოოპერატიული უსაფრთხოება შეიძლება შეიქმნას ორ ან მეტ სახელმწიფოს შორის. უმარტივესი და ტრადიციულად ყველაზე გავრცელებული ინტერპრეტაცია ეკუთვნის საერთაშორისო ურთიერთობების ნეორეალისტურ თეორიას, რომელიც აყალიბებს რამდენიმე ძირითად თეზისს: სახელმწიფო არის ანალიზის ერთეული; იგი ცდილობს გააუმჯობესოს თავისი უსაფრთხოება, ხშირად სხვების ხარჯზე; საერთაშორისო ანარქიული სისტემის პირობებში თანამშრომლობა გართულებულია.

კოოპერატიული უსაფრთხოების შეთანხმებები არაერთხელ განვითარდა ბოლო ორასი წლის განმავლობაში, როდესაც სახელმწიფოები დარწმუნდნენ, რომ მათ სჭირდებათ უსაფრთხოების გარემო პირობების გაუმჯობესება. ეს მცდელობები

მერყეობს ევროპის შეთანხმებიდან – რომელიც შეიქმნა ნაპოლეონის ომების დასრულების შემდეგ – ევროპის უსაფრთხოებისა და თანამშრომლობის ორგანიზაციამდე.

ევროპის შეთანხმება – ადრეული კოოპერატიული უსაფრთხოება, ფაქტობრივად, პირველი რეალური ძალისხმევაა კოოპერატიული უსაფრთხოებისთვის; ერთა ლიგა – კოლექტიური უსაფრთხოების მიღწევის წარუმატებლობა; გაერთიანებული ერების ორგანიზაცია – კოლექტიური უსაფრთხოება და კოოპერატიული უსაფრთხოება; დასავლეთ ევროპა – პროტოტიპული უსაფრთხოების საზოგადოება; ნატო – კოლექტიური თავდაცვიდან კოოპერატიულ უსაფრთხოებამდე; ეუთო – ადგილი კოოპერატიული უსაფრთხოებისთვის? სამხრეთ-აღმოსავლეთ აზიის ქვეყნების ასოციაცია (ASEAN) – შეზღუდული კოოპერატიული უსაფრთხოება დემოკრატიის გარეშე.

კოოპერატიული უსაფრთხოების მომავალი

კოოპერატიული უსაფრთხოების წარმატება რამდენიმე ფაქტორზეა დამოკიდებული. უპირველეს ყოვლისა, ის მოითხოვს რწმენას, რომ გარკვეულ ქვეყნებს აქვთ საერთო მომავალი და რომ თანამშრომლობა სთავაზობს საუკეთესო შესაძლებლობებს მათი ეროვნული ინტერესების მისაღწევად. ისტორიულად, საერთო საფრთხის აღქმა იყო უსაფრთხოების სისტემის ჩამოყალიბების ყველაზე ხშირი და ყველაზე ეფექტური საფუძველი. ეს ნამდვილად იყო ევროპის შეთანხმების, ნატოს, ევროკავშირის და ASEAN-ის შემთხვევაში.

იმის გამო, რომ ეროვნული ელიტები მზად იყვნენ ერთად ემუშავათ საერთო საფრთხის წინაშე, მათ ჩამოაყალიბეს საერთო იდენტობა, რომელიც სცდებოდა ეროვნულ საზღვრებს და ამლიერებდა მათ საერთო მიზნის გრძნობას. ჩამოყალიბების შემდეგ, ეს ახალი იდენტობა შეიძლება საკმაოდ მდგრადი იყოს, რაც საშუალებას მისცემს უსაფრთხოების მექანიზმებს გადალახონ საფრთხეები, რომლებმაც ისინი პირველად შეაერთეს.

დღეს ევროპისთვის საფრთხეები სულ უფრო მეტად ტრანსნაციონალური ფენომენია. მათ შორისაა კორუფცია, ორგანიზებული დანაშაული, მიგრაცია, ეპიდემიური დაავადებები, ეკოლოგიური კატასტროფები და ტერორიზმი. ასეთი რთული

პრობლემების დაძლევა შესაძლებელია მხოლოდ ეროვნული საზღვრების მიღმა ერთიანი მოქმედებით. რამდენადაც საფრთხის ქვეშ მყოფი სახელმწიფოები ერთად მუშაობენ, ისინი იღებენ კრიტიკულ ცნობიერებას მათი საერთო მომავლის შესახებ და ჩვენ შეგვიძლია ველოდოთ, რომ კოოპერატიული უსაფრთხოება ნორმად იქცევა.

ამავდროულად, უსაფრთხოების მრავალმხრივი მიდგომების აუცილებლობა ეფუძნება კოოპერატიულ უსაფრთხოებას. ეს განსაკუთრებით ეხება მცირე ქვეყნებს, რომლებსაც სჭირდებათ რესურსების გაერთიანება. ბალტიისპირეთის ქვეყნები კარგ მაგალითს იძლევა და სამხრეთ-აღმოსავლეთ ევროპაში ბოლოდროინდელი მცდელობები იმედისმომცემია. კონსენსუსური გადაწყვეტილების პრაქტიკა ხშირად ეხმარება ამ მრავალმხრივ უსაფრთხოების მიდგომას საერთო იდენტობის ჩამოყალიბებაში და, შესაბამისად, იგრძნობა კოოპერატიული უსაფრთხოების საჭიროება.

კოოპერატიული უსაფრთხოება სულ უფრო მეტად გამოიყენება, როგორც ეროვნული უსაფრთხოების გაძლიერების მექანიზმი. ქვეყნები ინდივიდუალურად იქცევიან რაციონალურად, მაგრამ ამით იმოქმედებენ საკუთარი გრძელვადიანი ინტერესების საწინააღმდეგოდ. თვითდახმარებაზე და ძველი სტილის დაბალანსების ქცევაზე დაყრდნობამ ადგილი დაუთმო სტაბილურობის ხელშეწყობის ერთობლივ ძალისხმევას. იმ სახელმწიფოებს შორისაც კი, რომლებსაც არ გააჩნიათ საერთო ღირებულებები, შესაძლებელია თანამშრომლობის უსაფრთხოება. ASEAN მნიშვნელოვანი პრაქტიკული მაგალითია ამ მხრივ. კოოპერატიულ უსაფრთხოებასთან მიახლოება ხდება თითოეულ შემთხვევაში, მაგრამ მეორე მსოფლიო ომის დასრულების შემდეგ შეიქმნა უსაფრთხოების რამდენიმე საზოგადოება – განსაკუთრებით დასავლეთ ევროპაში.

მას შემდეგ, რაც ცალმხრივად გამოყენებული სამხედრო ძალა დიდწილად დისკრედიტირებული გახდა, როგორც პოლიტიკის ინსტრუმენტი, ქვეყნები გაერთიანდებიან, რათა გამოიყენონ ძალა კოლექტიურად მათი უშუალო სამეზობლოში უსაფრთხოების გასაძლიერებლად. უფრო მეტიც, ისინი გადადგამენ სხვა ნაბიჯებს, ეკონომიკურ და სხვა სახის, უსაფრთხოების გარემოს

გასაუმჯობესებლად, რათა შემცირდეს ახალი საფრთხეების წარმოშობის ალბათობა. უსაფრთხოების ძველი ტრადიციული კონცეფციები არაადეკვატური აღმოჩნდა ამ საკითხების მოსაგვარებლად. თანამედროვე უსაფრთხოების გამოწვევების ბუნება იწვევს კოოპერატიული უსაფრთხოების მზარდ გამოყენებას.

გამოყენებული ლიტერატურა

Mihalka, M. (2001). Cooperative Security: From Theory to Practice. Marshall George C. *European Center for Security Studies*, 003.

Baldwin, D. (1997). The Concept of Security. *Review of International Studies*, 23, 1, 3-26.

Wolfers, A. (1952). 'National Security' as an Ambiguous Symbol. *Political Science Quarterly*, 67, 4, 485.

Glaser, C. (1977). The Security Dilemma Revisited. *World Politics*, 50, 1, 171-201.

As cited in Andrew Butfoy, *Common Security and Strategic Reform: A Critical Analysis* (1997). New York: St. Martin's Press.

Axelrod, R. (1984). *The Evolution of Cooperation*. New York: Basic Books.

Deutsch, K. (1957). *Political Community and the North Atlantic Area*. Princeton: Princeton University Press.

The French first used gas in grenades in 1914. The Germans followed by carrying out the first large-scale chemical attack on April 22, 1915 at Ypres, Belgium. Chlorine gas was released from gas cylinders along six kilometers of the front line. The Germans claimed that they did not violate the 1899 agreement because they did not use projectiles.

Carter, Ashton B., Perry, William J., Steinbrunner, John D. (1993) *A New Concept of Cooperative Security*. Washington, DC: The Brookings Institution Press.

Holbrad, C. (1970). *The Concert of Europe: A Study in German and British International Theory*. New York: Longman, 127.

Quoted in Ole Waever (1998). Insecurity, Security and Asecurity in the West European Non-War Community. Adler, E., Barnett, M. eds. *Security Communities*. Cambridge: Cambridge University Press, 83.

Statement by Harold Macmillan, British MP. URL: <http://www.liv-coll.ac.uk/europetrip/Europe%20journey/schuman.htm>; accessed December 2000.

The Schuman Declaration, May 9, 1950. URL: <http://www.let.leidenuniv.nl/history/rtg/res1/declaration.html>.

Prime Minister of the Republic of Poland Jerzy Buzek, "Priorities of the Polish Foreign Policy," speech at the Paaskivi Society, Helsinki, November 4, 1999. URL:<http://polcon.tripod.com/buzek.html>.

Rotterdam Algemeen Dagblad, June 26, 1997. Translation by Foreign Broadcasting Information Service, FBIS-WEU-97-177.

Irish Department of Foreign Affairs Press Release, October 13, 1999. URL: <http://www.irelandemb.org/press/46.html>.

NATO Secretary General Javier Solana, "NATO's Role in Building Cooperative Security in Europe and Beyond," speech at the Yomiuri Symposium on International Economy, Tokyo, Japan, October 15, 1997.

Sestak, J. (1997). State Secretary at the Slovak Ministry of Foreign Affairs. Harbingers of Gloom Will Not Help: interview by Leopold Moravcik. *Bratislava Pravda*.

Organization for Security and Co-operation in Europe (OSCE) Handbook (2000). Prague: 17-18. URL: <http://www.osce.org/publications/handbook/index.htm>.

Acharya, A. (1998). Collective Identity and Conflict Management in Southeast Asia. Adler, E., Barnett, M. eds. *Security Communities*. Cambridge: Cambridge University Press, 203.

ASEAN Free Trade Area (AFTA): An Update, November 1999. URL: <http://www.asean.or.id/general/publication/afta-upd.htm>.

ASEAN Web Site. URL: <http://www.asean.or.id/>.

Іваницька Ольга Павлівна

*доктор історичних наук, професор,
Донецький національний університет імені Василя Стуса,
м. Вінниця, Україна*

ORCID: 0000-0002-5512-1542

Чальцева Олена Михайлівна

*доктор політичних наук, професор,
Донецький національний університет імені Василя Стуса,
м. Вінниця, Україна*

ORCID: 0000-0003-3922-7619

ОСОБЛИВОСТІ БЕЗПЕКОВОЇ ПОЛІТИКИ ІСПАНІЇ У ХХ – ХХІ СТОРІЧЧЯХ

У Королівстві Іспанія розпочався зі смертю Ф. Франко у 1975 році новий історичний етап: етап мирного демонтажу авторитарного режиму та унікального демократичного транзиту до повноцінної демократичної системи. На цьому шляху Іспанії належало розв'язати одне з найсуттєвіших державних завдань – підготувати й реалізувати нову зовнішньополітичну стратегію, головна мета якої полягала у набутті нею суб'єктності у міжнародних відносинах, у повноцінній інтеграції в європейські й світові структури та процеси, і, найголовніше, гарантуванні таким чином власної національної економічної та військово-політичної безпеки (Marin Jose Maria, Molinero Carme, Ysas Pere, 2001, P. 247 – 321; Arostegui Julio, Bahamonde Angel, Molinero Carme, Otero Luis Enrique, Ysas Pere, 2003, P. 245 – 306).

Іспанська історіографія виділяє загалом дві моделі безпекової зовнішньої політики, які сповідували й практикували постфранкістські уряди, і які різняться одна від одної базовими принципами й пріоритетами. Перша модель, в основу якої було покладено атлантизм та унілатералізм, тобто пріоритетну співпрацю з США та НАТО, реалізовували уряди Союзу демократичного центру (СДЦ) на чолі з Адольфо Суаресом й Леопольдо Кальво Сотело та Народної партій (НП) з Хосе Марією

Альфредо Аснаром Лопесом, продовжуючи фактично безпекову політику франкізму. Іншу зовнішньополітичну модель, яка отримала назву європейської з акцентом на першочергову співпрацю з європейськими структурами та європейськими країнами, та мультилатералізмом, впроваджували уряди соціалістів (Іспанська соціалістична робітничка партія – ІСРП), очолювані Феліпе Гонсалесом Маркесом та Хосе Луїсом Родрігесом Сапате́ро (*Politica exterior de España y Relaciones con America Latina*, 2011, P. 112 – 118; Garcia-Calvo Carola, 2010, P. 53 – 59).

Геостратегічні, безпекові та оборонні інтереси таласократичної Іспанії у другій половині ХХ століття через її унікальне географічне периферійне розташування зосереджувались на південному фланзі континентальної Європи, тобто на півдні Іберійського півострова, у Середземномор'ї та Магрибі, в ареалі яких розташовувалась низка проблемних у безпековому вимірі для Мадрида точок: півострів Гібралтар, контрольований з 1713 року Великобританією, Гібралтарська протока, яка з'єднує Атлантику з Середземним морем, іспанські анклави і міста-порти Сеута і Мелілья на території Марокко, який вимагає їх повернення і збереження таким чином територіальної цілісності і суверенітету марокканської держави, Західна Сахара, Канарські острови у контексті претензій на них Алжиру, конфліктний Магриб як зона іспанського національного інтересу і безпекового контролю за цим регіоном. Середземноморський простір, до якого належить південне і південно-східне узбережжя Іспанії, через своє вигідне економічне і геополітичне розташування є воротами до Атлантичного океану і перехрестям, контактною й конфліктною зоною низки європейських, африканських і азійських держав. Водночас він виконує роль своєрідного мосту між Сходом і Заходом, а Іспанія є головною з'єднувальною ланкою між Європою та Північною Африкою.

Нагадаємо, що франкістська Іспанія, опинившись по завершенні Другої світової війни у міжнародній ізоляції і не будучи членом ООН та інших світових та європейських організацій і союзів, шукала безпекових гарантій у двосторонніх стосунках з країнами, які її визнавали. Вирішальну роль у прориві її міжнародної ізоляції зіграло іспано-американське зближення,

що почалося 1947 року. 1953 року Іспанія отримала статус стратегічного союзника США і була підключена, не будучи членом НАТО, до північноатлантичної безпекової та оборонної структури. У цьому ж році, 26 вересня, було підписано іспано-американську широкомасштабну «Угоду про оборону», відому також як Мадридський пакт». США у відповідності з угодою орендували в Іспанії три військово-повітряні бази (Торрехон, Сарагоса, Маррон) і військово-морську базу Рота. При сприянні США були значно модернізовані іспанські підприємства з виробництва озброєнь і військової техніки (Sabin Rodriguez, 1997, P. 210-214; Bennassar, 1996, P. 175; Fusi, 2001, P. 118).

Іспано-американська військово-оборонна і безпекова співпраця розширювалась у 1963 році було підписано нову угоду, за якою була створена нова безпекова структура – американо-іспанський консультативний комітет з питань оборони. У «Спільній декларації», оприлюдненій з нагоди підписання угоди 1963 року, йшлося, що вона є «частиною угоди щодо забезпечення безпеки атлантичної й середземноморської зон». Нарешті, у серпні 1970 року підписано Договір про дружбу і співпрацю між Іспанією та США, який розглядався як якісно новий етап у розвитку партнерських відносин між двома країнами у безпековій сфері (Marin Jose Maria, Molinero Carme, Ysas Pere, 2001, P. 181-182).

Варто зауважити, що, незважаючи на майже 40-річне існування в Іспанії авторитарного франкістського режиму, у зовнішній політиці, зокрема, у безпековій царині, не відбулося з початком демократичного транзиту кардинальних змін у визначенні національних безпекових пріоритетів, зберігалася спадковість з минулим.

У зовнішньополітичному концептуальному плані демократичні уряди А.Суареса та Л.Кальво Сотело виходили із того, що Іспанія офіційно розглядалася як «середня за значущістю держава», здатна відігравати суттєву роль у європейській безпековій політиці. На цьому фоні майбутнє Іспанії у безпековому сенсі трактувалось у нерозривному зв'язку з європейськими державами. Так само у контексті приналежності Іспанії до західної цивілізації все більш наполегливими ставали

заяви щодо її вступу до НАТО, який давав країні такі переваги: прискорення процесу преговорів про членство в ЄС, розв'язання проблеми Гібралтару, модернізацію збройних сил у царині забезпечення національної оборони, захисту від можливих конфліктів (Федорова, 2014, С.35-37).

Незважаючи на внутрішньополітичні дискусії та міжпартійні суперечки, уряд Л.Кальво Сотело 30 травня 1981 року вручив у Вашингтоні офіційний документ про приєднання Іспанії до НАТО. 10 грудня 1981 року міністри НАТО схвалили вступ Іспанії до альянсу. Після схвалення парламентами 15 країн-членів НАТО Іспанія стала з 1982 року 16-им членом цієї військово-політичної організації.

Отримавши перемогу на парламентських виборах 1982 року, ІСРП провела 12 березня 1986 року вперше в історії Альянсу загальнонаціональний референдум щодо «особливого статусу» Іспанії в НАТО, на який було винесено наступні питання: відмова від вступу в інтегровану військову структуру НАТО; не входження іспанських збройних сил в єдину систему військового командування; заборона розміщення, складування чи ввозу ядерної зброї на іспанську територію; поступове скорочення військової присутності США в Іспанії. Іспанці підтвердили «особливий статус» Іспанії в альянсі (52,5 відсотка іспанців висловилися за НАТО, 39,8 відсотка – проти). Це дозволило Мадриду брати активну участь у діяльності керівних органів альянсу і при цьому зберігати свободу дій при прийнятті рішень, які стосувалися забезпечення національної і міжнародної безпеки. У лютому 1988 році було завершено процес затвердження низки документів, які визначали місце і рівень участі Іспанії в НАТО. Іспанія ввійшла в Комітет планування НАТО, стала членом Групи ядерного планування, прийняла участь в організації ППО НАТО, а також у формуванні військово-морських сил НАТО у Східній Атлантиці, взяла на себе зобов'язання щодо матеріально-технічного постачання військових підрозділів НАТО та захисту Гібралтарської протоки (Marin Jose Maria, Molinero Carme, Ysas Pere, 2001, P. 373-374, 385-388).

Гнучкий підхід до теми «європеїзм – атлантизм» став одним з фундаментальних елементів зовнішньої політики Іспанії

на новому етапі розвитку міжнародних відносин, тобто на початку 1990-х років. Звідси розпочалася трансформація концепції національної оборони у новій Директиві національної оборони 1992 року, в якій вказувалася, що різні кризи за межами Європи показали, що безпека Іспанії залежить не тільки від безпеки її територій, але і від того, що відбувається в інших частинах світу. Безпека повинна розумітися на колективному рівні; у такому взаємозалежному світі жодна країна не в змозі наодинці протистояти новим ризикам Ці слова стали одним із гасел зовнішньої політики Іспанії у 1990-х роках, зокрема, народнофронтівського уряду Х. М. Аснара. Його реалізація сталася у реформуванні «іспанської моделі» членства в НАТО, тобто приєднання країни до військових структур Альянсу. Офіційний Мадрид претендував на керівництво натовським командуванням, яке б включало ареал Гібралтарської протоки і всієї території країни, на отримання важливих посад в інших командуваннях Альянсу в Європі і Атлантичному регіоні, підтверджував у майбутньому свій без'ядерний статус. У грудні 1997 року міністри оборони країн НАТО затвердили нову структуру командувань Альянсу: спеціально для Іспанії створювалось на її території нове південно-західне комбіноване субрегіональне командування, у зону якого попадала вся територія країни (материкова Іспанія, Канарські і Балеарські острови, а також зона Гібралтарської протоки), за виключенням Сеути і Мелільї, які знаходилися поза сферою відповідальності НАТО. Іспанський штаб дислокувався у передмісті Мадрида. 30 вересня 1999 року у містечку Ратамарес (неподалік Мадрида) відбулося відкриття Об'єднаного штабу південно-західного регіонального командування НАТО, який очолив іспанський генерал-лейтенант Х.Нарро (Іваницька О.П. Зовнішня політика країн Західної Європи та Північної Америки у постбіполярний період (1990-і - 2000-і роки), 2012, С.400-402).

Отже, Іспанія не ставить під сумнів необхідність збереження НАТО як фактору стабільності, як і необхідність присутності американських збройних сил в Європі як найважливішої умови збереження безпеки на європейському континенті. Членство в НАТО посприяло модернізації іспанських збройних сил

за сучасними натовськими стандартами. Нині Іспанія прагне трансформації НАТО у дієвий інструмент попередження регіональних конфліктів. Це завдання особливо гостро постало і перед Україною на її шляху до членства у цьому військово-політичному оборонному й безпековому блоці.

Література

Marin Jose Maria, Molinero Carme, Ysas Pere (2001). *Historia politica de España. 1939 –2000*. Madrid: Edicion Istmo, S. A.

Arostegui, J., Bahamonde, A., Molinero, C., Otero, L. E., Ysas, P. (2003). *Historia de España siglo XX. 1939 – 1996*. Madrid: Catedra.

Politica exterior de España y Relaciones con America Latina. Iberoamericanidad, Europeizacion y Atlantismo en la politica exterior española (2011). Madrid: Fundacion Carolina.

Garcia-Calvo, C. El Papel de las Ideas, Valores y Creencias del Lider en la Definicion y Acciones de politica exterior: España 2000 – 2008 (2010). *Relaciones Internacionales*, 13, 35 – 63.

Sabin Rodriguez Jose Manuel. La Dictadura franquista (1936-1975) (1997). *Textos y documentos*. Madrid: AKAL.

Bennassar Bartolome. Franco (1996). Madrid: EDAF.

Fusi, J. P. (2001). *Franco. Spanien unter der Diktatur. 1936–1975*. Madrid: Ediciones RIAZP.

Федорова, К. О. (2014). *Зовнішня політика Іспанії на початку XXI століття*. Warszawa: Diamond trading tour.

Іваницька, О. П. (2012). *Зовнішня політика країн Західної Європи та Північної Америки у постбіполярний період (1990-ті – 2000-ті роки)*. Київ: Видавничий Дім «Слово».

Міщенко Ілона Володимирівна
кандидат юридичних наук, доцент,
Національний університет «Одеська юридична академія»,
м. Одеса, Україна
ORCID: 0000-0002-5373-5057

ДО ПИТАННЯ ВІДПОВІДАЛЬНОСТІ ЗА МІЖНАРОДНИМИ ДОГОВОРАМИ ПРО ВЗАЄМНИЙ ЗАХИСТ СЕКРЕТНОЇ ІНФОРМАЦІЇ (НА ПРИКЛАДІ УГОДИ З США)

На сучасному етапі питання національної безпеки стоять особливо гостро. Ця багатогранна та складна категорія вимагає ґрунтовного аналізу та дослідження в контексті нових загроз, пов'язаних зі збройною агресією російської федерації проти України. З одного боку, міжнародна спільнота, окремі країни та союзи надають Україні суттєву допомогу та підтримку. З іншого боку, така тісна взаємодія накладає на нашу державу певні зобов'язання, вимагає відповідності очікуванням. Обов'язковий зворотній зв'язок, прозорість у використанні міжнародної допомоги та звітності, відповідний рівень комунікації – це той мінімум, що на даному етапі вимагається від нашої держави донорами допомоги. На перший погляд, такі вимоги є цілком виправданими та такими, що не несуть жодних загроз національній безпеці в цілому на та її окремим напрямам. Разом із тим, один зі складних моментів у цьому зв'язку – міжнародний контекст забезпечення національної безпеки певної країни, оскільки він знаходиться на перетині національних інтересів двох або більше країн. Історія знає приклади, коли країни, обґрунтовуючи свої дії необхідністю захисту своєї національної безпеки, відверто завдавали шкоди або загрожували безпеці інших держав.

Як вже було зазначено, іноземні країни – партнери, донори військової допомоги вимагають від України певних заходів у відповідь. Серед таких заходів надання різного роду інформації,

яка, окрім того, що є чутливою для нашої держави та суспільства, охороняється законом. Мова передусім йде про передачу інформації, що становить державну таємницю (секретної інформації). Загально відомо, що державна таємниця – найбільш охоронюваний вид інформації з обмеженим доступом, за неправомірне поводження з якою передбачена кримінальна відповідальність.

Відповідно до статті 32 Закону України «Про державну таємницю» секретна інформація до скасування рішення про віднесення її до державної таємниці та матеріальні носії такої інформації до їх розсекречування можуть бути передані іноземній державі чи міжнародній організації лише на підставі міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, або письмового мотивованого розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України на підставі пропозицій Ради національної безпеки і оборони України (Закон про державну таємницю, 1994). На офіційному сайті Служби безпеки України перелічено близько 50 міжнародних договорів про взаємний захист секретної інформації. Серед країн, з якими такі угоди укладено, до сих пір значиться Білорусь, Вірменія та інші члени Організації договору про колективну безпеку (ОДКБ), тобто союзників країни-агресора. Примітно, що подібний договір з російською федерацією було денонсовано ще у 2015 році (Закон про денонсацію, 2015).

Проаналізуємо угоду з одним з найбільших (якщо не найбільшого) донора військової допомоги – США. Ця угода стосується конкретної сфери обігу секретної інформації – сфери оборони. Сторонами Угоди між Урядом України та Урядом Сполучених Штатів Америки про охорону секретної інформації у сфері оборони є уряди цих країн. Охорона секретної інформації стороною-одержувачкою відбувається на підставі зазначеної угоди, а так само внутрішнього законодавства цієї країни. Якщо угоду можна змінити чи доповнити за домовленістю сторін, внутрішнє законодавство кожної з країн-підписантів залишається незмінним або змінюється лише за ініціативою та бажанням власної держави. Один з ключових меседжів угоди – сторона-

одержувач секретної інформації забезпечуватиме рівень охорони отриманої інформації, еквівалентний відповідному рівню охорони Сторони-джерела цієї інформації (Угода, 2003). Будь-які дії, передачі такої інформації здійснюються лише з письмового дозволу останньої. Логічно постає питання: які наслідки будуть наставати, якщо сторона не виконуватиме ці вимоги?

У цьому контексті особливої уваги заслуговують дві статті угоди, які стосуються відповідальності. Стаття 10 встановлює таке: «Кожна Сторона нестиме відповідальність за збереження всієї секретної інформації у сфері оборони іншої Сторони з моменту її офіційного одержання, під час її перевезення, передачі або зберігання на території своєї держави». У свою чергу стаття 11 містить наступне положення: «Кожна Сторона несе відповідальність за забезпечення режиму секретності на всіх державних та приватних об'єктах та установах, де знаходиться інформація іншої Сторони, і забезпечуватиме призначення на кожному такому об'єкті та в установі кваліфікованих спеціалістів з обов'язками та повноваженнями щодо контролю та охорони такої інформації» (Угода, 2003).

Варто нагадати, що стороною в угоді є уряд відповідної країни. Тож виникає логічне запитання, яким чином уряди країн-підписантів нестимуть відповідальність за порушення режиму секретності або втрату, модифікацію тощо секретної інформації? Що це буде за відповідальність? У зв'язку з тим, що угодою ці положення не деталізовані, можна уявити, що відповідальність має наставати відповідно до норм національного законодавства країни-отримувача інформації. За законодавством України, приміром, неможливо притягнути уряд (Кабінет Міністрів України) до, наприклад, кримінальної відповідальності, адже за неправомірні дії з секретною інформацією передбачена саме вона. Кримінальна відповідальність персоніфікована, а уряд є колективним органом (юридичною особою). Кабінет Міністрів України може нести хіба що політичну відповідальність у вигляді відставки. Однак навряд чи про таку відповідальність йдеться в аналізованій угоді.

Вочевидь відповідальність сторін угоди є формальною, втілити її у життя не уявляється можливим через брак

національних правових механізмів. За законодавством України відповідати за кримінальні правопорушення у сфері обігу секретної інформації може лише конкретна особа, якій секретні відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків. (Кримінальний кодекс України, 2001). Розділ 18 Кодексу США § 798 також встановлює відповідальність особи за несанкціоноване розкриття секретної інформації. (U.S.C., 2011). Отже зазначені статті угоди потребують перегляду в контексті приведення її змісту до загальних принципів притягнення до кримінальної відповідальності обох країн. Не дивлячись на примат міжнародного права, реалізувати на практиці зазначені положення у тому вигляді, в якому вони закріплені в угоді неможливо. Положення угоди не виключають притягнення до відповідальності конкретних осіб, винних у витоку або іншому порушенні режиму доступу до секретної інформації іншої країни. Разом із тим *pacta sunt servanda*, і для цього підписанти мають робити все можливе, в тому числі вносити зміни в міжнародні договори.

Література

Закон про державну таємницю 1994 (Верховна Рада України). *Офіційний сайт Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>

Закон про денонсацію Угоди між Кабінетом Міністрів України та Урядом Російської Федерації про взаємну охорону секретної інформації 2015 (Верховна Рада України). *Офіційний сайт Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/464-19#Text>

Угода між Урядом України та Урядом Сполучених Штатів Америки про охорону секретної інформації у сфері оборони 2003. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/840_082#Text

Кримінальний кодекс України 2001 (Верховна Рада України). *Офіційний сайт Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/2341-14>

18 U.S.C. 798 (2011) – Disclosure of classified information. URL: https://www.govregs.com/uscode/expand/title18_partI_chapter37_section798#uscode_7

Орленко Володимир Васильович
*Міжрегіональна Академія управління персоналом,
м. Київ, Україна*

ДЕРЖАВНИЙ КОНТРОЛЬ ЯК СКЛАДОВА МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ БЕЗПЕКИ

Сьогодення світу, де виклики та загрози стають все більш глобальними та непередбачуваними, міжнародна співпраця у сфері безпеки стає надзвичайно важливою складовою стабільності та процвітання держав. З ціллю забезпечення ефективного функціонування цього міжнародного механізму, надаючи йому відомчу точність та системність, невід'ємною є роль державного контролю. Державний контроль, що ґрунтується на високих стандартах, прозорості та відповідальності, є не лише гарантом надійності та довіри серед партнерів, а й фундаментом до вирішення спільних завдань у сфері безпеки.

Міжнародне співробітництво у сфері безпеки, а також реалізація євроінтеграційного вектору Україною на сучасному етапі передбачає побудову ефективного державницького апарату, який би відповідав усім наявним нормам ЄС. Задля налагодження сталого функціонування державних органів виникає потреба у побудові ефективної мережі державного контролю, незалежного від інших інстанцій. Державний контроль є важливим аспектом будь-якої демократичної системи для забезпечення державного контролю, в якій державні органи зобов'язані діяти відповідно до закону та в інтересах громадян. В свою чергу, Україна, як незалежна країна, здійснює механізми державного контролю для забезпечення ефективного та відповідального управління. Відповідно, актуальним постає вивчення функціонуючих в Україні механізмів державного контролю та їх майбутніх перспектив.

Відзначимо, що державний контроль є важливою складовою демократичної системи, оскільки він забезпечує баланс та

взаємодію між різними гілками влади, забезпечує відповідність владних дій інтересам громадян та суспільства і сприяє підвищенню довіри до державних органів.

Визначимо, ключові ознаки, які визначають науковці, які характеризують державний контроль:

- організаційний апарат, що об'єднує фахівців, зайнятих контрольною діяльністю, спрямованої на перевірку виконання рішень органів державної влади;
- форму політичної організації;
- контроль, що здійснюється від імені державних органів незалежно від завдань і виду діяльності, яку вони здійснюють;
- державновладну функцію контролю – контрольні органи надають примусові директиви для усунення виявлених недоліків;
- можливість контрольних органів винести питання про відповідальність осіб, винних у виявлених порушеннях, і у відповідних випадках вжити заходи державного примусу (Parfenova, 2014; Горбова, 2019; Терещенко, 2019).

Аналізуючи вищезначені критерії можемо визначити механізми державного контролю, які є необхідні в його життєдіяльності та впливають на сектор безпеки, як систему організаційних, правових і процедурних засобів та методів, що використовуються державою для виконання функцій нагляду, перевірки та регулювання діяльності суб'єктів влади, організацій та інших учасників суспільного життя. Нами визначені наступні ключові механізми державного контролю: регулятивний, правовий, антикорупційний, попереджувально-профілактичний.

Регулятивний механізм є системою організаційних, нормативних та процедурних заходів, спрямованих на створення ефективної системи контролю та забезпечення дотримання встановлених норм, стандартів і правил. Його основні складові взаємодіють для забезпечення якості, відповідності та ефективності діяльності суб'єктів контролю.

Створення та забезпечення діяльності контрольних органів є ключовим елементом регулятивного механізму державного контролю. Держава здійснює цей крок з метою забезпечення ефективного нагляду та перевірки в певних сферах діяльності,

де існують ризики невідповідності законам, стандартам та правилам. Створення спеціальних контрольних органів дозволяє сконцентрувати компетенції та ресурси для забезпечення якості та безпеки відповідно до встановлених норм. Такими органами можуть виступати НАБУ, НАЗК, Антимонопольний комітет, податкові органи, спеціальні комісії тощо. Ці контрольні органи наділяються чіткими функціональними повноваженнями та завданнями, спрямованими на виконання конкретних завдань контролю. Вони мають зобов'язання перевіряти діяльність суб'єктів контролю відповідно до визначених критеріїв та стандартів. Такі органи можуть виявляти порушення, проводити аналіз ризиків та рекомендувати заходи для попередження негативних наслідків.

В контексті євроінтеграційних зусиль державний контроль виступає необхідною умовою для досягнення високих стандартів управління та розвитку суспільства. Спрямованість на наближення до європейських норм і цінностей вимагає реформування і модернізації механізмів контролю, забезпечуючи ефективну діяльність державних структур на користь громадян та загального розвитку країни.

Література

Parfenova, M. J. et al. (2014). Methodology making management decisions based on a modified Ramsey model. *Asian Social Science*, 10, 17, 292-301.

Горбова, Н. А. (2019). Природа державного контролю (нагляду) та генезис його законодавчого визначення. *Право та державне управління*, 1 (34), 1.

Терещенко, М. М. (2019). Державний контроль: сутність, основні підходи та концепції. *Вчені записки ТНУ імені В.І. Вернадського. Серія «Державне управління»*, 30 (69), 4, 117-121.

Рашевська Катерина Євгеніївна

*Навчально-науковий інститут міжнародних відносин,
Київський національний університет імені Тараса Шевченка,
м. Київ, Україна*

ORCID: 0000-0001-9090-1934

РЕ-ГЛОБАЛІЗАЦІЯ ЯК СЕРЕДОВИЩЕ ЗАОХОЧЕННЯ ТА РОЗВИТКУ СИСТЕМИ ПРАВ ЛЮДИНИ

Прагнення міжнародного співтовариства до миру та благополуччя після завершення Другої світової війни відобразилося не лише у створенні системи Організації Об'єднаних Націй (ООН), однак і в пришвидшенні розвитку багатосторонньої торгівлі. У взаємозалежності, недискримінації, прозорості та спрощенні комерційних відносин вбачалося уникнення нових конфліктів та зростання рівня життя у всьому світі. Протягом понад 70 років міжнародна спільнота рухалася в напрямку досягнення цих амбітних цілей, що призводило до поживлення глобалізації. Однак, пандемія, збройні конфлікти в різних регіонах світу, глобальна економічна криза, зростання нерівності та виклики, пов'язані зі зміною клімату, зумовили фрагментацію міжнародних торговельних відносин – поступовий перехід до односторонньої політики.

Найбільш помітною фрагментація є у зв'язку із застосуванням унілатеральних торговельних заходів (імпортних і експортних обмежень) та впровадження нетарифних бар'єрів. Крім того, різко збільшилася кількість імплементованих членами СОТ компенсаційних заходів: у той час, як у 2011 році до них вдалося 9 держав, у 2021 році – вже 41. Подібна політика призвела до зростання протягом 2015-2022 років суперечок усередині Комітету з доступу до ринку в 4 рази. За той же період, кількість торговельних спорів у рамках Ради з торгівлі товарами збільшилася в 9 разів (WTO, 2023).

Крім того, міжнародна торгівля все більше переорієнтовується за рухом геополітичних розломів. З початку повномасштабної агресії РФ проти України на основі індексів

подібності зовнішньої політики остаточно сформувалися “блоки” держав, темпи зростання торгівлі між якими на 4-6% нижчі, ніж всередині них (WTO, 2023). Міжнародні комерційні відносини стали все більш залежними від глобальної політичної ситуації і найбільше дану тенденцію помітно за відмінностями в голосуванні в Генеральній Асамблеї ООН.

Цікаво, що в питаннях, які стосуються збройного конфлікту в Україні, РФ у середньому “підтримують” (або ж шляхом голосування “проти” резолюцій в інтересах жертви агресії, або ж шляхом утримання від голосування) частина африканських, близькосхідних, латиноамериканських та азіатсько-тихоокеанських держав.

Китай, який рідко долучається до резолюцій, пов’язаних з Україною, залишається найбільшим торговельним партнером держави-агресорки зі зростанням торговельного обороту в 2022 році на 29,3% до рекордних \$190,27 млрд. (Павленко, 2023). Це означає, що РФ та Китай перебувають в одному “блоці”, а Україна та її сателіти – в іншому, відтак, досягнути змін у голосуванні всередині ООН, в тому числі за резолюції у гуманітарній сфері та у сфері захисту прав людини, можна виключно тоді, коли на додаток до геополітичних переваг державам, здебільшого, т.зв. Глобального півдня, будуть запропоновані нові поступки в торговельній сфері. Ними можуть бути більш сприятливі умови в зовнішньоторговельних угодах, притік інвестицій, дешеві кредити, програми технічної допомоги та допомоги з розвитку.

Фрагментація міжнародної торгівлі призводить до збільшення вартості товарів та послуг. Вона негативно впливає на глобальну безпекову ситуацію та нівелює досягнення у сфері зростання та розвитку в окремих державах і цілих регіонах. Це, у свою чергу, призводить до погіршення рівня життя та зuboжіння населення, зменшення видатків на соціальну та медичну сфери, сприяє радикалізації суспільств. Поглиблення фрагментації міжнародної торгівлі в довгостроковій перспективі значно ускладнить міжнародне співробітництво і в інших сферах, зокрема, щодо досягнення цілей сталого розвитку та вирішення глобальних проблем.

На думку експертів Світової організації торгівлі (СОТ), негативних наслідків сучасних тенденцій у сфері міжнародної торгівлі можна уникнути за допомогою ре-глобалізації. Остання є процесом інтеграції людей, економік та спільних для них викликів у міжнародну торгівлю шляхом поглиблення багатостороннього співробітництва. Ре-глобалізація здатна зробити міжнародну торговельну систему більш безпечною, інклюзивною та прозорою, що, у свою чергу, є сприятливим середовищем для заохочення та захисту прав людини.

Лише на рівні прозорої та справедливої міжнародної торговельної співпраці можна реалізувати рекомендації, сформовані Комітетом ООН з прав людини, зокрема, щодо:

- всеосяжної підтримки країн, що розвиваються, з боку розвинутих держав;
- впровадження договірної механізми щодо відповідальності приватних суб'єктів, зокрема транснаціональних корпорацій, за їхню діяльність, яка може не відповідати міжнародним стандартам у сфері захисту прав людини;
- розробки та перевірки інвестиційних правил через діалог з прав людини (UNHRC, 1980).

Крім того, диверсифікація міжнародних ринків та збільшення кількості глобальних торговельних ланцюгів сприяють зростанню стійкості держав до непередбачуваного дефіциту, як, наприклад, під час пандемії COVID-19 або у зв'язку із блокуванням РФ поставок продовольства, зокрема, зернових з України після початку повномасштабного вторгнення. Багатостороння торговельна система, яка зводить до мінімуму невинуваті тарифні і нетарифні бар'єри, також забезпечує мирне вирішення спорів, що сприяє міжнародному миру та безпеці в цілому. Так, збільшення на 50% торгівлі між двома державами зменшує ймовірність настання конфлікту між ними в середньому на 20% (Polachek, 1980).

Ре-глобалізація пропонує всім членам міжнародного співтовариства участь в управлінні міжнародними торговельними відносинами, взаємне стримування на міжнародній арені та майданчик для обговорення досягнення спільних цілей сталого розвитку. Багатостороння міжнародна торгівля розширює

можливості для внутрішньої людиноцентричної соціальної та економічної політики, полегшує вихід держав із бідності та покращує перспективи для вразливих верств населення, зокрема заохочуючи права жінок.

Вільна багатостороння торгівля за певних умов сприяє зменшенню зубожіння, Наприклад, протягом 2015-2021 років Китай успішно скоротив кількість населення, яке живе в бідності, з 55,75 мільйонів до нуля. Такого результату вдалося досягнути через зменшення невизначеності торговельної політики, а, отже, підвищення її ефективності, що, у свою чергу, призвело до зростання прибутків національних підприємств. Стабільне та передбачуване торговельне середовище сприяло збільшенню експорту та посиленню конкуренції, а, отже, зниженню цін та підвищенню якості товарів. Насамкінець, багатостороння торгівля стимулювала інновації та зростання, зокрема, і в медичній та соціальній сферах.

Відтак, ре-глобалізація має стати відповіддю міжнародного співтовариства на загрозливі тенденції відходу окремих держав до фрагментації та умовного поділу світу на "блоки". Особливістю сучасного відкату до протекціонізму в міжнародній торгівлі, є ініціатива, яка походить не від приватних акторів, а від урядів держав, що надають перевагу сумнівним інтересам національної безпеки над добробутом власного населення. Це не лише справляє негативний вплив на систему захисту прав людини, однак, зважаючи на причини розпаду Другої світової війни, піднімає питання щодо миру й безпеки в усьому світі.

Література

World Trade Report (2023). Re-globalization for a secure, inclusive and sustainable future. WTO. URL: https://www.wto.org/english/res_e/booksp_e/wtr23_e/wtr23_e.pdf

Павленко, О. (2023). Товарооборот России и Китая достиг рекордных \$190 млрд. *Коммерсант*. URL: <https://www.kommersant.ru/doc/5761392>

Report of the Human Rights Committee (1980). Official records of the General Assembly, Thirty-seventh Session. Supplement No. 40, (A/37/40), annex V.

Polachek, S. (1980). Conflict and Trade. *The Journal of Conflict Resolution*, 24(1). URL: <https://journals.sagepub.com/doi/10.1177/002200278002400103>

Miaojie, Yu. (2023). Re-globalization or fragmentation: choices and challenges. *Opinion piece*. URL: https://www.wto.org/english/res_e/booksp_e/wtr23_e/wtr23_e.pdf

Дем'янюк Ольга Борисівна
кандидат економічних наук, доцент,
Західноукраїнський національний університет,
м. Тернопіль, Україна
ORCID: 0000-0002-4699-0172

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО З ПИТАНЬ ЕНЕРГЕТИЧНОЇ БЕЗПЕКИ

Енергетика, будучи стратегічно важливою галуззю економіки будь-якої країни, в умовах інтеграції та глобалізації світової економіки, виходить за межі внутрішньої політики конкретної держави та є важливим елементом не тільки національної безпеки, а й міжнародної.

Енергетична безпека є критично важливим аспектом управління енергетичною системою кожної країни та ключовим аспектом міжнародних відносин (Marhold, 2021), а отже тісно пов'язана з національною безпекою та зовнішньою політикою

Енергетичну безпеку як невід'ємну складову національної безпеки розглядають як «стан забезпеченості держави в паливно-енергетичних ресурсах, надійність та доступність їх постачання, що передбачають диверсифікацію енергетичних джерел, конкурентоспроможність та зниження монополії на енергетичні ресурси, запровадження енергозберігаючих технологій та розвиток альтернативних джерел енергії» (Шульга, 2019, С. 340).

Важливість енергетики для економічного розвитку країн, нерівномірність розподілу енергетичних ресурсів між країнами світу та необхідність боротьби зі зміною клімату, зумовлюють необхідність створення відповідних структур та вимагають налагодження міждержавного механізму співпраці в межах функціонування світової енергетичної системи. Розвиток міжнародного співробітництва у енергетичній сфері повинне здійснюватися на умовах безперебійного, безпечного і стабільного функціонування енергетичного сектору та забезпечення національних інтересів його учасників.

Останніми роками світові енергетичні ринки пережили потрясіння через пандемію коронавірусу та війну росії в Україні, а це ще більше загострило питання енергетичної безпеки та вимагає посиленого міжнародного співробітництва та діалогу між виробниками, споживачами та транзитерами енергоресурсів.

В основному міжнародне співробітництво в енергетичній сфері здійснюється на міждержавному та наднаціональному рівнях.

Міжнародне співробітництво щодо регулювання світового енергетичного ринку чи окремих його секторів на наднаціональному рівні здійснюється в межах спеціалізованих міжнародних організацій та форумів (Організація країн-експортерів нафти (ОПЕК), Міжнародне агентство з атомної енергії (МАГАТЕ), Агентство з ядерної енергії (АЯЕ), Міжнародне енергетичне агентство (МЕА), Міжнародне агентство з відновлюваної енергії (IRENA), Європейське Енергетичне Співтовариство, ЮНІДО, ООН тощо), які сприяють співробітництву між країнами у сфері енергетики, обміну інформацією, розробці міжнародних стандартів і правил та декларують сприяння глобальному енергетичному переході до чистої, низьковуглецевої, ефективної та безпечної глобальної енергетики.

Міждержавне міжнародне співробітництво реалізується через:

- укладання міжнародних (двосторонніх та багатосторонніх) угод і договорів, спрямованих на регулювання та спільне управління енергетичними ресурсами;

- розробку транскордонних енергетичних проектів, що полегшують транзит та транспортування енергоресурсів (газопроводи, електромережі) та сприяють ефективному використанню ресурсів та забезпеченню надійних постачань;

- спільну розробку і впровадження нових енергетичних технологій та реалізацію науково-дослідницьких проектів в галузі енергетики, таких як відновлювальна енергія і зберігання енергії, що сприяє підвищенню стійкості та зменшенню негативного впливу на навколишнє середовище.

Питання енергетичної безпеки формують сучасні міжнародні енергетичні відносини таким чином, що з одного боку, вони призводять до нових стратегічних альянсів і співпраці

між державами, які є основними гравцями на енергетичному ринку, а з іншого – вони є джерелами міжнародної напруженості, конкуренції та конфлікту, головним чином через розбіжність енергетичних інтересів та ролі на енергетичному ринку: країни-виробники (експортери) прагнуть забезпечити надійний попит на свої товари, і, тим самим забезпечити стабільні фінансові надходження від продажу енергоресурсів; країни-споживачі (імпортери) намагаються диверсифікувати джерела та постачальників енергоресурсів для того, щоб мінімізувати свою залежність від постачання енергетичних ресурсів із зовнішніх джерел і максимізувати свою енергетичну безпеку; а транзитні держави намагаються максимально використати свою роль транзитера через отримання максимального прибутку за надання відповідних послуг.

Значні коливання цін на світовому енергетичному ринку та виснаженість запасів традиційних видів енергоресурсів вимагають від країн-імпортерів диверсифікувати джерела енергопостачання, що посилює конкуренцію між країнами-експортерами. Саме диверсифікація енергопостачання є основною стратегією, яка використовується країнами для вирішення проблем енергетичної безпеки та забезпечення стійкості до шоків у постачанні енергії, при цьому необхідно враховувати не тільки різні джерела енергії, але й різних імпортерів і різні транзитні маршрути (Strojny, 2023).

Для будь-якої країни питання енергетичної безпеки залежить від низки таких чинників, як власна забезпеченість джерелами енергії, баланс експорту/імпорту енергоносіїв, структура диверсифікації енергопостачань, рівень споживання тощо. В межах держави високого рівня енергетичної безпеки можна досягти за рахунок внутрішнього (національного) або зовнішнього (імпортного) енергопостачання. Важливе значення у забезпеченні енергетичної незалежності, зменшення залежності від імпорту енергоресурсів та підсиленні власної енергобезпеки має розвиток альтернативної енергетики (відновлювальна енергія, ядерна енергія, технології збереження енергії).

Забезпечення міжнародної енергетичної безпеки вимагає спільних зусиль багатьох країн та міжнародних організацій для

розв'язання глобальних енергетичних викликів, таких як забезпечення постачання енергії, зменшення впливу на довкілля та забезпечення стійкості глобальних енергетичних ринків на основі забезпечення сталості, ефективності та безпеки глобальної енергетичної системи.

В сучасних умовах міжнародне співробітництво сприяє: розвитку та стабільності світового енергетичного ринку; попередженню конфліктів, пов'язаних з постачанням енергії та доступом до енергетичних ресурсів; стимулюванню розвитку та поширенню відновлювальних джерел енергії; покращенню доступу до енергії для країн, населення, яких не має сталого енергетичного постачання; фінансовій та технічній підтримці щодо розвитку та модернізації енергетичної інфраструктури; спільній розробці проєктів та технологій для зменшення енерговтрат під час транспортування та зберігання енергії тощо і, тим самим забезпечує глобальну енергетичну безпеку.

Література

Marhold, A.-A. (2021). Unpacking the Concept of 'Energy Security': Lessons from Recent WTO Case Law. *Legal Issues of Economic Integration*, 48, 147-170. URL: <https://ssrn.com/abstract=3848617>

Strojny, J., Krakowiak-Bal, A., Knaga, J., Kacorzyk, P. (2023). Energy Security: A Conceptual Overview. *Energies*, 16(13). URL: <https://doi.org/10.3390/en16135042>

Шульга, Є. В. (2019). Основи міжнародно-правового забезпечення енергетичної безпеки. *Право і суспільство*, 4, 337-342. URL: <https://doi.org/10.32842/2078-3736-2019-4-50>

Фоменко Діана Ігорівна
*Запорізький національний університет,
м. Запоріжжя, Україна*

ТРАНСФОРМАЦІЯ СИСТЕМИ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

З моменту повномасштабного вторгнення росії на територію України роль нашої держави у функціонуванні система міжнародного співробітництва є однією з провідних. Згідно з даними, наведеними на сайті Міністерства закордонних справ України, Україна активно співпрацює з такими міжнародними організаціями як, Рада Європи, ЮНЕСКО, Організація Об'єднаних Націй, Світова організація торгівлі (СОТ), Організація з безпеки і співробітництва в Європі (ОБСЄ), ОЧЕС тощо. Також, як зазначається, Україна має постійні представництва при Європейському Союзі, місію при НАТО, при ООН, ЮНЕСКО та Раді Європи (Сайт Міністерства закордонних справ України, 2019), які дозволяють ширше представляти інтереси нашої держави на світовій арені.

Вторгнення агресора на територію України 24 лютого 2022 року спонукало міжнародну спільноту до активних дій з їхнього боку. 28 лютого Володимир Зеленський підписав заявку на членство України у Європейському Союзі. У документах йдеться про те, що Україна поважає цінності, закріплені у статті 2 Договору про Європейський Союз, і має честь подати заявку на членство відповідно до статті 49 цього Договору. «Україна, заплативши таку величезну ціну за європейський вибір та безпеку Європи, буде в змозі пройти цей шлях», – наголошується в документах (Офіційне інтернет-представництво Президента України Володимира Зеленського, 2022). Свій статус кандидата на членство в ЄС країна отримала вже 23 червня того ж року. Даний статус кандидата відкриває можливості отримання фінансової допомоги у трансформації суспільства, правової системи

та економіки на шляху до членства в ЄС, а також триматиме євроінтеграційні реформи нашої країни у пріоритеті. Україні буде доступна фінансова допомога для країн, які готуються для вступу до ЄС (Інструмент передвступної допомоги, ІРА). Така допомога може надаватись через гранти, інвестиції або як технічна допомога. Кандидатство також відкриває для України участь у програмах та ініціативах Євросоюзу (Єдиний веб-портал органів виконавчої влади України, 2022).

Дана статистика свідчить про те, що міжнародні організації, на прикладі ЄС, збільшили увагу до питань колективної безпеки та потреб України в підтримці. Багато країн, включаючи США та країни Європейського Союзу, ввели санкції проти країни-агресора відповідно до її дій в Україні. Це свідчить про суттєву зміну ставлення до росії в системі міжнародному співробітництві. Крім того, війна на території України викликала значну гуманітарну кризу, яка, в свою чергу, спричинила великий потік біженців та внутрішньо переміщених осіб, котрі потребують прихистку та психологічної допомоги. Ця криза гучно ставить питання про готовність і здатність міжнародного співтовариства ефективно реагувати на подібні ситуації.

Утім, одним з найголовніших питань, яке постало з 24 лютого 2022 року – питання про дієвість міжнародних організацій, таких як Організація Об'єднаних Націй (ООН) і Організація з безпеки та співробітництва в Європі (ОБСЄ).

Як зазначає [detector.media](#), з посиланням на висловлення політичного аналітика Артура Колдомасова (який свого часу пройшов стажування у постійному представництві Святого престолу при міжнародних організаціях у Відні, а саме при ОБСЄ, МАГАТЕ, Організації Об'єднаних Націй із промислового розвитку, Управлінні ООН із питань космічного простору та інших), питання щодо можливостей міжнародних організацій та їх реальний вплив на ситуацію виникало в усіх конфліктах, які сталися після Другої світової війни. «Під час югославських війн також поставало питання щодо доречності ООН та її інституцій. Зараз воно звучало по-новому, однак треба розуміти, що якихось повноважень і мандату, щоби приїхати та сказати «Припиніть!», у цих організацій немає. Адже вони не були так

створені першочергово. Якби вони мали надто велику силу, то це могло би перетворитися на глобальний уряд, чого не хоче низка країн, і я не думаю, що багато хто з українців хотів би такий формат», – каже експерт (Семенюта, 2023). Також, доречно навести слова Голови Українського центру безпеки та співпраці Сергія Кузана, який зазначив, що міжнародні організації, зокрема ООН, були створені як превентивні. Водночас війна в Україні оголила всі проблеми міжнародної архітектури безпеки, й виконати свою основну функцію превенції організаціям не вдалося. «Процедурність та бюрократизованість взяли гору над принципами, за якими створювалася Організація Об'єднаних Націй та її структурні підрозділи. Із 1970-х років ніхто у світі не оголошує війн, це робиться по-іншому, але суть не змінюється. Світ бачив, як готувалася ця війна в Україні ще з 2014 року, й ООН нічого не зробила. Коли схожа ситуація була в Іраку, ООН могла створити спеціальний військовий підрозділ задля стабілізування ситуації. Там були слабші держави, а коли перед ООН виникла Росія, архітектура безпеки посипалася», – зазначив експерт (Семенюта, 2023).

Дані висловлювання експертів свідчать про те, що дійсно ООН та подібні організації, які повинні надавати допомогу Україні щодо врегулювання військових дій та всебічно заохочувати громадськість до дій, цього не роблять, бо вони втратили свою ефективність через бюрократизацію та той факт, що вони не були для цього створені.

Трансформація системи міжнародного співробітництва в умовах російсько-української війни зазнала колосальних масштабів. Приміром, такий економічний і політичний союз, як ЄС, зробив великий крок назустріч Україні на її шляху до вступу у ЄС, оскільки таке прагнення у нашій державі існує з 03.2014 року – після Революції Гідності – підписання політичної частини Угоди про асоціацію, як зазначило Міністерство юстиції України (Сайт Міністерства юстиції України). НАТО засудила найбільш рішучим чином жорстоку і неспровоковану загарбницьку війну Росії проти України – незалежної, мирної і демократичної країни, близького партнера Альянсу. Як НАТО, так і держави-члени Альянсу продовжують надавати Україні допомогу

на безпрецедентному рівні з метою гарантування її основоположного права на самооборону (Сайт Організації Північноатлантичного договору, 2023). Втім незрозумілим залишається один факт – коли уламки ймовірного російського безпілотнока знайшли в районі села Плауру, що у Румунії, у повіті Тулча, що межує з українським містом Ізмаїл на Одещині, міноборони Румунії заперечувало цю інформацію через 2 дні. Це може свідчити про те, що не всі країни-члени міжнародних альянсів (Румунія є країною-членом НАТО з 2004 року) хочуть вступати у відкриту конфронтацію з росією. Причиною цього можуть бути такі чинники, як:

1. Страх перед ескалацією конфлікту;
2. Різні національні інтереси (наприклад, економічні та енергетичні, політичні інтереси);
3. Міжнародні обов'язки;
4. Економічні зв'язки з Росією;
5. Роздвібненість інтересів і тощо.

Як зазначає речник МЗС України Олега Ніколенко, «це [падіння російського безпілотнока на території Румунії] є черговим підтвердженням того, що російський ракетний терор становить величезну загрозу не лише безпеці України, але і безпеці сусідніх країн, зокрема держав-членів НАТО». Цей факт свідчить, що бездіяльність міжнародних структур може породити більше напруженості в регіоні та призвести до військових або політичних конфліктів за її межами. Важливо, щоб міжнародні організації і держави дотримувалися засад міжнародного права, активно співпрацювали для вирішення конфліктів і вчасно реагували на подібні інциденти, щоб запобігти ескалації та забезпечити стабільність і безпеку в регіоні.

Загалом, можна говорити про те, що система міжнародного співробітництва зазнала кардинальних змін в умовах російсько-української війни. Міжнародна спільнота активно допомагає Україні та сприяє її перемозі різнорізними шляхами: це і низка заходів щодо наближення її членства в ЄС, і систематичне надання потужної допомоги (як фінансової, так і гуманітарної) багатьма країнами, і проведення на міжнародному рівні численних самітів, де обговорюються важливі питання стосовно

України та війни, тощо. Отже, все це свідчить про резонансну зацікавленість провідних країн світу та міжнародної спільноти щодо найшвидшої перемоги України, бо наслідки російсько-української війни вже можна побачити не тільки на території нашої держави, адже вони вже поширюються (як-от безпрецедентний теракт ХАМАСу проти Ізраїлю та новий спалах війни між Ізраїлем та Палестиною) й можуть зростати надалі. І система міжнародного співробітництва заради цього вже зазнала значних трансформаційних змін, безпрецедентних з моменту завершення II Світової війни.

Література

Представництва України при міжнародних організаціях (2019). *Сайт Міністерства закордонних справ України*. URL: <https://mfa.gov.ua/mizhnarodni-vidnosini/predstavnictva-ukrayini-pri-mizhnarodnih-organizacijah>.

Володимир Зеленський підписав заяву на членство України у Європейському Союзі (2022). *Офіційне інтернет-представництво Президента України Володимира Зеленського*. URL: <https://www.president.gov.ua/news/volodimir-zelenskij-pidpisav-zayavku-na-chlenstvo-ukrayini-u-73249>.

Україна отримала статус кандидата на членство в ЄС (2022). *Єдиний веб-портал органів виконавчої влади України*. URL: <https://www.kmu.gov.ua/news/ukrayina-otrimala-status-kandidata-na-chlenstvo-v-yes>.

Семенюта, І. (2023). Ефективні чи марні: чому міжнародні організації весь час лише «стурбовані». *Детектор медіа*. URL: <https://ms.detector.media/trendi/post/32364/2023-07-07-efektyvni-chy-marni-chomu-mizhnarodni-organizatsii-ves-chas-lyshe-sturbovani/>.

Як Україна рухається до ЄС. *Сайт Міністерства юстиції України*. URL: <https://minjust.gov.ua/m/yak-ukraina-ruhaetsya-do-es>.

Відповідь НАТО на вторгнення Росії в Україну (2023). *Сайт Організації Північноатлантичного договору*. URL: https://www.nato.int/cps/uk/natohq/topics_192648.htm.

Мосієнко Оксана Вікторівна

кандидат економічних наук, доцент,

Поліський національний університет, м. Житомир, Україна

ORCID: 0009-0002-6148-2018

Якобчук Валентина Павлівна

кандидат економічних наук, професор,

Поліський національний університет, м. Житомир, Україна

ORCID: 0000-0003-2147-7994

БРЕНД УКРАЇНИ У СВІТОВОМУ ПРОСТОРИ

Бренд країни – це образні уявлення, які формують позитивний імідж і репутацію країни в світі, стають перспективною економічною зростаючою через розвиток певних галузей та послуг (Арончук, 2008, С. 47).

Культурно-історичний простір України увиразнює національну ідентичність, водночас представляє країну як багатонаціональне й мультикультурне середовище. Україна має безліч історико-культурних об'єктів, які формують стале уявлення про традиції та цінності нашого народу, сприяє позиціонуванню України, як колиски європейської цивілізації та невід'ємної частини європейської культурної спадщини. У нинішніх реаліях посилена увага до України, як європейської країни, сприяє формуванню її позитивного іміджу через культурно-історичну спадщину (історичні пам'ятки, знакові імена культурних/історичних діячів) та матеріальну культуру (звичаї, обряди, традиційні ремесла, національну кухню). Саме культурно-історичний спадок України має стати основою формування бренду у світі.

Формування сучасного бренду України у світовому просторі – це складний та довготривалий процес, який потребує зусиль держави, бізнесу та громадськості (Ukraine Now, 2023, рубрика). Одним з головних елементів формування сучасного бренду країни є позитивний імідж країни, який забезпечується успішною реалізацією національних потенціалів. Україна має потужний культурний та історичний потенціал, а також великий

потенціал у сфері технологій, особливо в IT-секторі. За останні роки, Україна зарекомендувала себе як досить приваблива для інвесторів країна (Липяцька, 2023, рубрика).

Щоб сформувати сучасний бренд України, необхідно виконати кілька важливих кроків (Ukraine Now, 2023, рубрика):

- розробити стратегію територіального світового брендингу, яка включає в себе аналіз національних особливостей, історії та культури України, а також потенціалу країни в різних сферах;
- створити ефективний інформаційний та комунікаційний механізм, який дозволить просувати позитивний імідж країни на світових ринках. Це може бути здійснене через використання різних засобів масової інформації, в тому числі соціальних мереж;
- створити і підтримувати інфраструктуру, яка приваблює інвесторів та туристів. Це може бути здійснено через розвиток транспортної мережі, готелів та ресторанів, а також розвиток технологічної інфраструктури;
- розвивати партнерські відносини з іншими країнами, оскільки це дозволяє покращувати імідж країни у світовому просторі.

Формування сучасного бренду України у світі повинно бути спрямоване на підвищення національної свідомості громадян та впізнаваності бренду у світі, зміцнення позицій країни на міжнародному ринку та привертання інвесторів і туристів. Важливою частиною стратегії формування сучасного українського бренду є корпоративна ідентичність. Термін є суто маркетинговим, але легко адаптується у територіальний брендинг. Сьогодні народ України міцно згуртований і кожен відчуває приналежність до єдиного національного центру. Саме така приналежність формує із розрізненого соціуму нову національну корпоративну структуру суспільства.

Основними інструментами, які можуть використовуватися для підтримки сформованого українського бренду є:

– Реклама історико-культурних пам'яток та туристичних «родзинок» в іноземних ЗМІ. Наприклад, розміщення реклами в національних телевізійних каналах, спеціалізованих виданнях, на рекламних щитах в містах і на вулицях, дозволить залучити увагу широкої аудиторії до бренду України.

– Підтримка участі у України в національних та міжнародних виставках та ярмарках. Участь у виставках та ярмарках, що відбуваються в Україні та за її межами, дозволить залучити увагу потенційних партнерів, клієнтів та інвесторів до товарного та промислового бренду України та продемонструвати його потенціал.

– Спонсорство та благодійність. Українські компанії можуть спонсорувати різноманітні благодійні проекти, такі як підтримка ветеранів, допомога дітям з особливими потребами, розвиток науки та культури, охорона навколишнього середовища тощо (Ukraine Now, 2023, рубрика). Це дозволить не тільки зробити добру справу, але й залучити увагу громадськості та іноземних партнерів до бренду України та його цінностей.

– Інфлюенс просування. Взаємодія з впливовими особистостями, співпраця з відомими блогерами, зірками, відомими особистостями дозволить залучити увагу широкої аудиторії до бренду України у світі та продемонструвати переваги країни (Липяцька, 2023, рубрика).

Отже, для формування і підтримки (просування) бренду України у світі, потрібно основну увагу приділити її культурно-історичному потенціалу, адже вікова історія нашої країни загубилася у світі, розчинилась радянським минулим та була вкрадена ворожим сусідом. Сьогодні настав час відновити історичну велич України шляхом формування її бренду в історико-культурному просторі Європи та світу. Бренд формується різноманітними заходами та інструментами, що включають в себе як традиційні, так і сучасні методи територіального бренд менеджменту. Брендкування України в просторі Європи та світу, як країни з унікальною культурною, історичною спадщиною та економічним потенціалом дозволить сформувати позитивний імідж України у світі, збільшити її туристичний потенціал для внутрішнього і зовнішнього споживача та дозволить використати геополітичне розташування України для покращення інвестиційного клімату країни.

Література

Ukraine Now міжнародна маркетингова кампанія українського уряду. URL: <https://www.ukrainenow.org>

Aronczyk, M. (2008). "Living the Brand": Nationality, Globality and the Identity Strategies of Nation Branding Consultants. *International Journal of Communication*, 43-54.

Липяцька, М. Бренд України за рік у світі зміцнився. URL: <http://nv.ua/ukr/opinion/viy-na-yak-zmicnivsya-brend-ukrajini-u-sviti-novini-ukrajini-50307878.html>

გიორგი კლიმიაშვილი

სტუ,

სამართლისა და

საერთაშორისო ურთიერთობების ფაკულტეტი

საერთაშორისო ურთიერთობათა სუბიექტის მნიშვნელობა

საერთაშორისო ურთიერთობების თეორიაზე საუბრისას, ერთ-ერთი უმთავრესი საკითხი საერთაშორისო ურთიერთობათა სუბიექტების საკითხია. საერთაშორისო სამართალი სახელმწიფოს განიხილავს, როგორც საერთაშორისო სამართლის ისტორიულად შემდგარ სუბიექტს.

საერთაშორისო სამართალსუბიექტობა რეალიზდება საერთაშორისო სამართლით განსაზღვრული უფლებებისა და ვალდებულებების ერთობლივი განხორციელებით (Фельдман, Курдюков, 1974). სახელმწიფოთა შორის წარმოშობილი ვალდებულებათა ხასიათი და მასშტაბი საერთაშორისო საჯარო სამართლის ნორმებშია კოდირებული, რომელიც ეყრდნობა *Pacta sunt servanda*-ს პრინციპს¹.

თანამედროვე საერთაშორისო სამართლის საწყის ეტაპად მიჩნეულია 1648 წლის ვესტფალის ზავი. სწორედ მითითებული ზავის პერსპექტივიდან განიხილება საერთაშორისო სამართალსუბიექტობა (Gross, 1948, P. 26). სუბიექტისათვის დამახასიათებელი უფლება-მოვალეობანი იყოფა ზოგადსუბიექტურ ე.ი ყველა სახის სუბიექტისთვის დამახასიათებელ და სპეციფიკურ ე.ი მხოლოდ სუბიექტთა გარკვეული ტიპისათვის დამახასიათებელ უფლება-მოვალეობებად.

საერთაშორისო სამართალსუბიექტობით სარგებლობენ: სახელმწიფოები, დამოუკიდებლობისათვის მებრძოლი ერები,

¹ საერთაშორისო სამართალში ხელშეკრულებისადმი ერთგულების პრინციპი – ხელშეკრულებები უნდა შესრულდეს.

რომლებიც სახელმწიფოებრიობის მოპოვებას ცდილობენ, საერთაშორისო მთავრობათაშორისი ორგანიზაციები, სახელმწიფოთა მსგავსი სფეციფიკური წარმონაქმნები. თანამედროვე საერთაშორისო სამართალი გარკვეული მოცემულობით სუბიექტად ცნობს აგრეთვე თავისუფლებისათვის მებრძოლ ერს ან ხალხს (ლ. ალექსიძე, 2010, p. 57). საერთაშორისო სამართალი, სამართლის სუბიექტად მიიჩნევს მთლიანად სახელმწიფოს და არა მხოლოდ სახელმწიფო ხელისუფლებას. საერთაშორისო სამართლის სუბიექტების კლასიფიკაცია შეიძლება ორი კატეგორიის მიხედვით: სუვერენულ და არასუვერენულ სუბიექტებად. სუვერენულ სუბიექტებად გვევლინება სახელმწიფო და დამოუკიდებელი სახელმწიფოებრიობისათვის მებრძოლი ერი და ხალხი. არასუვერენულ სუბიექტებს წარმოადგენენ საერთაშორისო მთავრობათაშორისი ორგანიზაციები, ასევე სახელმწიფოთა მსგავსი სპეციფიკური წარმონაქმნები. საერთაშორისო სამართლის სუბიექტად ასევე მიიჩნევენ ერთობას, რომელსაც უნარი შესწევს ისარგებლოს საერთაშორისო უფლებებით და იტვირთოს საერთაშორისო ვალდებულებები, აგრეთვე საერთაშორისო სამართლებრივ ველში განახორციელოს განსაზღვრული მოქმედებები (Henkin, Pugh, Schachter, Smit, 1987, P. 228). თუმცა, აქვე უნდა აღინიშნოს, რომ სრული უფლებაუნარიანობა მხოლოდ სახელმწიფოებს გააჩნიათ.

საერთაშორისო სამართლებრივ ურთიერთობებში, სახელმწიფოს ყველა თვისება უკავშირდება სუვერენიტეტს, რომელიც სახელმწიფოს პოლიტიკურ-სამართლებრივი თვისებაა. აღნიშნული უფლებით სარგებლობისთვის სახელმწიფოებს უნდა გააჩნდეთ დამოუკიდებელი მთავრობა, მოსახლეობა და ასევე ჰქონდეთ საკუთარი ტერიტორია (პიერ დე სენარკლენი იოან არიფენი, 2014). საერთაშორისო სამართლის თეორიაში, საერთაშორისო სამართალსუბიექტობის ტრადიციული კონცეფცია, უწინარეს ყოვლისა, განმარტებულია, როგორც სუვერენული სახელმწიფოს ხარისხი. აგრეთვე როგორც პრაგმატული კონცეფცია, რომელიც საერთაშორისო სამართლის თვალსაზრისით მიუთითებს ერთობის არსებობაზე (ნოდარ თოფურიძე, 2015). საერთაშორისო სამართლის სუბიექტები შეიძლება განისაზღვრონ როგორც

საერთაშორისო ურთიერთობებში ერთმანეთისგან დამოუკიდებელი წარმონაქმნები, რომლებსაც საერთაშორისო სამართლით დადგენილი უფლება-მოვალეობათა დამოუკიდებლად განხორციელების იურიდიული უნარი გააჩნიათ (Тункин, 1982, С. 83).

ბიბლიოგრაფია

Фельдман, Д. И., Курдюков, Г. И. (1974). *Основные тенденции развития международной правосубъектности*. Казань.

Gross, L. (1948). The Peace of Westphalia 1648-1948. *American Journal of International Law*, 42, 20-41.

Nussbaum, A. (1950). *A Concise History of the Law of Nations*.

ლ. ალექსიძე (2010). თანამედროვე საერთაშორისო სამართალი. თბილისი, 57.

Henkin, L., Pugh, R., Schachter, O., Smit, H. (1987). *International Law, Cases and Materials*.

პიერ დე სენარკლენი იოან არიფენი (2014). საერთაშორისო პოლიტიკა – საგარეო სუვერენიტეტი.

ნოდარ თოფურბე (2015). საქართველოს საერთაშორისო სამართალსუბიექტობა.

Тункин, Г. И. (1982). *Международное Право*. Москва.

Козка Андрій Вікторович

кандидат наук,

*Науково-Дослідницький Інститут,
Міжнародна академія наук і інноваційних технологій, м. Київ, Україна,
Експерт з наукової дипломатії ЄС*

Білик Артем Сергійович

*кандидат технічних наук, доцент,
голова УНДЦА «Зонд», м. Київ, Україна*

КОСМІЧНІ АНОМАЛІЇ ЯК ОБ'ЄКТ НАУКОВИХ ДОСЛІДЖЕНЬ: НЕОРОМАНТИКА ТА МІЖНАРОДНИЙ ФАКТОР БЕЗПЕКИ

*«Зв'язок космічної реальності з нами
набагато глибший і буденний, ніж ми думаємо!»
Академік В.І.Вернадський (1863-1945)*

NASA доручило дослідницькій групі вивчити невідомі повітряні явища (Unidentified Anomalous Phenomena UAP), спостереження за подіями, які з наукової точки зору не можна визначити як відомі природні явища (NASA Unidentified).

Головна астрономічна обсерваторія НАН України також проводить самостійне дослідження UAP. Для спостережень UAP українські астрофізики використовують дві метеостанції. Спостереження проводилися кольоровими відеокамерами в денному небі. Також розробили спеціальну методику спостереження для виявлення та оцінки характеристик UAP.

За даними, існує два типи UAP, які умовно називають:

- (1) «Космоси» (аномальні явища) та
- (2) «Фантоми».

Відзначимо, що Космоси – це світні об'єкти, яскравіші за фон неба. Фантоми – це темні об'єкти з контрастністю від кількох до приблизно 50%. Ми спостерігаємо значну кількість об'єктів, природа яких не ясна (Жиляєв, Петухов, Решетник, 2022; Білик, Коваленко, Керіченко, 2023).

Об'єктом наукового дослідження є навколишній світ, та форми його відображення у свідомості людей, які існують незалежно від нашої свідомості, відбираються відповідно до мети дослідження.

Зрозуміло, що наукова громадськість не завжди бачить все тільки в об'єктивно-науковому факторі а багато дослідників та взагалі спільнот, товариств романтичні ідеали щодо космосу та космічних проявлень на межі реальності та фантастики. Це також позитивно та нормально: поєднання практицизму в науці та філософських концепцій неоромантизму і головне не плутати почуття з науковими фактами!

Неоромантика у філософії: 1) Надзвичайність, незвіданість, неототожність чогось, що викликає емоційно-піднесене ставлення. 2) Художній метод у фантастичній літературі й мистецтві, прийнятий оптимізмом і прагненням показати в яскравих образах призначення людини. 3) Умонастрій, який характеризується ідеалізацією дійсності, мрійливою споглядальністю.

Щодо «державницького» та правового-секретного фактору, то можна зрозуміти, що також спеціальні служби держав та навіть 33 засідання ООН щодо проблематики АЯ (НЛО) відстежують цей момент як серйозний фактор безпеки. Так, на сайтах ЦРУ та федерального бюро розслідувань ФБР США можна ознайомитись з розсекреченими документами цього напрямку на звітах відповідно законодавства про зняття грифу секретності (FBI official web; Железняк, Козка, 2007).

Наприклад: зустрічається такий формат «СЕКРЕТНО: ТІЛЬКИ ЧИТАТИ» “SECRET:FOR EYES ONLY” та інші рівні та ступені секретності.... Конкретно немає фото прибульців, але є в соц.мережах відео нібито «збитих тарілок» та допиту прибульця. Але, досі нічого конкретного немає, бо чиновники та політики не беруть відповідальність.

Нобелівські лауреати, вітчизняні дослідники (Железняк, Козка, 2007) кажуть, що реальність також не так проста к вважають багато людей, можуть існувати *паралельні світи (parallel worlds)* та навіть *вертикальні вимір (vertical demensions)* і, куди людство може потрапити лише через певні умови: 1) якісна екологія,

2) відсутність ядерних випробовувань та війн та 3) біоетичного підходу до їжи (рух веганів), тобто людина дійсно повинна бути не егоцентрична а розумна, трансцендентна, духовна. Наука не завжди несе за це юридичну відповідальність.

Відомо, що американський фізик – розробник атомної бомби Оппенгеймер цікавився прадавніми технологіями та філософськими ідеями ведійського періоду Махабхарати та звісно класики перевіреної часом - Бхагавад гіти (11:32) та навіть цитував її: **ми знали, що світ не буде таким, як раніше**. Хтось сміявся, хтось плакав, більшість людей мовчали. Я згадав рядок з індуїстського писання Бхагавад-Гіти. Шрі Крішна намагається переконати принца Арджуну *виконати свій військовий обов'язок* і, щоб справити враження на нього, набуває багаторукої форми та каже: «*Тепер Я – володар світів став Смертю, руйнівником світів!*» (Oppenheimer).

Висновки. Можливо, доступ до реальних космічних об'єктів (прибульців з космосу, уламків космічних кораблів) – це вже не просто неоромантизм а практичний доступ до нових, надсучасних технологій в наш складний час вважається саме це відігравати буде роль кінцевого впливу на Перемоги у війнах ХХІ сторіччя. Ми, пропонуємо орієнтуватися на досвід як практичної академічної науки, астрофізиків, НАСА, Національної Академії наук України, військових, правоохоронців, так і громадські об'єднання, мудрість прадавніх культур для розуміння наскільки можуть бути корисними людству нові технології та підходи в синтезі науки для розвитку цивілізації заради мирного співіснування в сучасності та майбутньому.

Література

NASA Unidentified Anomalous Phenomena Independent Study.
URL: <https://science.nasa.gov/uap/>

Жиляєв, Б. Є., Петухов, В. Н., Решетник, В. М. (2022). Непізнані повітряні явища Спостереження за подіями. Головна астрономічна обсерваторія НАН України. *Cornel University*. URL: <https://arxiv.org/abs/2208.11215>

Білик, А., Коваленко, Є., Керіченко, О. (2023). УНДЦА «Зонд» Developers Meeting 2023-07-09 – Special with the Ukrainian SRCAA/Zond project <https://zond.kiev.ua>. URL: https://www.youtube.com/watch?v=ndfK3_V266M

Maccabee, B. (2000). *UFO/FBI Connection: The Secret History of the Government's Cover-Up Paperback*. URL: <https://www.amazon.com/UFO-FBI-Connection-Governments-Cover-Up/dp/1567184936>

FBI official web UFO documents. URL: <https://vault.fbi.gov/UFO>

Железняк, Г., Козка, А. (2007). *Параллельные миры*. Харьков – Киев.

Oppenheimer, J. R. Now I am become death... URL: <https://www.atomicarchive.com/media/videos/oppenheimer.html>

Oppenheimer: How he was influenced by the Bhagavad Gita. *BBC UK*. URL: <https://www.bbc.co.uk/news/world-asia-india-66288900>

КРИЗА СУЧАСНОЇ СИСТЕМИ МІЖНАРОДНОЇ БЕЗПЕКИ

Бадер Антон Васильович

доктор політичних наук, доцент,

ДЗ «Луганський національний університет імені Тараса Шевченка»,

м. Полтава, Україна

ORCID: 0000-0002-3670-5753

РОСІЙСЬКО-УКРАЇНСЬКА ВІЙНА КРИЗЬ ПРИЗМУ ЛОГІКИ ФУНКЦІЮВАННЯ КАПІТАЛІСТИЧНОЇ СВІТ-ЕКОНОМІКИ

Протягом усієї історії людства війна виступала могутнім засобом впливу на політичний процес. Проте динамічний розвиток сучасного світу, ще наприкінці ХХ ст. стимулював появу концепція щодо становлення нової, постіндустріальної епохи. В 1990-х рр. поширюється ідея переходу людства до інформаційного суспільства. За логікою вказаних теорій, війна як інструмент функціонування політичних систем повинна була зникнути, оскільки необхідність боротись за матеріальні ресурси відпадає, а інтелектуальні здобути насильницьким способом практично не можливо. Однак, названі особливості сьогодення не зумовили відмови від застосування війни в політичному процесі. Численні агресивні війни й воєнні конфлікти, нехтування міжнародним правом, очевидна дисфункційність ООН та повномасштабна війна, розв'язана російською федерацією в центрі Європи ще раз доводять правильність зазначеної тези.

На наш погляд, розв'язання заявленої проблеми потребує детального розкриття механізмів сучасної світ-системи. У такому контексті важливою позицією є те, що світ-економіка неодмінно передбачає формування держави-гегемона. І. Валлерстайн щодо цього зазначає: «Ідеальною ситуацією з погляду накопичення

капіталу всередині системи як цілого, є існування домінуючої держави, досить сильної для того, щоб визначати правила гри та стежити за тим, аби вони виконувались до кінця. Коли суперництво в якості системної умови заміщується гегемонією, це не означає, що держава-гегемон може все. Проте це означає, що вона може перешкоджати змінам (порушенням) правил з боку інших» (Wallerstein, 1996, С. 98).

Перетворення однієї з держав центру на гегемона, насамперед, передбачає її першість у конкурентному ринковому середовищі у виробничій, торговій та фінансовій сфері одночасно (Wallerstein, 2000, С. 256 – 257). Зазначена зверхність здобувається за рахунок того, що претендент довгий час не вкладає великі кошти в розбудову численної армії (Wallerstein, 1996, С. 99). Конкуренція за гегемонію завершується тоді, коли ці переваги одного з претендентів надають можливість зайняти йому привілейовану позицію, не пов'язану з ринковими механізмами в ядрі світ-системи. Передусім це відбувається під час глобального воєнного конфлікту. У контексті аналізованої проблеми важливо акцентувати на тому, що фінал боротьби за гегемонію завжди передбачає перемогу певної держави в тридцятирічній Світовій війні (Wallerstein, 2000, С. 258).

І. Валлерстайн називає три світові війни, що відбулись за період існування сьогоденної капіталістичної світ-економіки. Перша – війна 1618 – 1648 рр., у межах якої після перемоги над імперією Габсбургів постала Голландська гегемонія. Друга – 1792 – 1815 рр., пов'язана з наполеонівськими війнами, перемогою над Францією та становленням гегемонії Великобританії. Третя – характеризується як американо-германська війна 1914 – 1945 рр., наслідком якої була поява гегемонії США (Wallerstein, 2000, С. 258). Вочевидь, сьогодні ми є свідками четвертої війни за гегемонію. У всіх трьох випадках морська (авіаційна) міць долала сухопутну. І в кожному випадку сили, спрямовані на збереження базової структури капіталістичної світ-економіки, перемагали ті сили, що прагнули перетворити її на світ-імперію» (Wallerstein, 1996, С. 99 – 100).

На основі зазначеного спробуємо більш детально розібратись у причинах, що підштовхнули в 2022 р. російське керівництво

перевести воєнний конфлікт, що жеврів з 2014 р. у відкриту, повномасштабну агресію та війну. Перш за все, слід зазначити, що стан світової політико-економічної системи та політичний режим у росії відповідають характеристикам, за яких розгортається глобальне протистояння за гегемонію. Так, міжнародний порядок, установлений після Другої світової війни є на сьогоднішній день абсолютно не ефективним. ООН не має можливості якісно виконувати покладені на неї функції, оскільки гегемон, що відповідальний за підтримку міжнародної системи безпеки, знаходиться на стадії згасання своєї могутності (Бадер, 2020, С. 219).

Політична система росії характеризується недемократичним режимом. Аналіз практики функціонування капіталістичної світ-економіки надає можливість стверджувати, що держави з подібними політичними режимами і стають претендентами на гегемонію. Так, наполеонівська Франція, гітлерівська Німеччина, а тепер і путінська росія намагались у силовий спосіб змінити усталений порядок речей у світі. Немає жодних сумнівів у тому, що одним із центральних завдань Кремля є зміна статусу росії, або всієї глобальної політико-економічної системи. Проте підкреслимо, що вказані зусилля не призводили до реалізації поставлених агресором цілей. «І в кожному випадку сили, спрямовані на збереження базової структури капіталістичної світ-економіки, перемагали ті сили, що прагнули перетворити її на світ-імперію» – констатує І. Валлерстайн (Wallerstein, 1996, С. 99 – 100).

Окрім того, кожного разу претендент на гегемонію, що в силовий спосіб намагався змінити міжнародну політико-економічну систему, був з числа країн центру світ-економіки. Натомість, росія розташована у напівпериферійній зоні, що підтверджується домінуванням продажу корисних копалин у структурі експорту цієї країни. На цій основі, маємо можливість припустити, що або справжній претендент на гегемонію наразі знаходиться в тіні та виявить себе пізніше, або аналізовані події запуснуть процеси сутнісної реконструкції чи, навіть, повної ревізії капіталістичної світ-економіки, яка визначала розвиток людства з середини XVI ст.

Уважаємо за потрібне зазначити, що знаходження росії в напівпериферійній зоні, її технологічна відсталість від країн центру, обумовлюють застарілість методів ведення війни, застосованих у повномасштабній агресії проти України. Зокрема, в. путін неодноразово заявляв, що його крилаті та балістичні ракети точково знищують об'єкти військової інфраструктури. Однак, високоточна космічна система наведення, по типу тієї, що використовувалась США в Перській затоці або Югославії, у росії просто відсутня. Зазначене призводить до низької точності попадання, значної руйнації цивільної інфраструктури та численних жертв серед мирного населення. Підкреслимо, що обрана в. путіним тактика тотальної війни також абсолютно застаріла. Сьогодні невелика, мобільна, рухлива група, озброєна новітнім обладнанням, цілком може протистояти значно переважаючим силам супротивника (Бадер, 2016, С. 63). Вказане цілком підтверджується провалом швидкої наступальної операції 2022 р. та численними втратами росії у техніці й живій силі.

Провальною виявилась й інформаційна кампанія росії, що передувала її агресії проти України. На відміну від 2014 р., коли ситуація була не однозначною, в 2022 р. абсолютна більшість населення України не підтримала дії рф. Підкреслимо, що навіть у Південно-Східних регіонах, які вважались лояльними до росії, громадяни активно виступили за збереження суверенітету своєї держави. Зрозуміло, що вказана ситуація стала одним із факторів неспроможності швидкого захоплення російськими військами великих міст, таких як: Харків, Маріуполь, Бахмут тощо. Разом з тим, це ж стимулювало росіян перейти до тактики терору та планомірного знищення оточених міст. Наголосимо, що численні жертви серед мирних громадян, руйнація цивільної інфраструктури, створення ситуації гуманітарної катастрофи, однозначно, переводять військово-політичне керівництво росії та особисто в. путіна у розряд військових злочинців.

Таким чином, невід'ємним елементом політичного процесу в межах капіталістичної світ-економіки є світові війни за гегемонію. Однак, пояснити дії російського президента виходячи з зовнішніх факторів, а саме функціонуванням світової політико-економічної системи, або тенденціями

в геополітиці, на наш погляд, неможливо. Росія – країна напівпериферійної зони, що експортує енергоносії, а сучасні товари з високою доданою вартістю не виробляє та не вироблятиме в найближчій перспективі. Тобто жодна реконструкція світ-економіки не може змінити місце та статус росії у цій системі. Теза Кремля стосовно військової загрози з боку України чи НАТО також виглядає нелогічною. В сучасних реаліях немає жодного практичного сенсу в захопленні території чи ресурсів, тим більш у країни з ядерною зброєю. Відповідно основними факторами, що підштовхнули російське керівництво до розв'язання російсько-української війни є внутрішні. Авторитарна політична система рф потребує зовнішнього ворога для виправдання великої кількості силових структур та репресій проти опозиції. Не мало важну роль, на наш погляд, зіграв й особистісний фактор, зокрема, викривлені переконання й збочені амбіції в. путіна та його оточення.

Література

Wallerstein, I. (2000). *The Essential Wallerstein*. New York: The New Press.

Wallerstein I. (1996). The Inter-state Structure of the Modern World-system. Smith S., Booth K., Zalewski M. (eds.). *International Theory: Positivism and Beyond*. Cambridge: Cambridge University Press, 87-107.

Бадер, А. В. (2020). *Політичні системи та збройне насилля: цілісно-системний аналіз*. Старобільськ: ДЗ «ЛНУ імені Тараса Шевченка».

Бадер, А. В. (2016) Трансформація засобів та форм реалізації збройного насилля у сучасному світі. *Науково-теоретичний альманах «Грані»*, 10, 60-65. doi: <https://doi.org/10.15421/1716106>

Цокур Євген Георгійович

доктор політичних наук, доцент,

Запорізький національний університет, м. Запоріжжя, Україна

ORCID: 0000-0002-7605-0114

Чайка Ірина Юріївна

доктор філософських наук, доцент,

Запорізький національний університет, м. Запоріжжя, Україна

ORCID: 0000-0003-2315-7724

БЕЗПЕКОВІ СТРАТЕГІЇ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ: НОВИЙ ПОГЛЯД НА СИМУЛЯКР БЕЗПЕКИ

Потреба у безпеці є однією з базових у структурі людських потреб. А.Маслоу стверджує (Maslow, 1970, С. 57), що незадоволення потреб цього рівня визначає неможливість самоактуалізації і самореалізації особистості, і, як нам видається, розвитку соціальних систем в цілому. Споглядаючи історичні віхи суспільного розвитку, очевидним стає, що безпека завжди радше існувала як концепт, ніколи в повній мірі не постаючи як феномен. Врешті, суспільні системи задля забезпечення можливості свого існування, мали задовольнитися і цим. Сам стан безпеки є надзвичайно нестійким, і епізодично являючись, переважно втрачає своє буття. Таким чином, аналізуючи сучасні безпекові проблеми світу, можемо говорити про безпеку як про симулякр, «дійсність», яка приховує той факт, що її немає» (Бодріяр, 2004, С. 5).

Перша чверть ХХІ століття засвідчила хибність та неефективність більшості безпекових моделей, розроблених та реалізованих у столітті минулому. Незважаючи на чіткі сигнали щодо перспектив суттєвого погіршення безпекового середовища на початку ХХІ століття, як на локальному, так і на глобальному рівнях, належні висновки керівництвом держав та міжнародними інституціями так і не були зроблені. Більш того, було допущено

ряд фатальних помилок у організації світового порядку та безпеки протягом цього століття. Перш за все, йдеться про помилковість у визначенні головної загрози світовій системі безпеки. Після подій 11 вересня 2001 року, першість у протистоянні викликам світовій стабільності та порядку було віддано боротьбі з несистемним тероризмом, вочевидь, не зважаючи на національне коріння цього явища. Саме на боротьбу із аморфним, позбавленим національної ідентичності, тероризмом було кинуто головні зусилля ключових фундаторів та стейкхолдерів безпеки у світі (ООН, НАТО, тощо). Наслідком стали провальні, з точки зору, як змісту, так і результату, військові операції у Іраку, Афганістані, Сирії. Більш того, справжні керманічі та утримувачі терористичних структур отримали час та можливість для підготовки організації «гідної відповіді». До того ж, як результат невдач: держави та інституції, задіяні у зазначених антитерористичних операціях, суттєво послабили свої ресурси щодо можливості подальшого впливу на світові безпекові процеси. Крім того, невдачі, суттєві матеріально-технічні витрати, людські втрати, спонукали до переосмислення, та втрати підтримки відповідної політики всередині власних суспільств. Як наслідок уже 10-х роках XXI ст. до влади в деяких ключових державах, на яких лежала відповідальність за підтримку світового порядку, приходять, або були близьким до приходу, відверті популісти, прибічники ідеї «безпекового самоналаштування». Зараз важко сказати, чи була терористична активність початку XXI ст. спланованою акцією, чи це лише збіг обставин, який було вдало використано деякими режимами для реваншу за поразки минуло століття. Проте переоцінка ролі несистемного тероризму та небажання визнавати його реальну сутність, суттєво допомогли цим геополітичним гравцям. Тим більше, що вони і так мали певний «козир у рукаві» у вигляді невирішеності питання повномасштабного ядерного роззброєння. Це дозволило деяким країнам з відверто антидемократичними тенденціями розвитку, підштовхуваними жагою реваншу та ностальгією за втраченою вдаваною величчю, імперським амбіціями, зберегти статус ядерної держави. У зв'язку із цим, напівшахрайська схема передача української ядерної зброї

рф виглядає як відверте захоочення останньої до агресивної поведінки, алегорично співставне із поверненням знаряддя злочину злочинцю прямо у залі суду. Сподівання на ймовірні перспективи демократичного розвитку країни споконвічного терору та імперіалізму, виглядають, з боку тих, хто таке рішення розробляв та реалізував, в кращому випадку, як суцільне нерозуміння історії, її закономірностей, та реалій сьогодення. А якщо врахувати ще й фактор політичної корупції (яка, безсумнівно, стала яскравою ознакою, головним бічем, світових політичних процесів та національної політики кінця ХХ – поч. ХХІ ст., і охопила політичну та бізнес верхівку практично усіх країн світу), то вимальовується доволі песимістичний сценарій щодо системи світової стабільності та безпеки. На початку другого десятиліття ХХІ ст. у світі сформувалася парадоксальна політико-безпекова ситуація, згідно якої, міжнародне співтовариство, демократичне за своєю сутністю, налаштоване на мирне, конструктивне співіснування та розвиток країн та народів світу, своїми ж руками випустило з в'язниці історії «духів війни та терору». Зарадити цьому «запамороченню» могли б міжнародні інституції. В принципі, як колективно-колегіальні органи наддержавного рівня, вони для цього і створюються. Проте. Розмови про доцільність реформування ООН, принаймні, хоча б найкритичнішої його структури, Ради Безпеки, тривають уже кілька десятиліть, але реальні кроки у цьому напрямку не дуже помітні. Міжнародно-політична та безпекова нерівність, на кшталт, суттєвих відмінностей статусу та можливостей ядерних та неядерних держав, яка зберігається і донині, зводить дії ключових міжнародних безпекових та політичних інституцій лише до рівня рекомендацій та «стурбованостей» щодо дій політичних акторів, які, через безкарність та «гуманістичну терпимість», вже втратили зв'язок із реальністю і впевнено ведуть світ, з його занадто поблажливим та толерантним ставленням, до терористичної моделі ведення міжнародної політики, до чергової катастрофи.

Отже, перспективи становлення справедливого світового порядку і формування безпекових стратегій сьогодні, на жаль, як ніколи, є дійсністю, яка приховує той факт, що її немає.

Література

Бодріяр, Ж. (2004). *Симулякри і симуляція*. Київ: Основи.

Maslow, A. H. (1970). *Motivation and Personality*. New York: Harper and Row.

Юлдашев Олексій Хашимович
*доктор юридичних наук, професор,
Міжрегіональна академія упарвління персоналом,
м. Київ, Україна*

КОНЦЕПЦІЯ УСУНЕННЯ ЗАГРОЗ ГЛОБАЛЬНІЙ ТА РЕГІОНАЛЬНІЙ БЕЗПЕЦІ

“Сучасні загрози глобальній та регіональній безпеці” – надзвичайно вдала тема сьогодення. В чому полягають “Сучасні загрози глобальній та регіональній безпеці”, ХТО їх створює і ЯК їх усунути, нейтралізувати, попередити виникнення у подальшому – це те, що зараз хвилює людську спільноту і те, чому присвячена наша Концепція усунення загроз глобальній та регіональній безпеці (Концепція декласування росії).

В Концепції позначено основні напрямки діяльності, основні задачі з усунення загроз глобальній та регіональній безпеці. Це: 1) інформаційна складова, розгортання країнами колективного Заходу інформаційної війни проти росії; 2) пропозиції щодо побудови “Нового світового порядку”; 3) формування “ядерного кулака”, запровадження принципу симетричності і адекватності.

Вважаємо, що позначені напрямки діяльності є *необхідно достатніми* для досягнення головних цілей – усунення загроз глобальній та регіональній безпеці.

Стосовно **інформаційної складової, ведення інформаційної війни**. Це найбільш важлива складова. Адже якщо країни колективного Заходу одержали б перемогу на інформаційному фронті, то агресія росії проти України і погрози західним країнам припинилась би миттєво. Про відсутність потужної протидії на інформаційному фронті свідчить той факт, що більша частина світу вважає, що Америка – це агресор, загроза усьому світу. Вона спричинила війну росії проти України і здійснює ескалацію. Єдиний, хто може успішно протистояти Америці і захистити від неї і Україну, і багато які країни світу –

це росія. Тому усі мають підтримувати її. Ось чому одним із головних (якщо не головним) напрямів руху до усунення загроз з боку росії має стати інформаційна складова, в рамках якої потрібно зібрати максимально повну, систематизовану інформацію про російський державний шовінізм. Саме він є джерелом державного тероризму, який переріс у ЗВИЧАЙНИЙ ФАШИЗМ. Саме тому для усунення загроз глобальній та регіональній безпеці необхідно визначити, викрити перед усім світом його форми і масштаби, довести інформацію про дійсний стан речей до кожної країни, до кожного жителя планети.

Будемо розуміти загрозу як здатність завдання зла, а ЗЛО – як знищення, катування, гвалтування людей, в т.ч. жінок, дітей, стариків, позбавлення їх їжі. Через розкрадання російськими загарбниками українських продовольчих ресурсів, нечуване за масштабами мінування української землі, руйнування портів, російську протидію експорту українського зерна Чорним морем, світ опинився на межі глобальної кризи продовольчої безпеки. Постраждали десятки країн, зокрема, у Африці. Зло це також руйнація усього створеного на благо людству (будинків, заводів, фабрик, енерго і іншої критичної інфраструктури – всього того, без чого сучасна людина існувати не може). Отже росія, путінський режим – це ЗЛО, направлене виключно на деструктивні цілі: по перше, на знищення людей, природи, усього живого. По друге – на виробництво, створення нової зброї масового знищення (замість виробництва того, що потрібно людині на добро, скажімо, створення нових якісних авто, смартфонів), розпалювання у світі гонки озброєнь. Ще раз: багато людей створювало, як кажуть, “у поті та крові”, виробляло те, що потрібно для життя, що робить його краще. Раптом з’являється невіглас, виходець з бандитського петербурзького підвороття, неуч, недоісторик і заявляє: “українського народу, України немає!” Оскільки цей народ і країна об’єктивно є, то недоісторик-маразматик, збирач земель “руських” починає знищувати і народ, і країну, катувати, гвалтувати, стирати із лиця землі українські міста і села. Нещодавно терористи з Гази теж шокували світ своїми звірствами. Бойовики ХАМАСа не шкодували нікого: вбивали і знущалися над солдатами, чоловіками, жінками та дітьми. Увесь

світ облетіли кадри з тими страшними звірствами, які зчинив ХАМАС. І світ здригнувся. Але ж в Ізраїлі це продовжувалось день, дні. В Україні подібне (і навіть, набагато більш людиноненависницьке) російські орки творять щоденно вже майже два (!) роки. Президент Ердоган каже: в Гаазі відбувається різанина. А що путін робить в Україні – цукерки людям роздає? Орки вбивають, катують, гвалтують. Вже всі розуміють, що російський солдат – це не “визволитель”, а садист, гвалтівник, вбивця, мародер. Важко, навіть, уявити, який ступінь озвіріння має бути у орка, щоб розправлятися з дітьми та жінками, катувати, відрізати у живих військовополонених голови або геніталії, закопувати людей в братські могили... Все це засвідчується у соціальних мережах. Це по перше. По друге – терористичний акт 7 жовтня організований росією. Кажуть, проплати ХАМАСУ за скоєне здійснювались через відповідні чеченські структури.

Абсолютне зло – це те, що спрямоване на повне знищення людства. До цього призведе світова ядерна війна, про яку вже давно товкмачить кремлівський нелюдь. Він пообіцяв своїм зазомбованим оркам, що в разі ядерної війни вони потраплять в рай як мученики, а решта «здохнуть». Визнання путіна абсолютним злом обґрунтовується не тільки тим, що він розгорнув активну підготовку до ядерної війни, але й вибудував та приводить у дію усю “вісь зла”. Згадаємо демарш Китаю стосовно Тайваня, що почався водночас з розгорненням широкомасштабного військового терору проти України. Приблизно у той час Північна Корея активізувала військові загрози своєму південному сусіду. Пізніше, коли росія почала втрачати остаточну надію на військовий успіх в Україні, Іран – (через свій проксі – ХАМАЗ) здійснив напад на Ізраїль і т.д. За всіма цими осередками займання третьої світової стоїть росія. Про чи не на повну схожість дій російських терористів і палестинських бойовиків говорять лідери ведучих західних країн, відомі закордонні аналітичні центри, наукові аналітики, військові експерти. Схожість як за своєю підступністю, звірячою жорстокістю, так і за виправданнями: “це не ми”, “це постановка” (повтор того, що російські терористи казали у Бучі), так і

в розповсюдженні постійної брехні (ХАМАС навмисно обманув світові ЗМІ, звинувативши Ізраїль у влучанні ракети у лікарню). Як ми зазначали, Москва спланувала і брала чи не головну участь у підготовці і забезпеченні проведення ХАМАСом 7 жовтня масованої атаки на Ізраїль. Йдеться про відключення електронних систем захисту на кордоні з Ізраїлем, виведення апаратури з ладу, блокування нормального її функціонування і т.д. Величезна роль росії як активного провокатора в організації масових заворушень, анти-ізраїльських протестних рухів по всьому світі, координації підготовки військових дій мусульманського світу проти Ізраїлю і США. Адже путін, незважаючи ні на що, продовжує судорожно чіплятися за владу, що вислизає за підсумками його війни. Створюючи вибухову ситуацію у світі, він дуже розраховував на розв'язання цивілізаційної війни Сходу із Заходом, відволікання останнього від допомоги Україні. Це дасть шанс на певний військовий успіх, а отже зробить омріяну путіним-вбивцею, міжнародним злочинцем перемогу на президентських виборах (на жаль, ця перемога буде зафіксована незалежно від підсумків голосування) більш правдоподібною. Доля людства воєнного злочинця путіна ніколи не хвилювала.

Такого роду інформацію про дійсний стан речей має бути, як зазначалось, доведено до кожної країни, до кожного жителя планети. Безумовно, це потребує величезних коштів (відповідні витрати на пропаганду вже десятки років несе росія), координації зусиль багатьох країн. Але це вкрай потрібно зробити. Адже тоді значно менше знадобиться витратити на зброю, втратити людей, відновлювати зруйноване і т.п.

Саме це призведе до декласування росії, забезпечить (як це не парадоксально), руйнацію світової "вісі зла", перемогу добра над злом.

Щодо побудови "Нового світового порядку". Діючий світовий порядок, а точніше, механізм його забезпечення аж ніяк не заважав (можна довести, що навпаки, сприяв) державі-терористу, державі-агресору вчиняти терор у міжнародному масштабі, а також захоплювати території інших держав. Тому в світі давно вже склалася думка про необхідність зміни існуючого

порядку і побудови нового. Але який це має бути порядок, як його побудувати – ніхто чітко і конкретно не говорить. Тому вважаємо за доцільне викласти відповідні наші судження, положення. Тим більше, що ці положення є частиною, складовою Концепції усунення російських загроз глобальній та регіональній безпеці.

Новий світовий порядок має координувати сумісні зусилля держав в двох вимірах – мирному (охорона навколишнього середовища, космос тощо), а також у військовому вимірах. Це забезпечення глобальної та регіональної безпеки, усунення терористичних і військових загроз (запобігання ним). Нас буде цікавити другий вимір. Щодо діючої системи боротьби з тероризмом. На рівні ООН вона включає “Глобальну контртерористичну стратегію” (ГКТС) та Контртерористичний центр (КТЦ) ООН. Цей центр, як зазначається у нормативних документах, сприяє розвитку міжнародного співробітництва у справі боротьби з тероризмом та надає підтримку державам-членам у здійсненні Глобальної контртерористичної стратегії. Однак, зазначена система, як і інші інституції ООН, абсолютно бюрократична, якщо казати дипломатично. Якщо ж говорити так, як воно є насправді, то вона не просто бюрократична, а вкрай шкідлива, оскільки і сам документ – ГКТС і механізми здійснення Стратегії – просто відволікають від дійсної боротьби з тероризмом. Да і поняття тероризму у згаданій Стратегії – допотопне. Таке враження що Стратегія асоціює тероризм з терористом-одинаком. Мабуть, у чалмі і з великою чорною бородою. А що таке державний тероризм, російський державний тероризм? Про це авторам Стратегії невідомо. Точніше, про росію відомо. Але тільки те, що її представники – очолюють КТЦ ООН (!). Тобто, терористи очолюють міжнародну боротьбу з тероризмом.

Виходячи з наведеного, немає сумніву, що новий світовий порядок, механізм його забезпечення має бути вибудований заново, з “чистого листа”. На наш погляд він має включати: I. Перелік злочинних діянь, які доцільно інтерпретувати як терористичні акти, злочини військового тероризму; II. Перелік санкцій за зазначені злочинні діяння; III. Механізми забезпечення виконання покарання.

I. Терористичні акти і злочини військового тероризму. ми ставимо на один рівень, оскільки всі вони суспільно небезпечні. Терористичні акти – це те, чим займалася росія принаймні, з моменту її виділення зі складу СРСР. Радянський тероризм – це окрема історія. Російський тероризм складає сутність, основний зміст російської державної політики, яка є політикою державного тероризму і знаходить свій прояв у найрізноманітніших формах. Так, готуючись до війни з Україною, з НАТО, росія не тільки нарощувала свою військову міць, але й нищила, терористичними методами, воєнний потенціал своїх можливих супротивників: підривала воєнні склади з боєприпасами в Україні, Чехії, Болгарії, насаджувала повсюдно, по всьому світові своїх провокаторів, шпигунів. Використовувались всі можливі і неможливі (ті, які за рівнем своєї підступності, цинічності, підлості нормальній людині, нормальній державі і не прийде в голову використати) засоби. Це вже і згадані підриви, в т.ч. на енергетичних об'єктах, захоплення заручників, і організація заворушень за кордоном, спрямованих проти діючої там влади, і кібернетичні атаки на критичну інфраструктуру країн, злами урядових сайтів інших країн, втручання у вибори у владу чи не у всіх державах світу, не кажучи вже про вбивства, отруєння іноземців і своїх громадян за кордоном. Це також масові підкупи політичних партій і урядовців за кордоном, міжнародних структур, ЗМІ, провокування мільйонних міграцій по всьому світу тощо. Широко використовується організація масових заворушень в чужих країнах і багато що інше. І все робиться задля впливу на населення і керівництво цих країн, примушення їх до дій, вигідних росії, до політичних поступок. Саме завдяки державі терористу, світ почав втрачати стабільність і безпеку, поринаючи в обстановку невизначеності та страху. І вся ця деструктивна діяльність держави агресора здійснювалася і здійснюється з метою реалізації нею своєї імперської, терористичної сутності.

Щодо злочинів військового тероризму. Будучи, за своєю суттю, терористичною державою, росія веде війну, яку характеризують як військовий тероризм (захоплення Чорнобильської атомної станції, ЗАЕС, знищення енергетичної інфраструктури, викрадання українських дітей, захоплення

цивільних заручників тощо). Юристи-правозахисники готують досє воєнних злочинів для подання до Міжнародного кримінального суду зі звинуваченням росії в навмисному спричиненні голоду під час війни проти України, використанні його як зброї. Окрім того, Парламентська асамблея Ради Європи підтвердила свою підтримку створенню спеціального міжнародного кримінального трибуналу «для притягнення до відповідальності російського керівництва, включаючи владіміра путіна», за їхні дії, починаючи з незаконної анексії Криму, війни на Донбасі та збиття літака рейсу МН17. Парламентська асамблея Ради Європи закликала держави-члени Ради визнати владіміра путіна нелегітимним після закінчення його нинішнього президентського терміну та оголосила росію диктатурою. Як відомо, в ухваленій одноголосно резолюції ПАРЕ також закликала припинити всі контакти з путіним, за винятком гуманітарних контактів і в прагненні до миру.

Пропонуючи криміналізувати зовнішню гібридно-терористичну діяльність держав, ми розробили проект (структуру і часткове наповнення) кодексу гібридно-терористичних і військових злочинів. Обов'язковим має стати невідкладне розслідування з наступним покаранням винних. При цьому особливу увагу ми пропонуємо приділити кримінальній відповідальності за “нові (для міжнародного кримінального права)” злочини. Наприклад, застосування голоду як зброї, викрадання дітей з окупованої території, захоплення міжнародно визнаних світовою спільнотою територій інших держав, розповсюдження брехливої інформації, що призвело до загибелі (масової загибелі) людей. Ця зброя знаходиться поза радарями, що дає змогу вести війну, відкидаючи всі звинувачення в тому, що відбувається. А це і є якраз тим, що іманентно московії. А саме: постійна і суцільна брехня, що завжди була і є сутністю державної політики як у внутрішньому, так і у зовнішньому вимірах.

Наголошуємо, що криміналізація гібридно-терористичної діяльності має бути нарешті, зроблена і не за довгі роки, як це звично відбувається у занадто вже неквапливому споглядально-мрійливому ритмі міжнародного життя, а на протязі декількох місяців (краще – тижнів). Такі ж терміни ми пропонуємо і для

проведення розслідування міжнародних гібридно-терористичних злочинів. Це і буде однією з складових нового світового порядку.

Окрім відповідальності за гібридно-терористичні діяння, держава-терорист, держава-агресор має бути покарана за розв'язання та ведення війни, а також скоєні воєнні злочини (і перш за все, сам диктатор). Це пропонується реалізувати (розробити та застосувати) в рамках другої складової нового світового правопорядку. Йдеться вже про наступний об'єкт міжнародно-правової відповідальності – гарячу, відкриту війну однієї країни проти другої. Ми виходимо з того, що війни – це абсолютно негативне, не допустиме явище, яке має не тільки категорично заборонятися, але й того (тих), хто вдасться до неї, слід суворо карати. Як за масове вбиваство, а це не менше як смертна кара. Але в нинішньому міжнародно-правовому просторі такого розуміння ще й не склалося, а отже і нічого в цьому плані не робиться. У 1928 році було укладено Договір про заборону війни як засобу національної політики (Пакт Бріана-Келлога), згідно з яким підписанти Договору всіляко засуджують застосування війни як засобу урегулювання міжнародних спорів і відмовляються у своїх взаємних відносинах від такого як знаряддя національної політики). Однак, як зазначалось, дієвого механізму примушення до незастосування війни немає. Такі органи як ООН (раніш Ліга націй), ОБСЄ, разом з відповідними міжнародно-правовими актами з не в змозі вирішити задачу забезпечення “миру у всьому світі”.

Особливу небезпеку людству несуть загарбницькі (колоніальні), спрямовані на повернення собі територій, які правитель країни-агресора вважав своїми), а також гібридні терористичні війни. Всі вони направлені на множення зла в світі, розпалювання ворожнечі, ненависті. До гібридних, терористичних війн слід відносити дії країни-агресора які полягають як у тотальному підкупі (з метою встановлення політичного контролю над країною, регіоном) політичних партій, їх лідерів, державних діячів), так у улаштуванні постійних провокацій, терористичних актів, вбивств, отруень. До гібридних, терористичних війн мають бути віднесені також

і фейки, налагодження пропагандистської брехні, що перевертає все з ніг на голову, створюючи величезний простір перевернутої (віртуальної) реальності. Всі зазначені дії становлять величезну загрозу для глобальної та регіональної безпеки. Саме за рахунок небаченої за масштабами і нечуваної, казкової за змістом дезінформації, брехні, яка поширюється в гігантських масштабах по всьому світові, росія, експлуатуючи свої історичні зв'язки з країнами Латинської Америки, Азії, Африки, вміло маніпулюючи своїми антиколоніальними та антизахідними настроями, створює залежність авторитарних режимів від російської зброї та грошей, аби залучати суспільство і політиків цих країн на свій бік. Як результат, росія одержує підтримку у населення низки країн, у голосуванні в ООН, в обході економічних санкцій, поповненні армії тролів у соцмережах тощо. Під впливом російського зомбування знаходяться країни «Глобального Півдня», де мешкають мільярди людей. Це також Латинська Америка та ін. Російська (а в свій час радянська) широкомасштабна пропаганда, міцно утвердила сильні антиамериканські настрої. Прикриваючись гаслами позбутися однополярності, впливу США на захист демократії та покінчити із "міжнародним хаосом", який нібито створює Америка, росія творить свої мерзенні злочини, тягне світ у прорву третьої світової.

Криміналізація гібридно-терористичної діяльності включає встановлення санкцій за відповідні діяння терористів, а також створення механізмів.

Волторніст Олександр Сергійович

*Навчально-науковий інститут міжнародних відносин,
Київський національний університет імені Тараса Шевченка,
м. Київ, Україна*

РОЗМИВАННЯ ТРАДИЦІЙНИХ ПАРАДИГМ БЕЗПЕКИ: ВИКЛИКИ СУЧАСНІЙ СИСТЕМІ МІЖНАРОДНОЇ БЕЗПЕКИ

Сучасна система міжнародної безпеки стикається з глибокою кризою, глибина якої резонує через традиційні рамки, які довгий час підтримували глобальну стабільність. Світ став свідком трансформації природи загроз, залучених учасників і засобів, через яких безпека ставиться під загрозу. Традиційна державоцентрична модель, яка колись була міцною у своїй простоті, виявляється все більш неадекватною у вирішенні багатогранних викликів, які виникли у 21 столітті.

Мета цього есе – заглибитися в кризу сучасної системи міжнародної безпеки. Ми будемо орієнтуватися на складній території глобальної безпеки, визнаючи зміну динаміки від державних конфліктів до більш складного спектру викликів. Це охоплює кіберзагрози, транснаціональний тероризм, зміну клімату та посилення ролі недержавних акторів на міжнародній арені. Це есе підкреслює необхідність еволюції в тому, як ми сприймаємо безпеку та підходимо до неї, наголошуючи на тому, що для подолання незахищеності сучасного світу потрібна більш цілісна та адаптована структура.

Коли ми перетинаємо ландшафт міжнародних відносин, що постійно змінюється, стає зрозумілим імператив: адаптуватися, переоцінити та шукати нові парадигми, які можуть більш ефективно захистити глобальний мир і процвітання. Розуміючи глибину кризи, ми краще готові прокласти курс на більш стійку та всеосяжну систему міжнародної безпеки.

Криза сучасної системи міжнародної безпеки

У недалекому минулому міжнародна система безпеки дотримувалася відносно стабільної структури, де національні

держави були головними акторами. Правила ведення бойових дій часто визначалися звичайною військовою силою, дипломатією та міжнародними угодами. Проте світ, у якому ми живемо сьогодні, відзначається швидко розвиваючим ландшафтом, де традиційна державно-орієнтована модель безпеки щосили намагається встигати за загрозами та викликами, що виникають.

Змінний ландшафт: мінлива природа загроз

Традиційна міжнародна система безпеки, визначена основоположними принципами міжнародного права (принцип державного суверенітету, принцип (юридичної) рівності держав, принцип невтручання однієї держави у справи іншої та принцип колективної безпеки), спиралася на суверенітет національних держав і військову силу як основу безпеки. Сьогодні визначення безпеки більше не обмежується військовими загрозами з боку інших держав. Навпаки, це охоплює складну мережу викликів. Яскравим прикладом є поява кіберзагроз. Зі збільшенням залежності від технологій і взаємозв'язку державні та недержавні суб'єкти тепер можуть запускати кібератаки, які потенційно можуть підірвати економіку, скомпрометувати критичну інфраструктуру та навіть вплинути на вибори. Повсюдне поширення цих цифрових загроз змусило країни переглянути свої стратегії безпеки (Hussain & Razali, 2020, С. 3).

Окрім кіберзагроз, тероризм набув транснаціональної форми. Недержавні актори, такі як Аль-Каїда та ІДІЛ, вийшли за рамки кордонів та ідеологій, що зробило традиційні державоцентричні заходи менш ефективними. Ця еволюція кидає виклик основним принципам суверенітету та територіальної цілісності (Calléja, 2021, С. 8).

Нові актори: недержавні та піддержавні актори

Однією з визначальних характеристик сучасної кризи безпеки є зростаюча роль недержавних і піддержавних акторів. Ці організації, починаючи від транснаціональних корпорацій і закінчуючи неурядовими організаціями, групами повстанців і злочинними мережами, безпрецедентно впливають на динаміку міжнародної безпеки. Наприклад, приватні військові компанії часто діють у зонах конфлікту, стираючи межу між державними та недержавними акторами. Вони надають різноманітні послуги

від логістики до бойової підтримки, сприяючи конфліктам складним і часто нерегульованим способом (Lüdert, 2023, С. 192).

Криза не обмежується загрозами безпеці, а поширюється на тих, хто прагне зберегти безпеку. Оскільки багато недержавних акторів беруть участь у гуманітарній діяльності та діяльності з розвитку, роль держав як виняткових постачальників суспільних благ ставиться під сумнів. У цьому зміненому ландшафті такі організації, як Організація Об'єднаних Націй та інші міжнародні організації, повинні адаптуватися та співпрацювати з різними недержавними суб'єктами для виконання своїх місій (Ide, 2016, С. 498).

Багатогранні виклики: зміна клімату та дефіцит ресурсів

Безпека більше не визначається лише військовими та геополітичними інтересами. Зміна клімату та дефіцит ресурсів є критичними проблемами з далекосяжними наслідками для безпеки. Наслідки зміни клімату, від підвищення рівня моря до екстремальних погодних явищ, можуть призвести до переміщення, конфліктів ресурсів і загострення існуючої напруги. Перед лицем цих екологічних викликів міжнародне співтовариство має переосмислити парадигми безпеки, спрямовані на усунення корінних причин цих загроз (Ide, 2016, С. 508).

Дефіцит ресурсів, будь то прісної води чи рідкісних мінералів, може спровокувати регіональні конфлікти та порушити глобальні ланцюги поставок. Щоб подолати ці виклики, держави повинні співпрацювати в питаннях управління ресурсами, пом'якшення наслідків клімату та охорони навколишнього середовища (Calléja, 2021, С. 11).

Виклики традиційній структурі

Криза сучасної системи міжнародної безпеки докорінно змінює те, як безпека сприймається, прагнеться та досягається. Вона ставить під сумнів принципи суверенітету, територіальної цілісності та невтручання у внутрішні справи держав. У взаємопов'язаному світі ці принципи повинні адаптуватися до змін глобального ландшафту.

Державоцентрична модель, яка колись слугувала наріжним каменем міжнародних відносин, повинна поступитися більш

комплексному, адаптивному та спільному підходу до безпеки. Розгляд багатогранної природи сучасних загроз потребує зміни парадигми. Це передбачає визнання цінності співпраці, зміцнення міжнародних інституцій та залучення недержавних акторів як невід'ємних компонентів системи глобальної безпеки.

Висновок. Криза сучасної системи міжнародної безпеки є відображенням динамічного та взаємопов'язаного характеру світу XXI століття. Виклики безпеці, з якими ми стикаємось сьогодні, більше не обмежені кордонами чи чітко визначені державоцентричними парадигмами. Натомість вони виникають із складної мережі транснаціональних, технологічних, екологічних і соціальних факторів. Вирішення цієї кризи потребує зміни в мисленні, яка наголошує на адаптивності, співпраці та цілісних стратегіях безпеки.

Коли ми орієнтуємося в цьому новому ландшафті безпеки, вкрай необхідно переглянути міжнародні норми, інститути та правові рамки. Держави повинні вийти за межі традиційної політики сили та визнати, що колективні дії та співпраця є ключовими для вирішення глобальних проблем, які загрожують миру та процвітання. Роблячи це, ми можемо працювати над більш стійкою, адаптивною та інклюзивною системою міжнародної безпеки, яка краще відповідає потребам нашого складного та взаємопов'язаного світу.

Література

Calléja, L. (2021). Transnational terrorism: a threat to global security. *Universidade Autónoma de Lisboa, 12, 1, 1-12.*

Hussain, A., Razali, S. (2020). A Review on Cybersecurity: Challenges & Emerging Threats. *NISS2020: Proceedings of the 3rd International Conference on Networking, Information Systems & Security, 28, 1-7.* URL: <https://doi.org/10.1145/3386723.3387847>

Calléja, L. (2021). Transnational terrorism: a threat to global security. *Universidade Autónoma de Lisboa, 12, 1, 1-12.*

Lüdert, J. (2023). *Non-State Actors at the United Nations Contesting Sovereignty.* Routledge.

Литвин Юліан Васильович

*Національний університет «Львівська політехніка»,
м. Львів, Україна*

Лакіза Вікторія Володимирівна

*кандидат економічних наук, доцент,
Національний університет «Львівська політехніка»,
м. Львів, Україна*

ORCID: 0009-0008-0552-8425

ВПЛИВ ЕКОНОМІЧНИХ КРИЗ НА МІЖНАРОДНУ БЕЗПЕКУ: ШЛЯХИ ЇХ ПОДОЛАННЯ

У наш час світ переживає непередбачувані коливання на фінансових ринках, які викликають різноманітні економічні виклики для країн усього світу. Економічні кризи не тільки загрожують стабільності окремих національних економік, але й мають значний вплив на міжнародну безпеку. Швидкі зміни у фінансових потоках, спад виробництва та безробіття можуть стати осередком негативних подій, що вражають політичну стабільність, соціальний клімат та міжнародні відносини. Саме тому особливої ваги набуває важливість розуміння впливу економічних криз на міжнародну безпеку, дослідження специфічних прикладів криз та їхніх наслідків, а також дослідження можливих шляхів подолання цих викликів. Важливим завданням сучасної політики є пошук балансу між економічною стійкістю та міжнародною безпекою, і тільки через ретельне вивчення цих питань можна знайти оптимальні рішення для стабільності та мирного співіснування у світі.

Насамперед варто розглянути причини виникнення економічних криз. Однією з основних причин економічних криз є недостатня регуляція фінансових ринків, а також недбале ставлення до ризиків. Фінансовий сектор може стати джерелом системних ризиків, коли банки та інші фінансові установи надмірно ризикують і, відповідно, ведуть непродуману політику

щодо залучення кредитних ресурсів. Це може зумовити створення «фінансових балонів», які в один момент можуть не витримати, та спричинити виникнення економічної кризи.

Ще однією причиною виникнення економічних криз є недостатня конкуренція та монополізація ринків. Великі корпорації можуть зловживати своїм становищем та створювати перешкоди для розвитку малих та середніх підприємств. Це, в свою чергу, може спричинити зниження інноваційності та ефективності економіки, та зрештою призвести до зростання безробіття й зниження рівня якості життя населення. Також важливо враховувати глобалізацію та вплив економічних криз в одній країні на інші. Зростання торговельних та фінансових зв'язків між країнами створює ризик поширення кризових явищ. Наприклад, криза в одній країні може призвести до зниження попиту на імпорتنі товари та послуги, що може негативно вплинути на економіку інших країн.

Як ми знаємо, економічні кризи можуть спричинити напруження в міжнародних відносинах. Одним з недавніх прикладів є глобальна фінансова криза, яка виникла в Сполучених Штатах, де вона прискорила економічну рецесію, яка почалася в грудні 2007 року (і закінчилася в червні 2009 року). Витоки кризи розглядаються, в основному, як поєднання краху на ринку житла, в результаті якого багато складних фінансових активів банків випарувалися, і слабкого регуляторного нагляду за банківською діяльністю та індустрією цінних паперів). Банки не бажали і не могли давати позики, тоді як корпорації збільшували свої грошові запаси, що призвело до занепаду економіки Сполучених Штатів і перекинулося на глобальну фінансову систему та світову економіку. Витоки кризи розглядаються, в основному, як поєднання краху на ринку житла, в результаті якого багато складних фінансових активів банків випарувалися, і слабкого регуляторного нагляду за банківською діяльністю та індустрією цінних паперів. Банки не бажали і не могли давати позики, тоді як корпорації збільшували свої грошові запаси, що призвело до занепаду економіки Сполучених Штатів і перекинулося на глобальну фінансову систему та світову економіку (Кінкейд, Тарр, Велті, 2010, С. 7). Саме дана криза

призвела до загострення глобальної економічної нестабільності та зниження здатності країн до втручання.

Тож, узагальнимо наслідки економічних криз для міжнародної безпеки. Насамперед, це збільшення політичних ризиків, адже економічні кризи створюють ідеальний ґрунт для політичних радикалів та екстремістів. Наприклад, під час економічної кризи в Греції радикальні партії здобули популярність, що в свою чергу вплинуло урядову стабільність. Також важливим наслідком економічних криз, які супроводжуються значними економічними проблемами, є збільшення кількості міжнародних конфліктів між країнами. Зокрема, конфлікт між росією та Україною має історію економічних суперечностей, які сприяли загостренню ситуації. Негативним наслідком економічних криз також є скорочення фінансування військово-оборонної промисловості, наслідком чого є зростання вразливості країн перед можливими зовнішніми загрозами.

Для подолання економічних криз необхідно вживати комплексних заходів. Тож, розгляньмо декілька основних шляхів подолання економічних криз:

1) активізування міжнародної співпраці: країни повинні співпрацювати для розв'язання глобальних економічних викликів, тому розробка спільних оборонних стратегій та надання фінансової підтримки може сприяти стабілізованню ситуації;

2) реформування внутрішніх економічних політик: країни повинні провести структурні реформи з тим, щоби поліпшити конкурентоспроможність та стимулювати економічний розвиток. Це може включати в себе податкові реформи, зменшення бюрократії та покращення інвестиційного клімату в цілому;

3) створення якісних передумов для розвитку людських ресурсів: збільшення інвестування в освіту та навички може покращити продуктивність праці та сприяти інноваціям, що є ключовими для стійкого економічного зростання.

4) заохочення інновацій та підприємництва: уряди країн мають створити сприятливі умови для розвитку інновацій у підприємницькій практиці, і це може включати в себе

надання фінансової підтримки дослідженням та розвитку нових технологій;

5) сприяння розширенню міжнародної торгівлі: збереження та розширення доступу до міжнародних ринків може допомогти стимулювати економічне зростання; ініціювання та укладання угод про вільну торгівлю та зниження тарифів можуть зробити світову торгівлю більш динамічною.

Отже, економічні кризи є важливими викликами для міжнародної безпеки, і саме тому вони потребують спільних зусиль з боку країн та міжнародних спільнот. Шляхи подолання цих криз включають в себе сприяння міжнародній співпраці, реформування внутрішніх економічних політик, розвиток людських ресурсів та зміцнення міжнародної фінансової та соціальної інфраструктури. Тільки за умови співпраці у напрямку реалізування цілеспрямованих антикризових заходів можна забезпечити стале економічне зростання та забезпечити міжнародну безпеку на довгострокову перспективу.

Література

Kincaid, J., Tarr, G. A., Wälti, S. (2010). *Federalism and the Global Financial Crisis: Impacts and Responses*. URL: <https://www.cairn.info/revue-l-europe-en-formation-2010-4-page-3.htm>

Швець Катерина Андріївна

Донецький національний університет імені Василя Стуса,

м. Вінниця, Україна

ORCID: 0000-0001-5272-3268

БЕЗПЕКА УКРАЇНИ В МІЖНАРОДНОМУ КОНТЕКСТІ СУЧАСНОСТІ

Ситуація у сфері безпеки, що складається під впливом складного динамічного процесу, в основі якого лежать глобалізація, науково-технічний прогрес, інформатизація супроводжується виникненням нових ризиків та загроз для формальних та неформальних акторів політики.

Водночас відбувається послаблення базових інститутів міжнародного регулювання, які виявляють недостатню ефективність у протидії сучасним викликам у сфері безпеки. Ключові позиції в наднаціональних та транснаціональних інституціях займають провідні держави світу, які здебільшого і домінують у глобальних економічних процесах та впливають на вирішення проблем міжнародної безпеки. Варто зазначити, що наразі відбувається посилення впливів транснаціональних корпорацій та фінансових груп на економічний і суспільно-політичний розвиток національних держав, що супроводжується зниженням ролі останніх у вирішенні широкого кола питань політики та безпеки на світовому, регіональному і національному рівнях. На тлі посилення взаємодії і взаємної залежності країн світу формуються нові «центри сили», конкуренція між якими за вплив та ресурси постійно зростає. Збільшується рівень відкритості міжнародної системи, що відкриває нові безпрецедентні можливості і водночас формує нові загрози та виклики безпеці на глобальному, регіональному та національному рівнях. Нагальною потребою стає створення більш гнучких систем безпекової взаємодії, здатних швидко й ефективно реагувати на нові виклики.

Нове розміщення й співвідношення політичних сил порушує баланс сил і інтересів у світі, змінює характер, масштаби й зміст

колишніх викликів, загроз та ризиків. Регіональні й локальні безпекові виклики дедалі більше глобалізуються, набуваючи все більш комплексного характеру. Процеси глобалізації перетворилися на найважливіший фактор впливу на безпекову та оборонну політику провідних країн світу на найближчу, середньострокову й довгострокову перспективу, що ставить перед Україною нагальне завдання визначити та оцінити характер і значущість сучасних викликів і загроз для її національної безпеки (Скалецький, 2021, С. 5).

Сучасна система європейської безпеки перебуває у стані випробування через загострення ситуації у світі. Специфіка безпекового середовища в Європі полягає в тому, що загроза виникнення тут (ред. у Європі) повномасштабного воєнного конфлікту оцінюється як низька, натомість сукупний ефект від дії новітніх загроз міг би мати руйнівні наслідки.

На сьогодні жодна з європейських країн не спроможна самостійно вирішувати стратегічні проблеми безпеки. НАТО, ЄС, ООН та ОБСЄ наділені виконувати роль ключових елементів в архітектурі європейської безпеки.

Як відомо, неодноразово в історії були спроби створення на універсальному рівні системи колективної безпеки. Перша із них пов'язана з появою Ліги Націй, яка протягом двох десятиліть намагалася вберегти світ від нових воєн, але не зуміла. Після Другої світової війни в 1945 р. була утворена Організація Об'єднаних Націй (далі – ООН), щоб «позбавити прийдешні покоління від лиха війни» і тим самим запобігти повторенню жахів світових воєн. Сьогодні публічні актори політики усвідомлюють, що в ООН немає політичної волі й економічного інтересу діяти відповідно до Статуту ООН. Вона немає ані прописаних процедур, які мають негайно застосовуватися, ані дієвих механізмів реалізації і це проблема не тільки ООН, ОБСЄ, а й багатьох інших міжнародних інституцій (Кінаш, 2022, С. 563). Серед низки сучасних науковців панує думка, що жодна міжнародна структура, включаючи ООН і ОБСЄ, більше не здатна у повній мірі попереджувати та зупиняти збройні конфлікти на планеті, а міжнародна система безпеки виявилася не спроможною виконати поставлені перед нею завдання.

Відповіддю на існуючі загрози міжнародній безпеці має бути цілеспрямована спільна діяльність міжнародних безпекових структур, країн і народів із усунення явищ, тенденцій і чинників, що унеможлиблюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей та здатні деформувати соціальне та природне середовища до стану, несумісного з існуванням. Держави, дбаючи про національну, а відтак і про міжнародну безпеку, мають неухильно дотримуватись вимог міжнародного права, особливо міжнародних принципів з питань заборони, обмеження та знищення окремих зразків засобів масового ураження. Відтак, слід звернути прискіпливу увагу на потребу осмислення тих проявів глобалізації, що радикально змінюють безпекову теорію та практику. Зокрема, принципово нового значення набувають основоположні ідеї безпекового мислення – національні цінності, національні інтереси, державний суверенітет, безпекові системи та інститути, безпекові гарантії тощо (Кінаш, 2022, С. 426).

Вбачаємо, що для подальшого безпекового статусу України необхідним є взаємозв'язок вступу до ЄС і НАТО, оскільки ці дві міжнародні організації взаємно доповнюють одна одну. Сьогодні очевидно, що Україна відіграє важливу роль у формуванні майбутнього безпекового ладу у світі. Адже нині, завдяки зусиллям України, війна, яку розгорнула Російська Федерація на нашій території, не перетворюється на загрозливу глобальну ситуацію. Україна набуває навичок та досвіду у військовій сфері, включаючи розвідку, розвиток кіберсфери та енергетику, якими може поділитися з іншими суб'єктами міжнародного права. Також ми вважаємо, що роль НАТО для євроатлантичної безпеки та в цілому для міжнародної залишається ключовою, а Україна довела, що може бути надійним союзником Альянсу (Скрипник, 2011, С. 212). Також слід відзначити, що подальші формати співробітництва України з НАТО повинні тривати не тільки у сфері постачання певних нових видів озброєння для захисту Україною свого державного суверенітету, а й повинна бути активна участь представників Альянсу у підготовці наших військових в питанні володіння сучасними видами озброєння.

Водночас Україна отримує багато переваг не лише в безпеково-оборонному, але й у соціально-економічному аспектах, що в умовах війни є надважливим. Також співробітництво з НАТО має сприяти швидшому вступу до Європейського Союзу, адже більшість держав ЄС водночас є членами Альянсу.

Підводячи підсумок, зазначимо, що нині ми стикаємось із найсерйознішими загрозами міжнародній безпеці: агресивні війни, насильство, можливість застосування ядерної, радіологічної, хімічної та біологічної зброї, тероризм. Ці міжнародні загрози перетинають національні кордони, вони взаємопов'язані і повинні усуватися на всіх рівнях: міжнародному, міжнародно-регіональному та національному. Саме тому, у сучасному контексті зростає визнання необхідності в розширеній концепції міжнародної безпеки та змістовно-функціональному реформуванні міжнародних безпекових структур.

Література

Кінаш, Н. Б. (2022). Міжнародна безпека як умова плюралістичної демократії. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття* (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права): у 2 т: матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.). Одеса: Видавничий дім «Гельветика», 425-427.

Кінаш, Н. Б. (2022). Міжнародна безпека як фактор формування національної безпеки України. *Юридичний науковий електронний журнал*, 9, 562-564.

Скалецький, Ю. М. (2021). *Проблеми впровадження культури безпеки в Україні*. Київ: НІСД.

Скрипник, О. М. (2011). *Історія міжнародних організацій*. Умань: ПП Жовтий О.О.

Фурсай Олександра Володимирівна

*Навчально-науковий інститут міжнародних відносин,
Київський національний університет імені Тараса Шевченка,
м. Київ, Україна*

ORCID: 0000-0003-1318-4550

«ВАКЦИНОДЕМІЯ» ЯК ЕЛЕМЕНТ СВІТОВОГО ГІБРИДНОГО ПРОТИСТОЯННЯ ДЕМОКРАТІЇ ТА АВТОКРАТІЇ

Широкомасштабне вторгнення російських військ в Україну в лютому 2022 року представляє собою лише чергову фазу великої російсько-української війни, яка триває вже дев'ятий рік. Наслідки цієї війни ми зможемо побачити на всій архітектурі майбутнього світопорядку. У період пандемії коронавірусної хвороби COVID-19 став яскравим прикладом світового зіткнення акторів міжнародних відносин, що впроваджують у суспільно-політичному житті своїх держав та реалізують у зовнішній політиці конфліктуючі ідеології – демократичне та авторитарне правління. Нинішні події в Україні, а саме відкрите військове вторгнення Росії, подальше загострення безпекової кризи перш за все в європейському регіоні є лише наступною фазовою ідеологічного протистояння, яке можна було спостерігати під час подолання людством пандемії COVID-19. Прояви інфодемії та її особливого формату – вакцинодемії – зафіксували суть глобального протистояння, що визначатиме міжнародні процеси на ближчі десятиліття. А саме: протистояння демократії та авторитаризму, який в Росії невдовзі оформиться як неототалітаризм. Їх протистояння визначатимуть, окрім решти суспільних явищ, структуру та зміст світового інформаційного простору.

Феномен «вакцинодемії» посилив дилему для урядів та суспільств нестійких держав: який режим правління обирати – авторитарний чи демократичний – для ефективного подолання соціальних, економічних та безпекових наслідків пандемії. Це є особливо критичним питанням для нестабільних транзитивних

демократій у Східній та Центральній Європі. Ми переконані, що навіть на тлі відкритої агресії Росії проти України, яка розпочалася 24 лютого 2022 року як новий етап російсько-української війни, інформаційне змагання у рамках пандемії COVID-19 слід розглядати як окремий акт модерного протистояння авторитарних і демократичних держав, їх випробуванням на ефективність, здатність до взаємодії, подолання вузьких національних інтересів на користь спільним потребам (спів)існування, загалом збереження та укріплення ідей та цінностей демократичного владарювання як найбільш доцільної для виживання нації та захисту державного суверенітету. Адже дискусія про те, що авторитарні чи навіть тоталітарні держави завдяки своїй внутрішній консолідації, здатності їх урядів до одноосібних швидких рішень, впливу на соціальні комунікації та втаємничення інформації, поліцейського примусу та державній пропаганді навіть за неефективної системи охорони здоров'я здатні сформувати у власного населення та симпатиків в інших державах стійку ілюзію, що недемократичний режим більш могутній та дієвіший у екстремальних ситуаціях. Ситуація з пандемією та її інформаційним відображенням – інфодемією, на наш погляд, дало авторитарним лідерам хибну уяву, що вони можуть також і у питаннях геополітики вдатися до нарощування та втілення своїх експансіоністських, неоімперіалістичних та шовіністичних намірів. Тому можна твердити, що керована пропагандистськими центрами істерія навколо COVID-19 (включаючи широкий міжнародний рух антивакцинологів, що є і в Конгресі США, і серед членів Європейського парламенту) підігрівала войовничі, загарбницькі настрої в Росії. А сама вакцинодемія стала зручним форматом для нового витка інформаційного протиборства, насадження великодержавної зверхності, нагнітання шовіністичних настроїв серед російського населення методами урядової пропаганди. Це підштовхувало, зокрема, авторитарний режим Путіна до воєнного вторгнення в Україну, а серед російського суспільства зміцнило його шовіністичні, українофобські настрої, що виливається сьогодні у підтримці росіянами так званої «спеціальної воєнної операції», а по суті – війни.

Коли міжнародні політологи-дослідники окреслюють табір держав з авторитарною формою правління, які складають опозицію до табору демократичного, то першочергово йдеться про Китай та Росію. Може твердити, що вакцинна дипломатія Пекіна та Москви активно поєднувалася з маніпуляцією та дезінформацією для того, щоб підірвати довіру до західної вакцини, інститутів ЄС і західноєвропейських стратегій вакцинації, що по суті є типовим феноменом вакцинодемії. За інформацію Європейської служби зовнішніх справ Росія і Китай використовували для цього контрольовані державою медіа і соціальні мережі, зокрема офіційні дипломатичні акаунти. До російської кампанії з просування вакцини Sputnik V були залучені державні органи, державні компанії та державні ЗМІ. Російські офіційні особи не тільки просували Sputnik V, а й використовували дезінформацію, щоб звинуватити Захід і ЄС в саботажі російської вакцини (EEAS SPECIAL REPORT UPDATE: Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic, 2021).

Прокремлівські ЗМІ, зокрема й офіційний акаунт Sputnik V в Twitter, намагалися підірвати довіру суспільства до Європейського агентства з лікарських засобів (ЕМА) – поставити під сумнів його процедури та політичну неупередженість тим самим прагнучи підірвати і фрагментувати загальноєвропейський підхід до забезпечення поставок вакцин. Повідомлення з контрольованих державою ЗМІ Росії в основному зосереджені на просуванні Sputnik V, наклепі на західні вакцини і звинуваченні ЄС в його невдалій вакцинації або боротьбі з COVID-19 (EEAS SPECIAL REPORT UPDATE: Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic, 2021).

Схожу картину – хаотизований, роз'єднаний «колективний Захід», бездіяльне НАТО, яке утримується від прямої сутички із Росією, яка прагне в Україні повернути, як вважають російські лідери, «історичну справедливість», – ці міркування також побудовані на оцінках досвіду боротьби західних країн проти наслідків коронавірусу. Як ми пам'ятаємо, той досвід був не надто вдалим, якщо аналізувати його через призму інформаційних,

особливо медійних повідомлень. Ми не можемо виключати того, що саме розгубленість демократичних держав у подоланні пандемічної кризи, певний «пандемічний націоналізм», декларований Дональдом Трампом на початку її розгортання, стали ще одним чинником, щоб В. Путін схвалив рішення про відкрите воєнне вторгнення в Україну.

Натомість російський уряд публічно культивував зверхність Росії, її технологічну та науково-технічну перевагу над рештою світу, що спонукало ріст мілітаристських та шовіністичних настроїв серед власного населення (Official website vaccine against coronavirus Sputnik). Такі заяви виглядали вкрай популістичними, оскільки за умов закритої Росії важко знайти підтвердження наявності у російської фармацевтичної індустрії, технологічно залежної від західного постачання, таких потужностей, щоб забезпечити і себе, і своїх партнерів обіщаним препаратом.

Натомість у західних урядів виникли підозри, що Кремль використовує повідомлення про створення Sputnik V як новий привід для пропагандистської атаки. Так, уряд Франції звинуватив Росію в поширенні разом із вакциною своєї «пропаганди та агресивної дипломатії» (AFP News Agency on Twitter, 2021). Емманюель Макрон зазначив, що через пандемію коронавірусу і спроби Росії та Китаю політично вплинути на постачання вакцин, європейські країни опинилися на порозі світової війни нового типу (Franceinfo, 2021).

Не дивлячись на відмову Європейського Союзу використовувати російську вакцину, Угорщина стала однією з перших країн ЄС, яка почала використовувати Sputnik V. Прем'єр-міністр Угорщини Віктор Орбан прокоментував дане рішення наступним чином: *«Немає західної чи східної вакцини, є лише погана та хороша»*. Та підкреслив, що наразі ЄС неспроможний задовольнити своїх громадян необхідною кількістю вакцини (T. Öztürk, Anadolu Ajansı 2021).

Загалом, вакцина Sputnik V так і не була поширена в Європі, але інформаційного галасу та поширення проросійських настроїв вона досягла. У Словаччині закупівля російської вакцини спричинила в країні політичну кризу. Події навколо закупки Sputnik V призвели до гучних звільнень і

політичної кризи у Словаччині (Укрінформ. Мультимедійна платформа іномовлення України, 2021). Міністр закордонних справ Іван Корчок навіть заявив, що вакцина Sputnik V є інструментом гібридної війни, яка роз'єднує країну (І. Сітнікова, Громадське телебачення України, 2021). Використання російської вакцини могло поставити європейські країни в залежність від Кремля, як це відбулося з постачанням енергоносіїв, та стати в очах виборців проявом підтримки російської політики. Це є ще одним підтвердженням тому, що будь-яка загально людська проблема – чи то пандемія 2020 року, чи міграційна криза в Європі 2015 року, чи кліматичні зміни – ставали інструментом агресивного впливу російської авторитарної держави, які були орієнтовані на руйнування єдності демократичного світу, підбив його цінностей та підготовку до відкритого силового перегляду світового порядку, руйнування безпекових стабілізаторів.

Глава уряду Литви Інгрида Шимоніте зазначала у своєму Twitter, що *В. Путін не хоче використовувати Sputnik V як ліки для російського народу. Він пропонує її світові як ще одну гібридну зброю для втілення принципу «розділяй і владарюй»* (І. Šimonytė, Twitter, 2021).

Література

About Sputnik V, Sputnik V. Official website vaccine against coronavirus Sputnik. URL: <https://sputnikvaccine.com/about-vaccine/>

BREAKING France slams Russia's Sputnik V vaccine as tool of 'propaganda and aggressive diplomacy (2021). *AFP News Agency on Twitter*. URL: <https://twitter.com/AFP/status/1375364153133662209>

Covid-19: the vaccine, a new issue of power on a global scale [Covid-19 : le vaccin, un nouvel enjeu de pouvoir à l'échelle Mondiale] (2021). *Franceinfo*. URL: https://www.francetvinfo.fr/sante/maladie/coronavirus/vaccin/covid-19-le-vaccin-un-nouvel-enjeu-de-pouvoir-a-l-echelle-mondiale_4348763.html

Šimonytė, I. (2021). [They say, Sputnik V is good but Putin doesn't care to use it as a cure for the Russian people – he offers it to the world as another hybrid weapon to divide and rule. This is neither news nor good...]. *Twitter*. URL: <https://twitter.com/IngridaSimonyte/status/1357767922106720258>

Сітнікова, І. (2021). У Словаччині вже шість міністрів подали у відставку: через закупівлю «Спутника V» у країні виникла політична криза. *Громадське телебачення України*. URL: <https://hromadske.ua/posts/u-slovachchini-vzhe-shist-ministriv-podali-u-vidstavku-cherez-zakupivlyu-sputnika-v-u-krayini-rozgorilas-politichna-kriza>

Read EEAS Special Report Update Short Assessment of Narratives and Disinformation around the COVID-19/Coronavirus Pandemic (Update December 2020 – April 2021). *EEAS Website*. URL: <https://euvsdisinfo.eu/uploads/2021/04/EEAS-Special-Report-Covid-19-vaccine-related-disinformation-6.pdf>

Прем'єр Словаччини подав у відставку через скандал із російською вакциною (2021). *Укрінформ. Мультимедійна платформа іномовлення України*. URL: <https://www.ukrinform.ua/rubric-world/3218168-premer-slovaccini-podav-u-vidstavku-cerez-skandal-iz-rosijskou-vakcinou.html>

Öztürk, T. (2021). Hungary premier: No East, West vaccines, only good, bad. *Anadolu Ajansı*. URL: <https://www.aa.com.tr/en/europe/hungary-premier-no-east-west-vaccines-only-good-bad/2154649>

Прищеп Роман Павлович

*Донецький національний університет імені Василя Стуса,
м. Вінниця, Україна*

REALPOLITIK ЯК ПРАКТИКА ЕКОНОМІЧНОГО ТИСКУ

Інтернет-енциклопедія трактує реальну політику як підхід до проведення дипломатичної чи політичної політики, що ґрунтується переважно на розгляді певних обставин і факторів, а не на суворому дотриманні явних ідеологічних понять або морально-етичних передумов. У цьому відношенні вона поділяє аспекти свого філософського підходу з аспектами реалізму та прагматизму. Її часто називають прагматизмом у політиці, наприклад, «проведення прагматичної політики» або «реалістичної політики».

До відомих прихильників Realpolitik у 20-му столітті належать Генрі Кіссінджер, Джордж Ф. Кеннан, Збігнев Бжезінський і Ганс-Дітріх Геншер, а також такі політики, як Шарль де Голль і Лі Куан Ю.

Наскільки реальна політика впливає на офіційну політику країн в умовах широкомасштабної війни Росії в Україні, було проведення дослідження двох голосувань країн в ООН стосовно українського питання. Перше голосування відбулося 12 жовтня 2022 року за резолюцію під назвою «Територіальна цілісність України: захист принципів Статуту ООН», де мова йшла щодо ставлення до збереження єдиної території незалежної країни. Друге голосування було проведено 16 листопада 2022 року. В ньому піднімалося питання стосовно збереження прав людини на одній з окупованих територій України, автономної республіки Крим. Здавалося б, ці дві резолюції тісно пов'язані між собою: якщо країна вважає неприпустимим окупацію території, то і права людини, яка проживає на окупованій території порушуються. Оскільки громадяни вимушені знаходитися під окупаційним режимом, в умовах утисків та переслідувань. З точки зору послідовності логіки, якщо територіальна цілісність України

порушена, то права людей, які проживають на окупованій території України, теж порушені. Оскільки вони змушені через зовнішній військовий тиск жити за правилами російської окупаційної влади. Тому голосування по двом питанням має бути логічним.

Проте, під час аналізу було встановлено, що якщо по першому голосуванню 143 із 193 країн-членів підтримали резолюцію територіальної цілісності України, то по другому голосуванню стосовно порушення прав людини на окупованій території 54 країни з 143 країн утримались. Спроби з'ясувати, що стало причиною непослідовної політики голосування в ООН, призвели до певних результатів. Було з'ясовано, що більшість із країн, що утримались щодо питання підтримки захисту прав людини на окупованій території АР Крим – це африканські республіки. Напередодні голосування у них відбулися певні дипломатичні та недипломатичні зв'язки з представниками російської дипломатії та лідерів, про що є інформація у відкритих російських джерелах, які були проаналізовані. Наприклад, 31 жовтня 2022 р., одразу після першого голосування в ООН, Росія направила до Лівії представників для поновлення роботи посольства (Коммерсант). А Єгипет, Кенія та Туніс за підписаними економічними договорами з Росією стали найбільшими імпортерами російської пшениці (Интерфакс). Гана, Нігерія, Руанда та Замбія вже чекають від російської держкорпорації «Росатом» затвердження будівництва на своїх територіях атомних електростанцій. А в Єгипті будівництво АЕС вже триває (The Insider).

Для африканського регіону вторгнення Росії в Україну поставило низку країн у незручне дипломатичне становище перед Європейськими країнами, з якими були тісні економічні стосунки. Схожа ситуація і для країн Південно-Східної Азії та Середнього Сходу, островів Океанії, країн Південної Америки та Карибського басейну, а також двох європейських держав – Сербії та Угорщини.

Наприклад, такі країни як Бангладеш, Оман, Саудівська Аравія, Ємен стали найбільшими імпортерами російської пшениці за бюджетною ціною у межах власної економіки

(Интерфакс). А Гана, Нігерія, Руанда та Замбія домовилися про будівництво атомних електростанцій за рахунок російського рубля. Досвід Бангладешу, який уже реалізував такий проект спільно з РФ, став для цих країн прикладом угоди.

Таким чином, питання економічного співробітництва стало основним механізмом впливу на прийняття нейтрального рішення в ООН стосовно резолюції прав людини на окупованій території АР Крим.

Другий напрям російського контролю над голосуванням резолюції в ООН від 16 листопада 2022 р. щодо прав людини в АР Крим, це розвиток туризму. Для цього було спеціально запущено російську платіжну систему «Мир» на території Єгипту. До цієї ініціативи приєдналися також Маврикій та Нігерія (Ведомости, 2022.13.10). Країни, які прагнуть розвинути туризм задля поповнення свого держбюджету в азіатському регіоні також вже запускають російську платіжну систему «Мир». До них відносяться Індонезія, Малайзія та Мальдіви (Tourdom.ru; Финтолк). Ще низка країн заради розвитку власного національного туризму дозволили російським авіакомпаніям відкрити прямі рейси на свої території. Це стосується Єгипту, Маврикія та Оману (Турпром; Profi+Travel; Асоціація Туроператоров).

Традиційна нафтова тематика, яка використовувалася до недавнього часу з Україною, активно застосовується зараз в зовнішній політиці Росії з африканськими країнами з метою тиску на їхнє політичне рішення. Також Росія має багато партнерів, з якими її пов'язує продаж або видобуток нафти. Серед них Єгипет, Ірак і Саудівська Аравія (Ведомости, 2022.16.11; ТЭКНОБЛОГ; DW).

Проведене дослідження показало, що реальна політика, яка ґрунтується на економічних національних інтересах, має вплив на зовнішньополітичну офіційну політику. І, не зважаючи на економічні санкції та публічне засудження європейськими країнами агресії на територію України, Росія продовжує відігравати значну роль у міжнародних рішеннях та здійснювати вплив на механізм прийняття рішень через економічний тиск на країни.

Література

В продаже туроператоров появились туры в Оман на прямых рейсах (2022). *Ассоциация Туроператоров*. URL: <https://www.atorus.ru/node/50206>

Остров Маврикий может начать принимать карты «Мир» (2022). *Ведомости*. URL: <https://www.vedomosti.ru/finance/news/2022/10/13/945386-ostrov-mavrikkii-mozhet-nachat-prinimat-karti-mir>

Россия возобновила поставки нефти в Египет, ОАЭ и на Кубу (2022). *Ведомости*. URL: <https://www.vedomosti.ru/business/articles/2022/11/16/950513-rossiya-vozobnovila-postavki-nefti-v-egipet-oe-i-na-kubu>

Россия в октябре увеличила отгрузку пшеницы на экспорт на 47% (2022). *Интерфакс*. URL: <https://www.interfax.ru/business/870372>

Россия направила в Ливию представителей для возобновления работы посольства (2022). *Коммерсант*. URL: <https://www.kommersant.ru/doc/5645239>

Опубликован список стран, куда российские туристы могут улететь прямыми рейсам: цены сильно упали (2022). *Турпром*. URL: <https://www.tourprom.ru/news/57638/>

Ирак хочет расширения участия компаний РФ в добыче нефти (2022). *ТЭКНОБЛОГ*. URL: <https://teknoblog.ru/2022/10/21/119641>

Топ-8 стран, где работают карты «Мир» (2022). *Финтолк*. URL: <https://fintolk.pro/top-8-stran-gde-rabotayut-karty-mir-osenyu-2022-goda/>

Байден разочарован. Саудовская Аравия играет на руку Кремлю? (2022). *DW*. URL: <https://www.dw.com/ru/razocarovanie-bajdena-saudovskaa-aravia-igraet-na-ruku-kremlu/a-63418912>

Прямые перелеты на Маврикий могут пошатнуть монополию Emirates (2022). *Profi+Travel*. URL: <https://profi.travel/news/56160/details>

Росатомное оружие. Как Россия использует свои АЭС за рубежом для шантажа и давления (2022). *The Insider*. URL: <https://theins.ru/ekonomika/254301>

Карты «Мир» могут заработать и в Малайзии (2022). *Tourdom.ru*. URL: <https://www.tourdom.ru/news/karty-mir-mogut-zarabotat-i-v-malayzii.html>

Из Екатеринбурга запустят авиарейсы к популярным курортам (2022). *URA.RU*. URL: <https://ura.news/news/1052599114>

РЕГІОНАЛЬНА БЕЗПЕКА В НОВИХ ГЕОПОЛІТИЧНИХ КОНЦЕПЦІЯХ

Бусленко Василь Володимирович

доктор політичних наук, доцент,

Волинський національний університет імені Лесі Українки,

м. Луцьк

ORCID: 0000-0001-8280-7104

УКРАЇНА В БЕЗПЕКОВІЙ ПОЛІТИЦІ РЕСПУБЛІКИ ПОЛЬЩА

Україна займає особливе місце в безпековій політиці Польщі в силу геополітичного становища, тісної економічної, політичної, культурної співпраці. Між двома державами існує довготривале стратегічне партнерство. Геостратегічне значення Польщі та України переконливо свідчить на користь формування в регіоні Середньої Європи тандему регіональних лідерів здатних до протистояння викликам та загрозам міжнародному порядку, який перебуває на етапі суперечливих та неоднозначних змін. В стосунках Польщі та України чітко вирізняється вимірна спільна ціль та стратегічний інтерес (Рапорт, 2021, С. 12). Це є відправною точкою для прийняття спільних узгоджених політичних рішень на базовому рівні.

В той же час партнерство України та Польщі реалізується в складних умовах багатьох асиметрій. Україна функціонує в «сірій зоні» безпеки між росією та євроатлантичними структурами інтеграції та безпеки, до яких належить Польща. Сама Україна не має чітких гарантій безпеки, на відміну від Польщі. Тому залишається більш вразливою до проявів проєкції сили з боку росії. Цій меті слугує тиск з використанням гібридних ресурсів, демонстрації військової сили, дезінформаційних заходів, у яких значну роль відіграє т. зв. історична політика. По-друге, істотним

наслідком функціонування в «сірій зоні» безпеки є асиметрія інституційних зв'язків Польщі та України, що означає членство в різних регіональних та субрегіональних організаціях (Рапорт, 2021, С. 17).

Виклики та загрози для Центральної та Східної безпеки і зокрема агресивна політика росії детермінує розвиток та динаміку відносин між Польщею та Україною в сфері питань забезпечення безпеки як на національному, так і регіональному рівнях. Загалом, безпекова політика Польщі стосовно України знайшла своє відображення у досить ґрунтовних концептуальних документах Польщі – Стратегії державної безпеки та Стратегії оборони. У них досить широко визначаються межі військово-політичної активності: регіон довкола Польщі, Європа та Євроатлантичний регіон. Польща вважає себе безпечною державою, а як основні розглядає внутрішні ризики. Можливість великомасштабної агресії проти Польщі до 2023 р. оцінювалася як малоімовірна. Більша увага приділялася виникненню регіональних та місцевих конфліктів. Присутність США в Європі, членство Польщі в НАТО і ЄС, демократизація України розглядалися Польщею як основний інструмент гарантування власної безпеки.

Польща також зацікавлена у входженні України до НАТО. Вона розглядає Центральноєвропейський регіон як цілісний з точки зору системи безпеки і виступає за розбудову системи (мережі) зв'язків у Центральній Європі в рамках ЄС та НАТО, а також понад їхніми кордонами. Принципи «відкритих дверей» в свою чергу, відображає національні інтереси України, яка прагне увійти в цей військовий союз.

З іншого боку, дії РФ до 2014 р. розглядалися Польщею як спроби порушити європейську співдружність. Держава припускала застосування збройних сил усередині держави, зокрема військ спеціального призначення, лише для надання допомоги органам державної влади, державної адміністрації та громадськості.

Безпекова політика Польщі стосовно України частково відображена в програмі Європейського Союзу «Східне партнерство», ініційованій Польщею та Швецією й затвердженій

ЄС у 2008 р. Більшість аналітиків сходяться на думці, що основним стимулом для Польщі в рамках «Східного партнерства» є залучення ресурсів ЄС, передусім фінансових, для вирішення завдань східної політики Польщі.

В умовах глобальних взаємозалежностей та спільних загроз з боку росії, для двосторонніх відносин між Польщею та Україною істотно зростала важливість змін, які відбувалися на Сході України як потенційного чинника глобальної міжнародної системи.

Нова геополітична реальність зумовлена гібридною війною росії проти України в 2014 р. внесла суттєві корективи в безпекову політику Польщі. З того часу питання національної безпеки стало відігравати домінуючу роль у порядку денному двосторонніх відносин. Прогнозуючи довгострокові агресивні кроки Кремля сторони розуміли важливість надійної, стабільної та передбачуваної співпраці. У 2008 році питання м'якої безпеки здавалися першочерговими, і нормативна сила ЄС була найкращим інструментом для їх врегулювання. Як реакція на нову політичну реальність стало затвердження Президентом Польщі Б. Комаровським 5 листопада 2014 р. нової Стратегії державної безпеки Польщі (*Strategię Bezpieczeństwa Narodowego RP*). Її реалізація стала продовженням політики активної участі ЄС у справах безпеки Східної Європи. Стабільним залишався курс на реалізацію рішень НАТО. Скажімо на саміті НАТО, який проходив у Варшаві в 2016 році було погоджено надання Україні комплексного пакету допомоги. На думку А. Легуцької польська політика безпеки сконцентрована на зміцненні НАТО як фундаменту оборони польської держави (Легуцька, 2019, С. 206). На цьому ж саміті країни Альянсу вирішили розмістити багатонаціональні батальйони НАТО у Польщі, Естонії, Латвії та Литві.

12 травня 2020 р. президент Польщі А. Дуда затвердив нову Стратегію державної безпеки. В документі чіткіше окреслено середовище безпеки. Зазначено, що найсерйознішою загрозою є неоімперіалістична політика влади Російської Федерації, яка реалізується із застосуванням військової сили. Підкреслено, що незаконна анексія Криму та дії на сході України порушили фундаментальні принципи міжнародного права і підірвали

основи європейської безпеки (Собчак, 2020, С. 7]. Було відзначено, що Російська Федерація розширює свої наступальні військові можливості, проводить масштабні військові навчання за сценаріями, що передбачають конфлікт з країнами Північноатлантичного альянсу, а також гібридні дії нижче порогу війни, що несуть ризик конфлікту, вживає комплексні дії невійськовими засобами, включаючи кібератаки та дезінформацію – прагнучи відновити свою силову позицію та сфери впливу.

Широкомасштабне вторгнення росії в Україну, що розпочалося 23 лютого 2022 р. призвело до переосмислення ситуації та оцінки агресивної політики Росії з точки зору загроз європейській безпеці. При цьому Україна стала відігравати ключового гравця від якого залежали сама безпека. Зміни на рівні глобальної міжнародної системи вимагали постійної діагностики та оцінки їх впливу на геополітичний простір Польщі та України, визначення інтересів та формування спільних стратегій. В цьому плані позитивним став політичний діалог між Україною та Польщею, який вівся, насамперед на рівні лідерів держав, установ виконавчої влади, на парламентському рівні.

Напад росії на Україну спричинив широку реакцію міжнародного співтовариства, покликану не лише ізолювати а й покарати державу в дипломатичній, економічній, та правових царинах. 14 грудня 2022 р. польський Сейм визнав Російську Федерацію як державу, яка підтримує тероризм і використовує терористичні засоби. Як стверджується в документі росія «систематично порушує права людини, міжнародне право та Статут Організації Об'єднаних Націй та ряд інших зобов'язань», «нападає на території інших країн, вчиняє збройні напади, військові злочини та геноциди» та «здійснює ворожі економічні дії, зокрема у сфері енергетики» (Сейм, 2022). Резолюція про визнання росії державою-спонсором тероризму була ухвалена більшістю у 231 голос, водночас 226 депутатів, включно з опозицією, участі в голосуванні не брали.

Співпраця України та Польщі в галузі безпеки спрямована на сучасність та майбутнє. Проте характер взаємовідносин між державами залежав і від сприйняття минулого з його складними суперечливими процесами. В той же час між українськими та

польськими політиками, істориками, державними діячами росло розуміння, що політизація т.зв. «чутливих» тем в умовах війни може бути використано росією як інструмент маніпуляцій з метою послаблення співпраці між державами, особливо в воєнній сфері. Тому на основних дискусійних майданчиках тема війни набувала більшої значимості і ваги, ніж складні питання спільної історії.

Відмітимо, що серед лідерів Польщі, Чехії, Словаччини існує косолідований підхід щодо гарантій безпеки України. Зокрема, у статті прем'єр-міністрів вищезазначених держав М. Моравецького, П. Фіали, Е. Гегера у журналі *Foreign Affairs* зазначено, що «впродовж багатьох років Кремль систематично підриває міжнародну стабільність і безпеку, порушуючи міжнародне право, застосовуючи силу або погрожуючи її застосуванням, а також підриваючи демократичні інститути за допомогою політичної та гібридної війни» (Фіала, 2023).

Таким чином, фундаментальним фактором, який формує безпеку Польщі, є її міцна інтеграція в трансатлантичні та європейські структури, а також розвиток двостороннього та регіонального співробітництва з ключовими партнерами, серед яких Україна. В цьому контексті значна увага приділяється заходам для зміцнення незалежності, суверенітету та територіальної цілісності України та підтримці їх прагнень до європейської та євроатлантичної інтеграції.

Широкомасштабне вторгнення Росії в Україну не призвело в Польщі до ухвалення якихось операційно-тактичних документів, свого роду «дорожньої карти», яка б відображала підходи в реалізації стратегічного партнерства в нових умовах. Натомість в залежності від перебігу політичних подій на законодавчому рівні було прийняття ряд документів, які в подальшому визначали напрямки стратегічної співпраці між державами.

Польща залишається головним логістичним хабом для міжнародної підтримки України в боротьбі з росією. Її роль у підтримці України є вирішальною. Партнерство між Польщею та Україною має симетричний характер і залежить у значній мірі від ініціатив України, спрямованих на забезпечення власної

безпеки а відтак і безпеки в регіоні. Йдеться про ініціативи України щодо необхідності надання їй військової допомоги.

Література

Fiala, P., Heger, E., Morawiecki, M. (2023, April, 24). The Free World Must Stay the Course on Ukraine. *Foreign Affairs*. URL: https://www.foreignaffairs.com/ukraine/free-world-must-stay-course-ukraine?gad=1&gclid=CjwKCAjwge2iBhBBEiwAfXDDBR_J6CKOTDfAfdq_ujuJpJnRsm8pNOEKIapsgy_NfP_gb_EzhliuGxoCzAsQAvD_BwE.

Legucka, A. (2019). Polityka zagraniczna Polski wobec Rosji po aneksji Krymu. *Wschód Europy. Studia humanistyczno-społeczne*, 5(1), 203–215. URL: <https://journals.umcs.pl/we/article/view/10174>.

Raport. Stan i perspektywy partnerstwa strategicznego Polski i Ukrainy. Punkt widzenia Polski i Ukrainy (2021). Lublin-Kijów. URL: <https://phavi.umcs.pl/at/attachments/2022/0110/115948-stan-i-perspektywy-partnerstwa-pl-web.pdf>.

Sejm uznał Rosję za państwo wspierające terroryzm (2022, Grudzień 14). *Sejm Rzeczypospolitej Polskiej*. URL: <https://www.sejm.gov.pl/>.

Sobczak, J. (2020). Nowa strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej. *Cybersecurity and Law*, 4(2), 7–36.

Стець Андрій Михайлович
кандидат юридичних наук,
Зеленогурський університет, м. Зелена Гура, Польща
ORCID: 0000-0002-3014-2400

БЕЗПЕКА ПОЛЬЩІ ТА УКРАЇНИ

У сучасному світі, що глобалізується, проблеми безпеки стають дедалі складнішими. Участь Польщі в Європейському Союзі та НАТО та шлях вступу України до цих інституцій недостатні для забезпечення безпеки громадян. Традиційні моделі безпеки постійно випробовуються новими та розвиваючими загрозами, про що яскраво свідчить війна Російської Федерації проти України, спрямована на винищення української нації.

Традиційно сприймана безпека громадян, як діяльність органів державної влади, спрямована на протидію загрозам громадському порядку, життю, здоров'ю та власності громадян, а також припиненню та відсічі будь-яким діям, що завдають шкоди цим благам, незалежно від того, чи надходять вони ззовні, з-за меж Польщі чи зсередини країни, здається занадто вузько зрозумілим. Нині їх слід розуміти ширше, включаючи сферу екологічної та енергетичної безпеки (Banaszak, 2012). Сюди ж слід додати політичну безпеку у вигляді впливу сусідніх країн на результати демократичних виборів через корупцію та інформаційні маніпуляції (Kowalska-Chrzanowska, Krysiński, 2023).

У цьому контексті аналіз кризи системи міжнародної безпеки, проблеми фейкових новин та гібридної війни стає ключовим для розуміння сьогоdnішніх реалій міжнародної безпеки як для України, яка бореться за своє існування, так і для Польщі, яка все більше атакована російськими кіберзлочинцями (Jurczak, 2023).

Порушення традиційних міжнародних норм:

Криза міжнародної системи безпеки, фейкові новини та гібридна війна є порушенням традиційних міжнародних норм. Перед обличчям цих викликів спільнота Центральної та Східної Європи має переглянути свій підхід до безпеки, інтегруючи

аспекти кібербезпеки, боротьби з дезінформацією та сучасними конфліктами в міжнародні стратегії безпеки. Це передбачає необхідність реформування Організації з безпеки та співробітництва в Європі, особливо ефективності т.зв. людського виміру ОБСЄ, яку поширює польська дипломатія. Буде потрібно відновити економіку, забезпечити енергію (ОБСЄ як форум для обміну досвідом) і підтримати захист груп, які особливо постраждали від конфліктів і війни (Kulesa, 2023).

Fake news як зброя сучасних конфліктів:

Фейкові новини стали широко використовуваним інструментом у сучасних конфліктах, впливаючи на політичні, соціальні та економічні процеси в країнах. Аналіз механізмів розповсюдження та впливу фейкових новин дозволяє виявити ключові зони, сприйнятливі до дезінформації, та розробити ефективні стратегії протидії цьому явищу.

Необхідність міжнародного співробітництва та інновацій:

Ефективна протидія кризі системи міжнародної безпеки, фейковим новинам та гібридній війні потребує комплексних дій держав, міжнародних організацій та приватного сектору. Запровадження інноваційних технологічних рішень, просування медіаосвіти та зміцнення міжнародного співробітництва є основними елементами формування стійкості суспільств і держав до сучасних загроз, зокрема корупції.

У сучасному глобалізованому світі виклики безпеці стають складнішими. Традиційні моделі безпеки постійно випробовуються новими загрозами, що розвиваються. У цьому контексті аналіз кризи системи міжнародної безпеки, проблеми фейкових новин та гібридної війни стає ключовим для розуміння сьогоденних реалій міжнародної безпеки. Слід також зазначити, що нові конфлікти та війни починають відволікати увагу міжнародної спільноти від війни, яка йде в Європі і від результату якої залежить мир у нашому регіоні. Прикладом може бути війна в Сирії в 2011 році, яка почалася з антиурядового повстання. Її причиною стало авторитарне правління Башара Асада. Натхненням для сирійців взятися за зброю стали успішні революції в Тунісі, Єгипті та громадянська війна в Лівії (так звана Арабська весна). Час від часу цю війну підбурюють російські

найманці, щоб відвернути увагу від повномасштабної війни Росії проти України під приводом ворожнечі між сунітами та шиїтами (Rosyjski generał ujawnił).

Війна ХАМАС-у проти Ізраїлю набуває такого ж значення, оскільки вона вирішить майбутнє Близького Сходу і навіть глобальний баланс сил. Його ініціювання може відвернути увагу від України і водночас спонукати китайські війська напасти Тайвань, оскільки Сполученим Штатам буде важко надавати допомогу на трьох фронтах. Окрім військової боротьби, найближчим часом особливе значення матиме фронт інформаційної боротьби (Sokala, 2023).

I. Криза системи міжнародної безпеки:

Криза системи міжнародної безпеки характеризується порушенням традиційних міжнародних норм і принципів, зростанням регіональних конфліктів та відсутністю ефективних механізмів врегулювання криз. Аналіз цієї кризи дозволяє визначити ключові сфери невизначеності та дестабілізації, у ситуації, коли ООН повинна реагувати рішуче.

II. Fakenews як загроза міжнародній безпеці:

В часі глобального інтернету та соціальних мереж неправдиві інформації (фейкові новини) становить серйозну загрозу для суспільств та країн. Типовим прикладом може бути інформація про нібито провокації НАТО, які загрожують Росії, або про те, що санкції ЄС і США, запроваджені проти Росії, є результатом дефіциту продовольства у світі тощо. Авторитетні джерела інформації підриваються, що призводить до дезінформації, поляризації суспільств та послабленні довіри до інститутів. Аналіз механізмів розповсюдження фейкових новин дозволяє зрозуміти їхній вплив на процеси прийняття рішень та громадську думку.

III. Гібридна війна – нова ера конфліктів

Гібридна війна являє собою еволюцію збройних конфліктів, що поєднує елементи звичайної війни, кібератак, дезінформації та асиметричної війни. Прикладом може бути операція Білорусі та Росії, яка використовує шлях нелегальної міграції для дестабілізації країн східного флангу НАТО а особливо Польщі.

Цей комплексний спосіб ведення війни ставить перед державами та міжнародними організаціями серйозний виклик, вимагаючи нових стратегій і міжнародного співробітництва. Ця форма бою особливо активно використовується владою Російської Федерації та є важливим інструментом впливу на безпеку нашого регіону (Pasek, 2022).

IV. Висновки: виклики та перспективи:

В умовах кризи системи міжнародної безпеки, поширення фейкових новин і гібридної війни існує нагальна потреба в міжнародному співробітництві, посиленні кібербезпеки, сприянні критичному мисленню громадян і розробці нових інструментів і стратегій для протидії цим загрозам (Drzewicki, 2011). Для забезпечення безпеки Євросоюз і НАТО мають бути розширені о Україну, а не обмежуватися лише відправленням гуманітарної допомоги та військового обладнання. Ми не можемо ігнорувати той факт, що до Росії постачається зброя з Китаю та Ірану та комплектуючі до зброї із західних країн, які використовуються проти України. Слід підкреслити, що для забезпечення стабільності та безпеки на міжнародній арені необхідно адаптувати традиційні структури безпеки до нових реалій, використовуючи також війська НАТО та інших країн для підтримки цілісності України. Інакше найближчим часом будуть атакувані Литва, Латвія та Естонія, а потім Польща на різних рівнях. Ми не можемо виключати загрози щодо нелегальних емігрантів в нашій частині континенту, інспіровані агентами впливу Російської Федерації. Економічна співпраця у відбудові України та майбутня військова співпраця між Німеччиною, Польщею та Україною ставатимуть дедалі важливішими, звісно, після того, як російських окупантів буде вигнано з України, інакше через 7-11 років після того, як Російська Федерація відновить свій військовий потенціал, почне нову війну в Європі.

Література

Banaszak, B. (2012). *Konstytucja Rzeczypospolitej Polskiej, Komentarz*. 2. Wydanie. Wydawnictwo C.H. BECK.

Kowalska-Chrzanowska, M., Krysiński, P. (2023). Fake newsy na temat wojny w Ukrainie w świetle projektu „Zgłoś Trolla”. *Zeszyty Prasoznawcze*, 66, 1 (253), 12-24.

Jurczak, T. (2023). Minister Krzysztof Szczerski w Radzie Bezpieczeństwa ONZ: Rosyjskie cyberataki na Polskę znacząco się nasiliły. *Dziennik Gazeta Prawna*, 26. URL: <https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8723199,rosyjskie-cyberataki-na-polske-sie-nasilily.html>

Kulesa, Ł. (2023). Polska obejmuje przewodnictwo w OBWE. *Polski Instytut Spraw Międzynarodowych*. URL: <https://www.pism.pl/publikacje/polska-obejmuje-przewodnictwo-w-obwe>

Rosyjski generał ujawnił dlaczego Kreml sprowokował wojnę w Syrii (2023). *Portal Społeczno-Polityczny Jagiellonia.org*. URL: <https://jagiellonia.org/rosyjski-general-ujawnil-dlaczego-rosja-sprowokowala-wojne-w-syrii>

Sokala, W. (2023). Wojna Izraela z Hamasem. Kto wygra walkę o serca opinii publicznej? *Dziennik Gazeta Prawna*. URL: <https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/9326859,wojna-izraela-z-hamasem-kto-wygra-walke-o-serca-opinii-publicznej.html>

Pacek, B. (2022). *Wojna hybrydowa na Ukrainie*. Warszawa, 111-175.

Drzewicki, A. (2011). Stosunki z Ukrainą w sferze bezpieczeństwa: polski punkt widzenia. *Polityczno-strategiczne aspekty bezpieczeństwa, I-2011/17*, 67.

Тодоров Ігор Ярославович

*доктор історичних наук, професор,
Ужгородський національний університет, м. Ужгород, Україна*
ORCID: 0000-0003-0986-9485

Тодорова Наталія Юріївна

*кандидат філологічних наук, доцент,
Ужгородський національний університет, м. Ужгород, Україна*
ORCID: 0000-0003-2282-6447

СТІЙКІСТЬ ТА ОПОРНІСТЬ УКРАЇНИ В КОНТЕКСТІ ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ

Співпраця із зовнішніми партнерами України в умовах російської інвазії має вирішальне значення в забезпеченні стійкості та опірності. Особливе місце тут займає співробітництво з Північно-Атлантичним Альянсом та майбутнє членство в НАТО. Термін національна стійкість почав використовуватися НАТО відносно недавно, з грудня 2015 року. На саміті Альянсу у Варшаві у 2016 р. було визначено стійкість як важливий засіб протистояння гібридним загрозам і суттєва основа успішного стримування та оборони, а також ефективним втіленням завдань організації. Зобов'язання щодо підвищення стійкості, ухвалені під час саміту НАТО у Варшаві, включало: посилення військових можливостей разом із підвищенням готовності цивільного населення протистояти загрозам; захист населення та територій держав-членів шляхом забезпечення неперервності державного управління, надання основних послуг та безпеки критичної цивільної інфраструктури, включаючи енергетику, транспорт та зв'язок; підвищення стійкості через інвестування у надійні військові здатності; захист національної інфраструктури та мереж від кібератак (Commitment to enhance resilience, 2016) .

Потенціал національної стійкості та національної безпеки в значній мірі обумовлений зовнішніми чинниками та їхнім врахуванням у відповідній державній стратегії. Договір про створення НАТО вже передбачав певні показники стійкості,

включаючи такі терміни як «самодопомога» та «самооборона,» які відображали головні принципи національної стійкості для учасників альянсу. Засади резильєнтності були також закладені у статті 3 Договору, яка вимагала, що всі союзники розвиватимуть свої індивідуальні та колективні спроможності для відбиття збройного нападу (The North Atlantic Treaty, 1949).

Співробітництво в галузі національної безпеки між Україною та НАТО розпочалося з підписання та впровадження Програми "Партнерство заради миру" (1994 р.) і Хартії про особливе партнерство (1997 р.). в 1997-2023 діяла Комісія Україна-НАТО (КУН) як інституційна основа для окремих партнерських програм та ініціатив. В 2023 р. КУН була трансформована в Раду Україна-НАТО.

Початок російської агресії в 2014 р. призвів до інтенсивного розвитку безпекового співробітництва між Україною та Альянсом. З липня 2016 р. Україна отримала Комплексну програму допомоги від НАТО, що призвело до розширення військової та військово-технічної співпраці між сторонами. В червні 2020 р. Україна отримала статус партнера НАТО з розширеними можливостями, що відкрило для неї доступ до додаткових можливостей співробітництва з Альянсом відповідно до комплексних положень Ініціативи оперативної сумісності партнерства.

Згідно з положеннями Річної національної програми в рамках Комісії Україна - НАТО на 2021 рік, передбачалася створення Національної системи стійкості. Ця система ґрунтувалася на міжвідомчій координації роботи між центральними органами виконавчої влади, іншими державними установами, громадськими організаціями, приватним сектором та міжнародними партнерами. У ситуації кризи посилення позицій України ставало однією з головних пріоритетних задач співробітництва України з Північноатлантичним Альянсом. Окремим аспектом були партнерські програми, які входили в рамки Річної національної програми і були спрямовані на підтримку соціальної стійкості і підвищення здатності відповідати на виклики безпеки на рівні територіальних громад. Певні програми також були спрямовані на підтримку управління об'єднаними територіальними громадами і надання інфраструкції

населенню щодо ризиків і загроз з точки зору соціальної стійкості цих громад. Річна національна програма також передбачала розробку та впровадження механізмів та методологічних підходів до оцінки ризиків і розробки наукових підходів до їх попередження в контексті Національної системи стійкості. Цей документ свідчив про успішність співпраці з НАТО, яке стало ключовим партнером у сфері зовнішньої політики і безпеки України та мало безпосередній вплив на формування системи регулювання і впровадження системи національної стійкості, а також на взаємозв'язок аспектів національної стійкості та національної безпеки з практичними зовнішньополітичними заходами (Указ Президента України, 2021).

Концепція національної стійкості України значним чином базується на наративі стійкості, який був розроблений під час створення концепції стійкості держав-членів Європейського Союзу. Цей наратив, зокрема, акцентується на протидії гібридним загрозам, особливо від Російської Федерації. Стратегія національної безпеки ЄС, яка була запущена у 2015 році, і План імплементації заходів у сфері безпеки та оборони (грудень 2016 р.), включають аспекти національної стійкості як важливу складову частину національної безпеки та заходів для її зміцнення. План також передбачає підтримку національної стійкості та стабільності зовнішніх партнерів Європейського Союзу, включаючи Україну.

В цьому контексті, програми та проекти, які залучали як українських, так і європейських учасників, такі як «Resilient Ukraine/Стойка Україна: громадянське суспільство та волонтери у зміцненні національної стійкості та безпеки України». Ця структура представляла новий підхід до розвитку національної стійкості як частини національної безпеки, який акцентував увагу на розвитку громадянського суспільства як важливого компонента стратегії національної стійкості. Цей підхід особливо підкреслював роль «самообілізації» громадянського суспільства як основи для забезпечення самовідтворення ключових параметрів соціальної стабільності в українському суспільстві, особливо в умовах агресії Російської Федерації, особливо на сході України. Можна стверджувати, що

подальше зміцнення підтримки структур громадянського суспільства в Україні, як суб'єктів процесу зміцнення національної стійкості з боку європейських структур, спроможне призвести до посилення уваги до ролі громадянських акторів у реалізації відповідних державних програм щодо зміцнення національної стійкості України.

Здійснення концепції політики національної стійкості в сучасній Україні тісно пов'язане із взаємодією з зовнішньополітичними партнерами країни. Ця взаємодія виявляється як у програмах та напрямках співпраці між міжнародними структурами та Україною, так і в орієнтації України на концепції національної стійкості та національної безпеки, які розробляються європейськими та північноамериканськими експертними групами.

Співробітництво України з євроатлантичними партнерами сприяє подальшій конкретизації та розширенню підходів Української держави до концепції національної стійкості як частини механізмів забезпечення національної безпеки. Роль громадянського суспільства у гарантуванні національної стійкості та соціальної стійкості територіальних громад є необхідною складовою структури національної стійкості України. Ці аспекти знаходяться під увагою європейських та євроатлантичних структур у контексті їхніх програм безпекового партнерства, спрямованих на підтримку національної стійкості України під час війни з Російською Федерацією. У цьому контексті, євроатлантичне спрямування міжнародного безпекового співробітництва України стало важливим компонентом включення національної стійкості в систему пріоритетів національної безпекової стратегії Української держави.

НАТО засуджує найбільш рішучим чином жорстоку і неспровоковану загарбницьку війну Росії проти України – незалежної, мирної і демократичної країни, близького партнера Альянсу. Як НАТО, так і держави-члени Альянсу продовжують надавати Україні допомогу на безпрецедентному рівні з метою гарантування її основоположного права на самооборону. На саміті НАТО у Вільнюсі у 2023 році держави-члени Альянсу підтвердили відданість майбутньому вступу України до НАТО. Держави-члени Альянсу і надалі підтримуватимуть Україну

і аналізуватимуть її здобутки у досягненні оперативної сумісності, а також додаткових демократичних і безпекових перетворень, що є необхідною умовою для вступу до НАТО (Комюніке Вільнюського саміту, 2023).

Основні напрями зовнішнього співробітництва України щодо питань опорності та національної стійкості мають глибоку взаємозалежність. Україні необхідно більше залучати зовнішній фактор до розвитку сучасних систем національної стійкості та опірності. Тому участь в програмах, започаткованих зовнішніми партнерами України, може відзначатися як важливий крок у подальшому розширенні національної політики в цьому контексті. Проте це не передбачає безпосереднього копіювання зовнішніх політик чи їх фундаментальних принципів. Замість цього, метою є збагачення українських політичних ініціатив у сфері національної стійкості та національної безпеки за рахунок зовнішнього (особливо, європейського) досвіду, що в свою чергу стає фундаментом для обміну досвідом із зовнішніми партнерами України. Такий підхід сприятиме досягненню ефективних результатів у зміцненні опорності та стійкості українців в майбутньому.

Література

Комюніке Вільнюського саміту видане главами держав і урядів країн-членів НАТО, які взяли участь у засіданні Північноатлантичної ради у Вільнюсі 11 липня 2023 року. URL: https://www.nato.int/cps/uk/natohq/official_texts_217320.htm?selectedLocale=uk

Указ про Річну національну програму під егідою Комісії Україна – НАТО на 2021 рік 2021 (Президент України). *Офіційний сайт Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/189/2021#Text>

Commitment to enhance resilience. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw (2016). NATO. URL: https://www.nato.int/cps/en/natohq/official_texts_133180.htm

The North Atlantic Treaty (1949). Washington D. C. URL: https://www.nato.int/cps/en/natohq/official_texts_17120.htm

ქეთი ჯიჯეიშვილი
პოლიტიკის დოქტორი, პროფესორი

საქართველო ევროპული ინტეგრაციის გზაზე

დამოუკიდებელ საქართველოსა და ევროსტრუქტურებს შორის ურთიერთობების დაწყება 1993 წლის მაისით თარიღდება, როდესაც ბრიუსელში შეკრებილმა სამხრეთ კავკასიისა და ცენტრალური აზიის სახელმწიფოების ვაჭრობისა და ტრანსპორტის მინისტრებმა ევროპული გაერთიანებების მესვეურებთან ერთად მიიღეს დეკლარაცია ტრანსრეგიონალური სატრანსპორტო დერეფნის განვითარების პროგრამის განხორციელების შესახებ. შემდეგ იყო ტაისისი“-ს პროგრამა, რომელმაც 1994 წლიდან ბევრი სიკეთე მოუტანა საქართველოს ეკონომიკური თუ სოციალურ-პოლიტიკური კუთხით, რასაც მოჰყვა 1996 წელს გადადგმული ნაბიჯები საქართველოსა და ევროკავშირს შორის ხელშეკრულებითი ურთიერთობების ჩამოყალიბების მიზნით – დაიდო პარტნიორობისა და თანამშრომლობის ხელშეკრულება (PCA), რომელიც 1999 წლიდან შევიდა ძალაში, 2004 წელს კი შემუშავდა ევროკავშირის სამეზობლო პოლიტიკა (ENP) (European Neighbourhood Policy.) საერთოდ, 2004 წლამდე ევროკავშირსა და საქართველოს შორის ურთიერთობები დონორსა და რეციპიენტს შორის ურთიერთობებს წარმოადგენდა. ამ პერიოდში ევროკავშირის საქართველოსთვის უკვე 450 მლნ. ევროს ოდენობის დახმარება ჰქონდა გაწეული და აშშ-სთან ერთად უმსხვილესი დონორი იყო. (გეგეშიძე, 2007, 14).

ევროკავშირის სამეზობლო პოლიტიკაში, რომელშიც გაერთიანებულია 16 სახელმწიფო, ძირითად მიზნად განისაზღვრა ახალი წევრი სახელმწიფოების მიღება მის შემადგენლობაში, გაფართოებულ ევროკავშირსა და მის მეზობელ ქვეყნებს შორის გამყოფი ხაზების წარმოქმნის თავიდან აცილება და სტაბილურობისა და კეთილდღეობის მხარდაჭერა.

საქართველოს მიწვევა ევროპულ `სამეზობლო პოლიტიკაში~ მონაწილეობის მისაღებად მნიშვნელოვანწილად `ვარდების რევოლუციის~ შედეგი იყო. (გეგეშიძე, 2018, 10) მიუხედავად იმისა, რომ ახალი მთავრობის უმთავრეს საგარეო-პოლიტიკურ პრიორიტეტს ნატოში გაწევრიანება წარმოადგენდა, ევროკავშირში ინსტიტუციური ინტეგრაციაც ასევე მკაფიოდ დადგა დღის წესრიგში. შეიქმნა ევროპული და ევროატლანტიკური ინტეგრაციის საკითხებში სახელმწიფო მინისტრის აპარატი, რომელიც მოწოდებული იყო გაეწია უწყებათაშორისი კოორდინაცია ევროკავშირთან ურთიერთობის მიმართულებით. (Gegeshidze, 2006, 10). ყველა სახელმწიფო დაწესებულების თავზე ევროპულმა დროშამ დაიწყო ფრიალი. აღსანიშნავია, რომ `სამეზობლო პოლიტიკის~ სამოქმედო გეგმაზე მუშაობისას ქართული მხარე დაჟინებით მოითხოვდა პრეამბულაში ევროკავშირის წევრობის პერსპექტივის დაფიქსირებას.

მიუხედავად იმისა, რომ `სამეზობლო პოლიტიკა~ საქართველოს, როგორც სახელმწიფოს, იმგვარ მოდერნიზებას გულისხმობდა, რომელიც მიზნად ისახავდა პოლიტიკური, სამართლებრივი და ადმინისტრაციული სისტემების ევროპულ სტანდარტებთან დაახლოებას, იგი ევროკავშირის წევრობასთან რაიმე კავშირს იმთავითვე გამორიცხავდა. ეს კი თბილისში არ მოსწონდათ.

სამაგიეროდ, ბრიუსელში არ მოსწონდათ განვითარების ე.წ. სინგაპურიზაციის მოდელი, რომელიც არსებითად ახალი მთავრობის ლიბერტარიანულ ხედვას ეფუძნებოდა და ყოველთვის არ ეთავსებოდა `სამეზობლო პოლიტიკის~ სამოქმედო გეგმით გათვალისწინებული რეფორმების დღის წესრიგს (გოგოლაშვილი, 2017, 11).

2008 წლის რუსეთ-საქართველოს ომმა ამ მხრივ მდგომარეობა რადიკალურად შეცვალა. მართალია, რუსეთიდან მომდინარე რისკების მიუხედავად, ევროკავშირს რუსეთთან გლობალურ დონეზე არ შეუცვლია თავისი საგარეო სტრატეგია – არ შეუწყვეტია ჩართულობის პოლიტიკა, რომელიც ეყრდნობოდა შეხედულებას, რომ ევროპის უსაფრთხოების მიღწევა შესაძლებელი იყო მხოლოდ რუსეთთან ერთად და არა მასთან დაპირისპირების გზით (ევროპის

საბჭო, 2016), მაგრამ გარკვეული გეოპოლიტიკური დასკვნები მაინც გააკეთა საქართველოსთან მიმართებაში – დააჩქარა ინტეგრაციის პროცესი, რამაც გარკვეულწილად განაპირობა კიდევ ომის შემდეგ, 2008 წელს აღმოსავლეთ პარტნიორობის ინიციატივისადმი (EaP) ევროკავშირის დადებითი გამოხმაურება. ხოლო 2013 წელს საქართველო-ევროკავშირის ასოცირების შეთანხმების პრაფირება, ღრმა და ყოვლისმომცველი თავისუფალი ვაჭრობის კომპონენტის ჩათვლით, რომელიც ძალაში შევიდა **2016 წლის 1 ივლისს**.

აღსანიშნავია, რომ ურთიერთობების დასაწყისში თავდაპირველ პროექტებში ევროკავშირი საქართველოსთან ინდივიდუალური პოლიტიკის წარმოების ნაცვლად, საქართველოს განიხილავდა რეგიონალურ კონტექსტში. როდესაც ხდებოდა ევროკავშირის მიერ პრიორიტეტთა განსაზღვრა ამიერკავკასიაში, მხედველობაში არ იღებდნენ საქართველოს თვითიდენტიფიკაციას, რომლის თანახმადაც იგი კულტურულად და ისტორიულად ევროპას აკუთვნებს თავს, ყოველთვის იყო გამორჩეული სამხრეთ კავკასიის სახელმწიფოებს შორის ევროპული მისწრაფებებით და დამოუკიდებლობის გამოცხადების დღიდან არასოდეს არ მომხდარა ევროპული იდეის დევალვაცია; მაშინ როდესაც სამხრეთ კავკასიის რეგიონის დანარჩენი ორი სახელმწიფო – სომხეთი და აზერბაიჯანი, თვითიდენტიფიკაციის განსაზღვრის დროს საკმაოდ არათანმიმდევრულები იყვნენ – სომხეთი, ოფიციალურად, რუსეთის სტრატეგიული პარტნიორი იყო, ხოლო აზერბაიჯანი დაბალანსებულ ურთიერთობას აწარმოებდა რუსეთთანაც და დასავლეთთანაც. ეს ფაქტი ქმნიდა გარკვეული უკმაყოფილების განცდას ქართულ საზოგადოებაში, მაგრამ თუ ამ ასკითხის უფრო სიღრმისეულ ანალიზს მოვახდენთ, ევროკავშირის ეს მიდგომები არც იყო გასაკვირი. ისტორიულად, ევროკავშირის გაფართოების ტალღებს თუ გავითვალისწინებთ, თითქმის ყველა ჯერზე რამდენიმე ქვეყანა ერთროულად უერთდებოდა ევროკავშირს, ვინაიდან ევროკავშირის ინტერესი, ძირითადად, რეგიონების მიმართ იყო, და არა კონკრეტული ქვეყნის მიმართ. გამონაკლისი იყო საბერძნეთი (1981წ.) და ბოლო, 2013 წლის მეშვიდე გაფართოება, როდესაც მხოლოდ ხორვატია შეუერთდა ევროკავშირს. ამიტომ შესაფერის მომენტში

საქართველომ მიიღო მეტად რაციონალური გადაწყვეტილება და გააკეთა განაცხადი ევროკავშირის წევრობაზე მოლდოვასა და უკრაინასთან ერთად, როგორც ასოცირების ტრიოს წევრმა.

უკრაინის წინააღმდეგ რუსეთის სრულმასშტაბიანმა და აგრესიულმა ომმა შეცვალა ევროპული უსაფრთხოების დღის წესრიგი. ამჟამად ევროკავშირმა შეძლო ბოლომდე გაეცნობიერებინა და ეღიარებინა რეგიონში ძალისმიერი პოლიტიკური კონკურენციის დაძაბულობა და საფრთხე, რომელსაც რუსეთი უქმნის ევროკავშირს, შესაბამისად, პოლიტიკა რუსეთის მიმართ ჩართულობიდან იზოლაციისკენ და შეკავებისკენ შეცვალა, გადახედა „რუსეთი უპირველეს ყოვლისა“ მიდგომასა და პრიორიტეტი მიენიჭა პარტნიორებსა და მოკავშირეებს (Meister, 2022).

ევროკავშირის უმაღლესი წარმომადგენლის ჯოზეფ ბორელის სიტყვით „პუტინის ომმა სათავე დაუდო გეოპოლიტიკურ ევროპას“ (Borrell, 2022). ევროკავშირმა უკრაინის წინააღმდეგ რუსულ აგრესიას თავისთვის სანქციების დაწესებით, ერთიანობის შენარჩუნებით, ტრანსატლანტიკური პარტნიორობის გამოცოცხლებით და თავისი ენერგოდამოუკიდებლობისა და თავდაცვისუნარიანობის განმტკიცებისკენ გადადგმული ნაბიჯებით უპასუხა.

2022 წელს 23 ივნისს ბრიუსელში გამართულ ევროკავშირის წევრი სახელმწიფოების ლიდერთა სამიტზე მიღებული გადაწყვეტილებით უკრაინამ და მოლდოვამ მიიღეს კანდიდატის სტატუსი, ხოლო საქართველომ ევროპული პერსპექტივა და პირობები კანდიდატის სტატუსის მისაღებად. ([https://matsne.gov.ge > document](https://matsne.gov.ge/document)). რაც ალბათ ყველაზე გეოპოლიტიკური ხასიათის გადაწყვეტილებაა, რომელიც ევროკავშირმა პუტინის ომის საპასუხოდ მიიღო.

ევროკომისიის პრეზიდენტის განცხადების თანახმად, უკრაინამ ევროპა გააოცა ომის პირობებში მისი სახელმწიფო ადმინისტრაციის ქმედითუნარიანობით, დეცენტრალიზაციის მაღალი ხარისხითა და ადგილობრივი მმართველობების მიერ დამოუკიდებელი გადაწყვეტილებების მიღების უნარით. მოლდოვას მიმართ, მიუხედავად მრავალი პრეტენზიისა, ევროკომისიის პრეზიდენტის ურსულა ფონ დერ ლაიენისა და

ევროკომისარ ოლივერ ვარჰელის თქმით, ახალი ლიდერშიპი იძლევა იმედს, რომ ქვეყანა ყველა პრობლემას გაუმკლავდება. (გოგოლაშვილი, 2022).

ორივე ქვეყანასთან მიმართებით აღინიშნა, რომ ევროკომისია ენდობა მათ მთავრობებს და უადვილდება მათთან თანამშრომლობა. საქართველოს შემთხვევაში, მიუხედავად იმისა, რომ „აპროქსიმაციის“ მაჩვენებლით უკრაინასა და მოლდოვას არ ჩამოვუვარდებით, ასეთი დამოკიდებულება ევროკომისიას არ გამოუთქვამ, რადგან. ჩათვალეს რომ საქართველოს ხელისუფლების რიტორიკა, შიდა პოლიტიკური სისტემის განვითარების დინამიკა და საგარეო პოზიცია უკრაინის ომთან დაკავშირებით თვალშისაცემად ჰგავდა ბ-ნი ორბანის რიტორიკასა და პოზიციას. საქართველომ ევროკავშირისათვის უფრო შესამჩნევი გახადა ევროკავშირის უნგრული პრობლემა, რომელიც აზიანებს როგორც ევროკავშირის შიდა ერთობას, ასევე აზიანებს მის საგარეოპოლიტიკურ რეპუტაციასა და საიმედოობას. (საბანამე, 2022, 34) მათი შეხედულებით საქართველოში სახეზე იყო მკაფიო ურთიერთდამოკიდებულება პოპულიზმს, პოლიტიკური პოლარიზაციის მაღალ დონესა და დემოკრატიის უკუსვლას შორის. ევროკავშირმა საქართველოს ევროკავშირის წევრობის კანდიდატის სტატუსის მისაღებად შესასრულებელად განუსაზღვრა 12 პირობა, რომელთა შორისაა; პოლიტიკური პოლარიზაციის დაძლევა, ინსტიტუტების გამართულად მუშაობა და მათი დამოუკიდებლობა, სასამართლოს რეალური დამოუკიდებლობა და მიუკერძოებლობა, ელიტური კორუფციის შემთხვევების ეფექტიანად გამოძიება, დეოლიგარქიზაცია, თავისუფალი მედიაგარემო და ა.შ. და მისცა შანსი მისი მრავალსაუკუნოვანი ოცნების განსახორციელებლად და ევროპულ ოჯახში დასაბრუნებლად.

გამოყენებული ლიტერატურა

გეგეშიძე, ა. (2018). საქართველოს ევროპული პერსპექტივა: როგორ დავიხლოვოთ მომავალი. კრ. საქართველოს ევროპული პერსპექტივის გახსნა. თბილისი: ლევან მიქელაძის სახელობის ფონდი. 10.

Gegeshidze, A. (2006). Georgia in the Wider Europe Context: Bridging Divergent Interpretations', CPC International Fellowship Program, Open Society Institute, 10.

გოგოლაშვილი, კ. (2017). საქართველო - ევროკავშირის ურთიერთობები და სამომავლო პერსპექტივები, პოლიტიკის დოკუმენტი, თბილისი: საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობების კვლევის ფონდი, 11.

European Council,. (2016, March 14). EU's Five Guiding Principles in Relation to Russia. <https://www.consilium.europa.eu/en/meetings/fac/2016/03/14/last>

Meister, S. (2022, November 29). "A Paradigm Shift: EU-Russia Relations After the War in Ukraine", Carnegie Europe. <https://carnegieeurope.eu/2022/11/29/paradigm-shift-eu-russia-relations-after-war-in-ukraine-pub-88476>

Borrell, J. (2022, March 24). Europe in the Interregnum: Our Geopolitical Awakening After Ukraine". <https://geopolitique.eu/en/2022/03/24/europe-in-the-interregnum-our-geopolitical-awakening-after-ukraine/>

საქართველოს საკანონმდებლო მაცნემ ევროკავშირის პოტენციური კანდიდატი ქვეყნის სტატუსით მონაწილეობა მიიღო ევროპის ოფიციალური ბეჭდვითი ორგანოების ფორუმში (EFOG). URL: <https://matsne.gov.ge>.

გოგოლაშვილი, კ. (2022). კანდიდატის სტატუსის მომლოდინე საქართველო ევროპულ პერსპექტივას მიიღებს, რაზე გვაქვს სანერვიულო? თბილისი: საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობების კვლევის ფონდი. URL: <https://gfsis.org.ge/ge/blog/view/1459>

საბანაძე, ნ. (2022). ევროკავშირის გაფართოების გეოპოლიტიკა: საქართველოს მაგალითი. პოლიტიკის დოკუმენტი. თბილისი: საქართველოს პოლიტიკის ინსტიტუტი. URL: <https://gip.ge/wp-content/uploads/2022/12/Policy-Paper-34-GEO.pdf>

გიორგი ჩხიკვიშვილი
სოციალურ მეცნიერებათა დოქტორი,
სტუ-ს ასოცირებული პროფესორი

საქართველოს ევროპული არჩევანი: ისტორიულ - პოლიტიკური ექსკურსი

ქართველი ხალხის ევროპისაკენ სწრაფვის ურყევი და უპირობო რწმენის სათავე ჩვენს ისტორიაში უნდა ვეძებოთ. ჩვენი გეოპოლიტიკის მიუხედავად თავისუფლებისა და თანასწორობის ევროპული ღირებულებები წითელ ზოლად გასდევდა ქართულ პოლიტიკურ აზროვნებას. რენესანსის პერიოდის საქართველო წარმოადგენდა მოწინავე ევროპულ ქვეყანას ადამიანთა უფლებების დაცვისა და ხელისუფლების გადანაწილების კუთხით. მან ერთ-ერთმა პირველმა შექმნა „ომბუცმენის ინსტიტუტი“- კარი საჯარო, რომელიც იძლეოდა სხვადასხვა სახის გადაცდომების გასაჩივრების საშუალებას; „ისნის კარავი“ კი პარლამენტის მსგავსს საკანონმდებლო უფლებებით აღჭურვილ მუდმივ დაწესებულებას წარმოადგენდა. სამწუხაროდ, ჩვენი ქვეყნის გეოპოლიტიკური მდებარეობის გამო საზოგადოების დემოკრატიული განვითარების ტენდენცია ნაადრევად განიმუხტა, საქართველომ შეწყვიტა ბუნებრივი განვითარება და მთელი შუა საუკუნეების მანძილზე პოლიტიკურად საქართველო ისლამური სამყაროს წევრი იყო. თუმცა ძირითად ნიჰნად ყოველთვის რჩებოდა დასავლეთისაკენ ხიდების გადება. ამას ემსახურებოდა ქართველი მწერლისა და ლექსიკოგრაფის სულხან საბა ორბელიანის მოგზაურობა საფრანგეთის მეფე ლუი XIV-სთან. სულხან-საბამ სცადა კათოლიკურ რწმენაზე მოექცია საქართველო იმ იმედით, რომ დასავლეთი კათოლიკური ქვეყნის დაცვას უფრო მოინდომებდა, მაგრამ ეს ვიზიტი უშედეგო აღმოჩნდა (macaberiZe, 2019, 108).

XVIII ს.-ის მეორე ნახევრის ქართული პოლიტიკური აზრი გაჯერებული იყო ფრანგი განმანათლებლების იდეებით. ვოლტერის გავლენით განსაკუთრებით გამოირჩეოდა დავით ბაგრატიონი,

ქართლ-კახეთის უკანასკნელი მეფის, გიორგი XII-ის, მემკვიდრე, რომელსაც ოთახში ვოლტერის სურათი ეკიდა და მას თავის მასწავლებლად აღიარებდა. მანვე თარგმნა ქართულად მონტესკიეს „კანონთა გონი“. (ასათიანი, 1933, 1933, 64-68.). მონტესკიეს ნაშრომის – „კანონთა გონის“ გავლენით არის შექმნილი ალექსანდრე ამილახვარის ბრწყინვალე ნაშრომი „ბრძენი აღმოსავლეთისა“ (საქართველოს ისტორიის ნარკვევები, 1973, 195).

დასავლეთისადმი ქართული პოლიტიკური აზრის სიმპატიების მიუხედავად, მსოფლიო პოლიტიკური ძალების მაშინდელი კონფიგურაციიდან გამომდინარე საქართველო არ აღმოჩნდა ევროპის ქვეყნების პოლიტიკური ინტერესების სფეროში, ამიტომ ჩვენმა ევროპულმა გზამ რუსეთზე გაიარა. რუსულად თარგმნილი გერმანული იდეალიზმის ტექსტებისა და რომანტიკოსი პოეტების რეციპირებით ხდებოდა ეროვნული იდეის შემოტანა მე-19 საუკუნის საქართველოში. რუსეთის გზით ვრცელდებოდა ევროპული იდეოლოგიები, განსაკუთრებით დიდი იყო სოციალისტური იდეების გავლენა. ქართული პოლიტიკური აზროვნების ევროპეიზაციამ შექმნა ის საფუძველი, რომელმაც შესაძლებელი გახადა ევროპულ ნიადაგზე შემუშავებული იდეოლოგიებისა და მოძრაობების საქართველოში გადმოტანა, შემდეგ კი დემოკრატიული პოლიტიკური კულტურის დამკვიდრების და დემოკრატიული სახელმწიფოს მშენებლობის მცდელობა.

ევროპულ ცივილიზაციაში საქართველოს „დაბრუნებაზე“, რაც მის ბუნებრივ მდგომარეობად მოიაზრებოდა, პირველად საუბარი დაიწყო სიმბოლისტ პოეტთა ჯგუფ „ცისფერი ყანწების“ წევრებმა მე-20 საუკუნის დასაწყისში. მათი დევიზი იყო „დასავლეთისკენ“. (ბრისკუ, 2017).

„განათლებულ ევროპასა და ჩვენს შორის სიახლოვე ორ თუ სამ წელიწადში არ წარმოშობილა. შორეულ წარსულში ყველაფერი ბევრად უკეთესად იყო; ჩვენ მიერ დავიწყებული ჩვენი წინაპრები ქართულად კითხულობდნენ პლატონს და შეგვიძლია ვთქვათ, რომ მათ ბერძნული ფილოსოფიის თავიანთი სკოლა დააარსეს“ – წერდა ცისფერყანწლების ერთ-ერთი ალამდარი პაოლო იაშვილი. (იაშვილი, 1995, 66) „ჩვენ ყოველთვის დასავლეთისკენ

მივისწრაფოდით.... თუმცა, გეოგრაფიული ადგილმდებარეობა ჩვენი უბედურება იყო“ - აგრძელებდა ცისფერყანწელების მეორე მედროშე გრიგოლ რობაქიძე.

ჩვენი ევროპულობის დამადასტურებელი ერთ-ერთი ყველაზე მყარი დოკუმენტი არის საქართველოს დამოუკიდებლობის (1918 - 1921 წ.წ.წ) დროს შექმნილი საქართველოს პირველი კონსტიტუცია, რომელიც შევიდა ევროპული კონსტიტუციების პირველ ათეულში და დემოკრატიული პრინციპების სამართლებრივი რეგულაციების კუთხით აღიარებულია, როგორც ერთ-ერთი ყველაზე დემოკრატიული კონსტიტუცია. სამწუხაროდ, ამ კონსტიტუციამ მხოლოდ 3 დღე იარსება, რადგან მოხდა საქართველოს ოკუპაცია და ანექსია საბჭოთა ძალების მიერ.

საქართველოს დამოუკიდებლობის აღდგენის შემდეგ ისევ იწყება აქტიური საუბრები საქართველოს მნიშვნელოვანი წვლილის შესახებ დასავლური ცივილიზაციის ჩამოყალიბება-განვითარებაში, რამდენადაც საქართველო იყო ერთ-ერთი პირველი ევროპული ქვეყანა, რომელმაც ქრისტიანობა სახელმწიფო რელიგიად აღიარა, ხოლო ქრისტიანული ფასეულობები ევროპული იდენტიფიკაციის ერთ-ერთ აუცილებელ კომპონენტად არის მიჩნეული.

ლუქსემბურგის ევროპულ კვლევათა ინსტიტუტის დირექტორის არმანდ კლესის მიერ თბილისის სახელმწიფო უნივერსიტეტში ლექციის წაკითხვისას საქართველოს ევროპული იდენტობის გასარკვევად დასახელებული იქნა ექვსი კრიტერიუმი, რომლებიც საფუძვლად უდევს ევროპულ ინტეგრაციას - პოლიტიკა, ეკონომიკა, სტრატეგია, გეოგრაფია, კულტურა და რელიგია. ეკონომიკა ცალსახად უარყოფს ჩვენს მიკუთვნებულობას ევროპულ სივრცესთან, რადგანაც იგი დასავლეთად წარმოგვიდგენს განვითარებული ინდუსტრიული ქვეყნების უმრავლესობას (ამ ნიშნით იაპონიაც ევროპული ერთობის წევრად მოიაზრება), გეოგრაფიული კრიტერიუმის მიხედვით სადავოა არის თუ არა საქართველო ევროპის ნაწილი. რაც შეეხება დანარჩენ ოთხ კრიტერიუმს, ისინი საქართველოს ევროპის ფარგლებში აქცევენ (ჩიქოვანი, 2005, 178). ამრიგად, არამარტო ქართველი ხალხის ევროპული თვითიდენტიფიკაციის, არამედ ასევე ზემოაღნიშნული კრიტერიუმების უმრავლესობის მიხედვითაც დასტურდება

საქართველოს ევროპულ ცივილიზაციასთან მიკუთნებულობის იდეა, რაც კიდევ ერთხელ დაადასტურა 2023 წელს IRI -ს მიერ ჩატარებულმა გამოკითხვამ, რომლის მიხედვითაც მოსახლეობის მხარდაჭერამ ევროკავშირში გაწევრიანებისათვის 89%-იან ნიშნული აჩვენება (IRI, 2023).

ბიბლიოგრაფია

მაცაბერიძე, მ. (2019). საქართველოს პოლიტიკური სისტემა. თბილისი: ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის გამომცემლობა, 108.

ასათიანი, ლ. (1933). ვოლტერიანობა საქართველოში. თბილისი, 64-68.

საქართველოს ისტორიის ნარკვევები (1973). თბილისი, ტ. IV, 195.

ბრისკუ, ი. (2017). ასე შორს, და მაინც ასე ახლოს. ევროპის სახე-ხატი საქართველოში: იდეათა ისტორია. <https://ge.boell.org/ka/2017/05/05/ase-shors-da-mainc-ase-axlos-evropis-saxe-xati-sakartveloshi-ideata-istoria>.

იაშვილი, პ. (1995). თარგმნილი ლიტერატურა. კრებული: ევროპა თუ აზია. თბილისი: ლიტერატურის მატეანე, 66.

ჩიქოვანი, ნ. (2005). საქართველოს კულტურული რაობა და ცივილიზაციური კუთვნილება ცივილიზაციასთან თეორიის კონტექსტში. თბილისი: თბილისის უნივერსიტეტის გამომცემლობა, 138.

IRI. (2023). <https://civil.ge/ka/archives/538757>

Gvantsa Abesadze

New higher education institution "New Uni", Tbilisi, Georgia

ALIGNMENT OF GEORGIA'S FOREIGN POLICY WITH THE EUROPEAN UNION'S FOREIGN AND SECURITY POLICY ON THE PATH OF INTEGRATION

Once the extension process started, the European Union incorporated the alignment of the countries with its common foreign and security policy as one of the main criteria among the prerequisites that the states wishing to join the organization should meet. And recent events in international politics, such as various crises and the most important - Russia's military aggression against Ukraine have once again made it visible how important it is to have a consensus in decision-making and a unified foreign policy with partner states.

It's worth noting that there has been a notable shift in Georgia's foreign policy strategy in recent period, one can observe that it is gradually moving away from European aspirations, as well as somewhat contradicting the common goal of rapprochement with the West. In addition to the fact that the country's political vector has changed towards the warming of relations with Russia, which itself leads to the increase of Georgia's dependence on the aggressor state, the strategic partnership agreement signed with China has also raised many questions.

Georgia's aspiration to join the EU is based on the Association Agreement, which further determines the integration process and the country's readiness to conduct its own foreign policy in line with the common foreign principles of the EU. However, recently, after the processes of negotiations and accession with the associated trio were especially accelerated, the adoption of controversial decisions by the Georgian side has raised concerns regarding the alignment of Georgia's policies with the EU's security and foreign policy direction. This fact was also substantiated by the European Council's report,

which indicated a significant drop in the compatibility rate to nearly 10% compared to previous years (Georgia's (mis)alignment).

The compatibility of the foreign policy of the partner countries with the decisions made by the EU was actively brought to the agenda by the Russia-Ukraine war in 2022. Due to Russia's aggression, the European Union developed up to 26 declarations based on common values, which mainly meant imposing sanctions on the aggressor state, and all member and allied states joined it, including Ukraine, Moldova and Georgia itself, however, the latter initially joined only 3 declarations. It is noteworthy that the Georgian side explained this decision with the policy of non-irritation and national interests. "Georgia's economy will collapse, we will harm our own people if we impose bilateral economic sanctions on Russia," the country's prime minister said (საქართველოს..., 2023).

At the same time, while during 2022-2023, Georgia joined only 51 of the 107 declarations issued by the EU in the field of foreign policy and security, which is equal to only 48% of the existing ones, it is actually behind the indicators of Ukraine (91%) and Moldova (60%) (საქართველოს..., 2023; Georgia's (mis)alignment). These statistics are further aggravated by the confusing policy towards Russia with the opening of flights and dependency in trade relations.

On the other hand, there is an argument of the Georgian side about the occupied territories, that if the country joins all the sanctions imposed on Russia, it will not only have a bad effect on the economy of Georgia, but will also lead to the recognition of the occupied territories, Abkhazia and South Ossetia, although the Czech ambassador, who represents Georgia in the EU, took a critical position on this, who considers the fulfillment of 12 recommendations as a necessary condition for Georgia's accession to the EU. "The answer is always that it could lead to the recognition of Abkhazia and South Ossetia, but in this case Georgia should practically refrain from developing any kind of foreign relations if it constantly acts in fear of recognizing the occupied territories." (ჩეხეთის..., 2023).

However, it should be noted that the government's main argument that joining the sanctions imposed against Russia will disproportionately affect the economy of Georgia and the political situation of the occupied territories is completely inconsistent with the

document issued by the EU on the protection of human rights and minorities, moreover, the statements made contradict one of the main criteria necessary for joining the EU – States must respect European values.

I think that recently, Georgia's foreign policy is two-sided and on the one hand it is striving to maintain a pro-European course, while on the other hand the country is experiencing a democratic regression, which, in addition to deepening relations with Russia, is an obstacle to the prospects of Georgia joining the EU. We can single out those signs that had a negative impact on the European perspective of the country and on the implementation of the 12 recommendations, which serve as a prerequisite on the way to Europeanization.

- Suppression of freedom of speech and expression within the country, including the suppression of the freedom of expression of various minorities and pressure on critical media channels.
- Attempts to modify legislation, which occurred amidst citizen protests and resembled a law similar to those in Russia.
- Restoration of flights and deepening of trade relations with Russia.

Therefore, it is crucial for Georgia's foreign policy to align closely with the EU's common foreign and security policy to enhance the effectiveness of its European integration process. On the one hand, the task is for the country to receive the status of a candidate for the European Union, and on the other hand, the intensifying competition among major global powers and the ongoing war in Europe should serve as a window of opportunity for Georgia to draw nearer to the West.

References

Georgia's (mis)alignment with the EU Foreign Policy (2023). URL: <https://civil.ge/archives/542831>

საქართველოს პრემიერ-მინისტრი ყატარის ფორუმზე (2023). URL: <https://www.radiotavisupleba.ge/a/32425557.html>

ჩეხეთის ელჩი საქართველოს ევროკავშირში გაწევრიანების კრიტერიუმებზე (2022). URL: <https://www.interpressnews.ge/en/article/120799-petr-mikyska-we-dont-want-to-see-georgia-in-war-the-population-of-georgia-can-be-calm-in-a-sense-that-there-is-no-condition-that-georgia-must-enter-into-the-war-with-russia-to-get-eu-candidate-status>

EU-ს საგარეო პოლიტიკასთან თანხვედრა, როგორც დამატებითი კრიტერიუმი (2023). URL: <https://netgazeti.ge/life/651363/?fbclid=IwAR3tMgYPk8WQrspoJxFsZGEUg10GDiLLgexo3jsGH1U0oomLk-q8xICeyDI>

EU-ის წევრობის კანდიდატის სტატუსის საბოჟატი. (2023). URL: <https://netgazeti.ge/life/655677>

What is EU Foreign Policy. URL: https://www.eumm.eu/en/eu_in_georgia/what_is_eu_foreign_policy

Вовченко Олексій Вікторович
*Державний торговельно-економічний університет,
м. Київ, Україна*

КОНТРОЛЬ ЗА ІНОЗЕМНИМИ СУБСИДІЯМИ ЯК ФАКТОР РЕГІОНАЛЬНОЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

Внутрішній ринок Європейського Союзу вважається одним із найпривабливіших місць для іноземних інвестицій та діяльності компаній з інших країн. Коли іноземні компанії отримують доступ до цього ринку, вони можуть користуватися різними перевагами, такими як вільний обіг товарів і послуг.

Проте, в останні роки стала актуальною проблема субсидування компаній, які діють на внутрішньому ринку ЄС, третіми країнами. Наприклад, Китай надає значну фінансову підтримку своїм підприємствам і їхнім дочірнім компаніям, які діють в ЄС. Якщо такі субсидії були б надані державою-членом ЄС, вони б розглядалися як державна допомога, і їхнє надання підпадало б під правила державної допомоги ЄС.

Однак, правила державної допомоги не застосовуються до фінансових внесків, отриманих від третіх країн. Тобто іноземні субсидії можуть створювати нерівні умови для гри на внутрішньому ринку: компанії, які отримують фінансову підтримку від держав ЄС, повинні дотримуватися правил державної допомоги, тоді як компанії, які отримують субсидії від третіх країн, не підпадають під ці правила. Таким чином, останні мають значну конкурентну перевагу перед компаніями ЄС у своїй економічній діяльності на внутрішньому ринку ЄС.

Європейська Комісія спостерігає за тим, як іноземні субсидії впливають на внутрішній ринок ЄС і призводять до спотворення конкуренції у рамках ЄС. Для регулювання цієї ситуації Комісія розробила новий інструмент контролю за іноземними субсидіями, а саме Регламент № 2022/2560 про іноземні субсидії,

що спотворюють внутрішній ринок, який вступив в силу 12 липня 2023 року. Цей інструмент дозволить Комісії розслідувати характер субсидій, наданих третіми країнами підприємствам, які діють на внутрішньому ринку ЄС, і вживати заходів, якщо виявиться, що ці субсидії спотворюють ринок. Тобто, це означає, що іноземні субсидії повинні дотримуватися принципів, подібних тим, які існують в системі державної допомоги ЄС, щоб забезпечити рівні умови для конкуренції.

Важливість Регламенту № 2022/2560 полягає також у тому, щоб врахувати міжнародні зобов'язання ЄС в рамках СОТ і уникнути будь-якої дискримінації. Таким чином, ЄС спрямовує зусилля на створення ефективних і справедливих правил щодо іноземних субсидій, щоб забезпечити справедливую конкуренцію на внутрішньому ринку ЄС, аналогічно до того, як це регулюється в рамках системи державної допомоги ЄС.

Відповідно до Регламенту № 2022/2560 іноземною субсидією, вважається така, що надана урядом країни, яка не входить до ЄС, якщо такий уряд брав участь у прийнятті рішення про надання субсидії, незалежно від того, чи була субсидія надана державною чи приватною організацією (Regulation (EU) 2022/2560, 2022).

Таким чином, під дію Регламенту № 2022/2560 підпадають іноземні субсидії надані третіми країнами, які відповідають наступним критеріям:

– у разі операцій злиття та поглинання підприємства, коли одне з підприємств, що зливаються, мета або спільне підприємство створюється в ЄС і генерує оборот ЄС у розмірі 500 мільйонів євро, а сторони отримали за останні три роки фінансові внески у розмірі 50 мільйонів євро (Regulation (EU) 2022/2560, art. 20, par. 3).

– у разі державних закупівель, якщо вартість контракту перевищує 250 мільйонів євро (125 мільйонів євро за окремий лот) та учасник тендеру отримав за останні три роки фінансування іноземної держави, що перевищує 4 мільйони євро (Regulation (EU) 2022/2560, art. 27, par. 2).

Отже, Регламент № 2022/2560 регулює такі види іноземних субсидій, які дійсно несуть загрозу безпеці внутрішньому ринку ЄС, шляхом витіснення із конкурентного ринку суб'єктів

господарювання, які діють у рамках внутрішнього права ЄС та є незалежними від коштів наданих третіми країнами.

Однією з країн, яка наразі створює небезпеку для внутрішнього ринку ЄС є Китайська Народна Республіка. За останні 11 років відбулися важливі придбання підприємств ЄС китайськими інвесторами, що фінансуються урядом, такі як інвестиції в португальську електромережу в 2012 році, придбання компанії *Pirelli* компанією *ChemChina* в 2015 році (*Deutsche Welle*, 2015) або продаж компанії *Logicor* Китайській інвестиційній корпорації в 2017 році (*LDaily*, 2017), придбання 57% порту Пірей (*LB.ua*, 2016) і нещодавнє придбання 24,9% порту Гамбург китайським гігантом *China Ocean Shipping Company (COSCO)* (*Arne Delfs; Josefine Fokuhl*, 2022)

Окрім цього, нещодавно компетентні органи ЄС заявили, що китайські електромобілі чинять тиск на європейських автовиробників, змушуючи їх виробляти недорогі електромобілі. Влада ЄС вважає, що ціна китайських електромобілів на європейському ринку приблизно на 20% дешевша за місцеві моделі. Це також дозволило китайським електромобілям зайняти 8% європейського ринку. За оцінками експертів, ця цифра ймовірно збільшиться до 15% до 2025 року, якщо компетентними органами не буде вжито розумних заходів (*Philip Blenkinsop*, 2023).

Зважаючи на це, Європейська комісія розпочала вивчення питання про те, чи варто запроваджувати штрафні тарифи на імпорт китайських електромобілів, щоб захистити автовиробників Європейського Союзу. Дослідження було розпочато через побоювання, що китайські електромобілі чинять тиск на європейських автовиробників. Європейська комісія вважає, що деякі китайські бренди отримують вигоду від субсидій, які надає китайський уряд.

Таким чином, контроль за іноземними субсидіями в рамках ЄС є важливим чинником підтримання економічної безпеки у регіоні, що у подальшому призведе до: по-перше, зміцнення конкурентноспроможності європейських виробників, що діють відповідно до законодавства ЄС та, по-друге, виключить загрозу дестабілізації внутрішніх ринків ЄС з боку третіх країн.

Література

Delfs, A., Fokuhl, J. (2022). Hamburg Port to Sell Stake to China's Cosco After Scholz's Push. *Bloomberg*. URL: <https://www.bloomberg.com/news/articles/2022-10-26/germany-agrees-on-24-9-sale-of-hamburg-terminal-to-cosco>.

ChemChina wants Italy's Pirelli (2015). *Deutsche Welle*. URL: <https://www.dw.com/en/chemchina-to-buy-italys-pirelli/a-18333555>.

Greece sold the port of Piraeus to the Chinese (2016). *LB.ua*. URL: https://lb.ua/world/2016/07/01/339078_greysiya_prodalala_kitayt_sam_port_pirey.html.

Philip Blenkinsop. EU to investigate 'flood' of Chinese electric cars, weigh tariffs (2023). *Reuters*. URL: <https://www.reuters.com/world/europe/eu-launches-anti-subsidy-investigation-into-chinese-electric-vehicles-2023-09-13/>.

Regulation (EU) 2022/2560 of the European Parliament and of the Council of 14 December 2022 on foreign subsidies distorting the internal market (2022). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2560>.

The sale of the logistics operator Logisor claims the status of the most expensive deal in the history of the entire industry (2017). *LDaily*. URL: <https://ldaily.ua/news/novosti/prodazha-logisticheskogo-operatora-logisor-pretenduet-na-status-naibolee-dorogostoyashhejsdelki-vo-vsej-istorii-otrasli>.

Мацишина Ірина Віталіївна

*доктор політичних наук, професор,
професор кафедри політології та державного управління,
Донецький національний університет імені Василя Стуса,
м. Вінниця, Україна*

ORCID: 0000-0002-2988-620X

ДО ПОНЯТТЯ МОРАЛІ ПОЛІТИЧНОГО РЕАЛІЗМУ В УМОВАХ ВІЙНИ

Стародавні римляни говорили, що «коли гримить зброя, закони мовчать». Тут моральний абсолютизм поступається місцем контекстуальної моралі, коли в схожих ситуаціях країни можуть надавати різну моральну оцінку діям агресора. Що вказує на домінування власних інтересів кожної країни у зовнішній політиці та актуалізації теорії політичного реалізму. Так в умовах широкомасштабної війни Росії проти України, міжнародна спільнота демонструє певні розбіжності в ставленні до цієї війни та у розумінні, що буде зі світом після її закінчення. Якщо для одних дослідників українська *перемога* має стати зміною світового геополітичного ландшафту (Український інститут національної пам'яті), то для інших встановлення миру може зупинити мілітаризацію європейської та американської зовнішньої політики (Meduza; NEWS IN RUSSIAN). На заяву Ноама Хомського щодо того, що «Україні вкрай необхідна мирна угода за умови поступок з обох сторін», українські вчені-економісти вимушені були написати відкритий лист щодо маніпуляційних тез вченого на кшталт «неактуальності питання Криму», «США підбурює українців воювати проти Росії», «Росії загрожує НАТО» тощо (Вокс Україна). Ці дві позиції апелюють до питання морального права в умовах війни, що надає можливість звернутися до теорії політичного реалізму сучасних дослідників.

Роберт Шютт наполягає на критичному обговоренні теорії політичного реалізму та пропонує його більше розглядати як *реалізм відкритого суспільства*. «Під реалізмом відкритого

суспільства я маю на увазі політичне бачення влади та інтересів, яке стосується ліберальних ідей через закон» (Schuett). Відхиляючи поняття моралі, яке корегується з власними національними інтересами у політичному реалізмі і може заперечувати загальну етичну нормативність моралі, вчений більше концентрується на лідерській дипломатії. Саме там він шукає спільне між раціональною зовнішньою політикою та відкритим суспільством. Шютт висуває три причини про важливість критичного дослідження політичного реалізму.

Перша причина – відродження інтересу до реалістичного політичного мислення за останні два десятиліття. Дійсно, ідеологія споживання та розвиток цифрових технологій створюють раціональне ставлення до політичного вибору. Політична поведінка як виборців, так і політиків, все більше спирається на популізм, як необхідну складову публічності. Теорія раціонального вибору сьогодні не працює, як і емоційна складова під час політичних рішень. Немає гарантії від помилок, прогнозування ризиків та втрат від політичних рішень. Як суб'єкта, так і об'єкта політики.

Друга причина – існує серйозна потреба у збалансованому класичному реалізмі, оскільки він виходить за межі свого традиційного розуміння та існує ризик його підміни. Особливо, коли йде загроза існуванню відкритого суспільства. «Коли впевненість влади та дипломатії поступається місцем чомусь ще невизначеному» (Schuett). Достатньо згадати Р.Трампа, якого більшість американського суспільства підтримала на президентських виборах саме за його радикальну програму: заборона на в'їзд мусульман, будівництво стіни уздовж мексиканського кордону, депортація всіх нелегальних мігрантів, позбавлення видатків на НАТО тощо (BBC). З часом з'ясувалося, що жоден з цих пунктів його програми не був до кінця виконаний.

Третя причина – загроза втрати критичного способу політичного мислення, оскільки стандартні пояснення реалізму у більшості сприймаються як неетичне безвідповідальне мислення, з обмеженою ідеологією виживання. «Це небезпечний міф про закрите суспільство, прикритий мовою романтизму

«шміттівського друга проти ворога», – пише Р.Шютт (Schuett). Тому теорія політичного реалізму, як реалізм інтересів конкретного суб'єкта та власних інтересів країни, сьогодні виходить за межі дипломатії.

Аналізуючи Р. Шютта та його концепцію реалізму відкритого суспільства, можна сказати що він пропонує певний інструментарій як бути реальними та бути моральними одночасно. Оскільки реальна політика має певну межу між цими поняттями, Шютт пропонує певний інструментарій між ідеєю та реальністю. Як можна жити та прагнути ідеалу, залишаючись в той час у реальному розумінні політичних подій та їхніх наслідків. На його думку, основою розвитку реалізму відкритого суспільства є реалістична та нормативна концепція держави. «Це реалізм людської природи, який стверджує, що ти і я однакові, і що для мирного спільного життя нам потрібні примусові елементи влади та закону» (Schuett). Він поєднує поняття «держави» та поняття «право», що не виключає національного інтересу у реалізмі, а доповнює його моральним правом. Його відмінність від теорії політичного реалізму Моргентгау полягає в тому, що правовий механізм є набагато складніше за національні інтереси, проте, він акцентується на нормі морального права як формі національного інтересу.

Тут мова йде не про абстрактну спекулятивність права, що ставиться на місто держави, а про продовження постмодерністських практик пошуку моралі в умовах війни для нації. Адріан Кройтц використовує поняття «метанормативності». Коли політична нормативність переважає моральну нормативність. І хоча окреслити джерела метанормативності вченому не вдається (Kreutz), можна припустити, що метанормативність є загальною ідеологічною моральною нормою для держави в цілому. Особливо, коли мова йде про збереження територіальної цілісності.

Ірландський вчений Сініша Малешевич, повертаючись до війни в Україні, вказує на відсутність морального абсолютизму у політичних конфліктах. «По-перше, надзвичайно непередбачуваний та мінливий характер військового середовища не допускає моральних абсолютів», – пише дослідник (Malešević).

Непередбачуваність та невизначеність не можуть надати моральної впевненості у військових конфліктах, проте, організаційна спроможність спротиву до агресора значно впливає на результат війни. І тут право на захист своєї території утворює структури моральної норми у відповідності до національних інтересів. Вчений пише, що армії воюють не для того, щоб захоплювати землю та вбивати мирних жителів, а в першу чергу, щоб зламати опір. «Незважаючи на значно більшу армію та більше озброєння, російські війська зазнали величезних втрат і не змогли контролювати багато територій, які вони окупували під час першої хвилі свого нападу. Таким чином, рішення про надання військової підтримки Україні також може ґрунтуватися на вагомих доказах того, що українські військові мають потужну організаційну спроможність відвоювати та контролювати території, які були окуповані російськими військовими. Надаючи більшу допомогу українським військовим, їх організаційна спроможність може продовжувати зростати до такого рівня, коли вони зможуть перемогти сили вторгнення та, зрештою, зупинити війну» (Malešević).

Ще одним аргументом на захист перемоги України у війні Малешевич бачить у солідарності за межами поля бою. Мікрорівень соціальної згуртованості посилюється взаємними моральними зобов'язаннями комбатантів та цивільними. «Таким чином, військова ефективність значною мірою залежить від здатності армії ідеологічно охоплювати мережі мікросолідарності та інтегрувати їх у ширші організаційні структури» (Malešević). Малешевич посилається на досвід хорватської армії під час війни у Югославії, коли координація мереж солідарності на макрорівні з широкими організаційними структурами допомогла повернути окуповані території. Таким чином, військова підтримка матиме значення у моральних контекстах солідарності. Коли національні інтереси є домінуючою формою солідарності, національні держави стають легітимною формою нормативної моралі.

Література

Відкритий лист Ноаму Хомському (та іншим однодумцям-інтелектуалам) щодо російсько-української війни (2022, 20 травня). *Вокс Україна*. URL: <https://voxukraine.org/vidkrytyj-lyst-noamu->

homskom-ua-inshym-odnodumtsyam-intelektualam-shhodo-rosijsko-ukrayinskoyi-vijny

Timothy Snyder: Why the Ukrainian Victory is Important for the World? (2022, 08 травня). *Український інститут національної пам'яті*. URL: <https://uinp.gov.ua/informaciyni-materialy/rosijsko-ukrayinska-viy-na-istorychnyy-kontekst/dr-timothy-snyder-why-the-ukrainian-victory-is-important-for-the-world>

Чи дотримався Трамп обіцянок, які дав під час передвиборчої кампанії? (2019, 20 січня). *BBC*. URL: <https://www.bbc.com/ukrainian/features-46937839>

Kreutz, A. (2023). Realism and metanormativity. *Inquiry*, 1-29. <https://doi.org/10.1080/0020174X.2023.2185907>

Malešević, S. (2023). The moral fog of war and historical sociology. *European Journal of Social Theory*. <https://doi.org/10.1177/13684310231165218>

«Те, хто дає зброю Україні, повинні розуміти – на кону життя не тільки українців, але й всіх інших» Інтерв'ю Ноама Хомського (2022, 21 липня). *Meduza*. URL: <https://meduza.io/feature/2022/07/21/te-kto-dayut-oruzhie-ukraine-dolzheny-ponimat-na-konu-zhizni-ne-tolko-ukraintsev-no-i-vseh-ostalnih>

Ноам Хомський: «Сказати «давайте продовжимо війну» – це сказати «давайте розрушимо світ, бо ми хочемо зробити вигляд, що у нас є принципи» (2022, 19 липня). *NEWS IN RUSSIAN*. URL: <https://expresso.pt/news-in-russian/2022-07-19-----2367abb9>

Schuett, R. (2022). The End of Open Society Realism? *Analyse & Kritik*, (44.2), 219-242. <https://doi.org/10.1177/0952695107082491>

Райков Артур Ернстович

*Навчально-науковий інститут міжнародних відносин,
Київського національного університету ім. Т. Шевченка,
м. Київ, Україна*

ВІЙНА В НАГІРНОМУ КАРАБАХУ ЯК ЧИННИК ГЕОПОЛІТИЧНИХ ЗМІН У РЕГІОНІ ПІВДЕННОГО КАВКАЗУ

Напередодні цьогорічної одноденної війни в Нагірному Карабаху ситуація в регіоні почала свій рух у бік великої кризи, яка мала б переформатувати положення регіональних та глобальних акторів міжнародних відносин на Південному Кавказі.

Результати Другої Карабаської війни 2020 року лише на деякий час зафіксували позиції сторін конфлікту та зовнішніх гравців. Азербайджан, хоч і одержав перемогу, був явно не задоволений, що не повністю контролював сепаратистське утворення. Поразка вірменських військ сколихнула внутрішньополітичну ситуацію у Вірменії, через що прем'єр-міністр Нікол Пашинян ледь не втратив свій пост, а сама країна та її населення почали відчувати сильну фрустрацію через невдалу військову кампанію (Roth, 2020). Сама ж Нагірно-Карабаська Республіка (НКР) фактично опинилася відірваною від Вірменії, оскільки територію довкола неї зайняли азербайджанські війська. Єдиним сполученням між НКР та Вірменією залишався Лачинський коридор, який, згідно з заявою президента Азербайджанської Республіки, прем'єр-міністра Республіки Вірменія та президента Російської Федерації, мав бути під контролем російських миротворців (Statement by President of the Republic of Azerbaijan, Prime Minister of the Republic of Armenia and President of the Russian Federation, 2020).

Угода про перемир'я законсервувала присутність російських військ в Карабаху (Statement by President of the Republic of Azerbaijan, Prime Minister of the Republic of Armenia and President

of the Russian Federation, 2020) і, що цікаво, посилила вплив РФ на офіційний Єреван.

Друга Карабаська війна виявилася проміжним етапом до подій вересня 2023 року. Жодна зі сторін не була близька ані до провалу, ані до реальної перемоги. Тому наприкінці 2022 року закономірною стала поява перших передумов нової конфронтації в регіоні.

Оскільки Росія зав'язла у війні проти України, відчувала і далі відчуває брак ресурсів, можливостей і часу на підтримку інтересів в інших регіонах, її вплив на процеси в Нагірному Карабаху ослабнув. Це відкрило для офіційного Баку поле для реалізації свого плану щодо відновлення контролю над Карабахом.

Для азербайджанського президента Ільхама Алієва було необхідно змінити ситуацію в регіоні на свою користь, тому що збереження статусу-кво 2020 року ставило під сумнів легітимність його влади, оскільки перемога у Другій Карабаській війні не була повноцінною (Куса, 2023). Восени 2022 року Азербайджан почав провокації на кордоні з Вірменією. Була реальна ймовірність переростання прикордонного конфлікту у нову війну з окупацією вже території Вірменії. У грудні того ж року Азербайджан розмістив блокпости в Лачинському коридорі, тим самим взявши у блокаду Нагірний Карабах (Krivosheev, 2023a).

Можна виділити дві цілі, які переслідував Азербайджан. По-перше, тиснути на Вірменію заради підписання мирного договору на азербайджанських умовах. По-друге, змусити карабаських вірмен йти на прямі переговори, часом ультимативні. Алієву необхідно було поставити крапку у конфлікті. Азербайджан намагався як у переговорами, так і зброєю нав'язати вірменам свої умови: від закріплення кордону між Вірменією та Азербайджаном до повної ліквідації будь-якої автономії в Нагірному Карабаху (De Waal, 2023).

На фоні збройних провокацій Азербайджану та блокади НКР інтенсивними були переговори між Азербайджаном і Вірменією. Головним чином посередниками у цьому процесі були РФ як гарант перемир'я та ЄС, на якого мали високі очікування в Єревані, вважаючи, що участь європейців укріпить позицію Вірменії (Krivosheev, 2023a). Інколи у переговори вступали

і Сполучені Штати (De Waal, 2023). Однак все ж таки конкуренція за головного медіатора була між РФ та ЄС.

З часом Росія не проявляла якоїсь сильної активності у примиренні двох держав. Є дві версії, чому ж Росія перестала брати активну участь у посередництві. З одного боку, це може бути наслідком агресії РФ проти України. Росія зав'язла у війні проти України, яка відтягує значну кількість ресурсів, часу і уваги. Тому можливостей займатися Південним Кавказом усе менше. З іншого боку, пасивність Росії, а часом і гра на користь Азербайджану (хоча Вірменія і РФ є союзниками в рамках ОДКБ), може говорити про кулуарні домовленості між офіційними Москвою і Баку (De Waal, 2023). Дуже дивно виглядало, коли російські миротворці не реагували на провокації азербайджанської армії, хоча б мали припиняти їх.

Піком нестабільності в регіоні став новий збройний конфлікт, ініційований Азербайджаном. Він протривав одну добу: уже 20 вересня 2023 року оголосили, що НКР погоджується на умови Азербайджану і буде розпущена (Gavin, 2023).

Які наслідки для країн регіону та глобальних акторів після перемоги Азербайджану? Для Азербайджану це завершення 30-річної проблеми сепаратизму та відновлення територіальної цілісності і суверенітету. Це стало для Ільхама Алієва шансом увійти в історію на рівні зі своїм батьком Гейдаром Алієвим. Перемога у війні дозволить Алієву укріпити владу, однак, імовірно, це буде йти паралельно з посиленням автократії. Також варто згадати і про карабаських вірмен, які почали масово покидати рідні домівки та їхати до Вірменії. Для Азербайджану це може бути вигідним, оскільки а) не потрібно домовлятися про їхній особливий статус, б) вільний виїзд карабаських вірмен нівелює можливість звинувачень офіційного Баку в етнічних чистках (Krivosheev, 2023b).

Тягар у вигляді підтримки НКР заважав Вірменії досягти порозуміння з сусідами. Визнання територіальної цілісності Азербайджану з боку Пашиняна відкриває дорогу до підписання мирного договору між країнами, а також до потенційної нормалізації відносин з Туреччиною, що може допомогти Вірменії в економічному плані. Паралельно виникає проблема з розміщенням 100 тисяч карабаських біженців (Krivosheev,

2023b). Мала в демографічному і економічному плані Вірменія стикнеться з проблемою інтеграції біженців, яким необхідно створити умови проживання та адаптації. Фрустрація і зневіра можуть спонукати карабаських вірмен приєднуватися до антиурядових акцій, що ще сильніше вдарить по внутрішньополітичній ситуації у країні. Однак не варто виключати, що частина карабаських вірмен може повернутися додому, якщо у мирному договорі між Вірменією та Азербайджаном буде включений пункт про їхній статус.

Не варто очікувати революційних зрушень у питанні підписання мирного договору між Вірменією та Азербайджаном. Певно, це буде рамковий документ, який зафіксує першочергові питання, як визначення кордонів та відновлення відносин (Krivosheev, 2023b). Однак далі вже виникатимуть додаткові питання і проблеми, наприклад, чи буде Азербайджан розбудовувати «Зангезурський коридор» (який проходить територією Вірменії) для сполучення з Нахічеванню, чи все ж таки відмовиться від цього проєкту.

РФ втратила позиції в регіоні. Без існування НКР немає місця її миротворчій місії. Відсутність реакції Росії на збройні провокації Азербайджану та відсутність підтримки з боку ОДКБ призвели до того, що Вірменія почала шукати нових партнерів. Критика Пашиняна щодо бездіяльності РФ вже призвела до погіршення відносин з РФ. Натомість зацікавленість до кооперації з Вірменією проявляють США та Франція. США провели спільні військові навчання (Garver, 2023), а Франція погодилася поставити Вірменії озброєння (Kavali, 2023). Влив РФ на політику Вірменії також зменшився. Під питанням тепер будуть стояти військова база РФ в Гюмрі, участь Вірменії в ОДКБ, а ратифікація Вірменією Римського статуту МКС ще більше погіршить відносини між Пашиняном і Путіним, на якого МКС видав ордер на арешт за депортацію українських дітей (International Criminal Court, 2023).

Перемога Азербайджану та завершення історії НКР ще не говорять про мир у регіоні. Нові раунди переговорів між офіційними Баку і Єреваном можуть знову розпалити конфронтації між державами, що також може загострити внутрішні протистояння в країнах, особливо у Вірменії.

Література

Roth, A. (11.11.2020). 'Nikol is a traitor': Armenia PM refuses to yield to opposition after Nagorno-Karabakh deal. *The Guardian*. <https://www.theguardian.com/world/2020/nov/11/nikol-is-a-traitor-armenia-pm-refuses-to-yield-to-opposition-after-nagorno-karabakh-deal>

Statement by President of the Republic of Azerbaijan, Prime Minister of the Republic of Armenia and President of the Russian Federation 2020 (President of Russia). URL: <http://en.kremlin.ru/events/president/news/64384>

Куса, И. (17.09.2023). Третья карабахская война: В чем логика обострения между Арменией и Азербайджаном? *Хвиля*. URL: <https://hvylya.net/analytics/279496-tretya-karabahskaya-voyna-v-chem-logika-obostreniya-mezhdu-armeniyey-i-azerbaydzhanom>

Krivosheev, K. (16.02.2023a). Could the new EU mission sideline Russia in Armenia-Azerbaijan settlement? *Carnegie Endowment for International Peace*. URL: <https://carnegieendowment.org/politika/89060>

De Waal, T. (09.08.2023). Armenia, Azerbaijan on the brink – again. *Engelsberg ideas*. URL: <https://engelsbergideas.com/notebook/armenia-azerbaijan-on-the-brink-again>

Gavin, G. (28.09.2023). Azerbaijan officially dissolves Nagorno-Karabakh. *POLITICO*. URL: <https://www.politico.eu/article/nagorno-karabakh-dissolved-azerbaijan-armenia-de-facto-president-samvel-shakhramanyan>

Krivosheev, K. (29.09.2023b). What the dissolution of Nagorno-Karabakh means for the South Caucasus. *Carnegie Endowment for International Peace*. URL: <https://carnegieendowment.org/politika/90667>.

Garver, R. (11.09.2023). US troops' arrival in Armenia for training riles Russia. *Voice of America*. URL: <https://www.voanews.com/a/us-troops-arrival-in-armenia-for-training-riles-russia/7264316.html>

Kayali, L. (4.10.2023). France will send military gear to Armenia. *POLITICO*. URL: <https://www.politico.eu/article/france-will-send-military-equipment-to-armenia/>.

Situation in Ukraine: ICC judges issue arrest warrants against Vladimir Vladimirovich Putin and Maria Alekseyevna Lvova-Belova (17.03.2023). *International Criminal Court*. URL: <https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and>

Ціватий Вячеслав Григорович
*кандидат історичних наук, доцент,
Заслужений працівник освіти України,
Київський національний університет імені Тараса Шевченка,
ORCID: 0000-0003-1505-7483*

КОНЦЕПТ «КРИЗОВА ДИПЛОМАТІЯ» І РЕГІОНАЛЬНА БЕЗПЕКА В УМОВАХ ТРАНСФОРМАЦІЇ СИСТЕМИ МІЖНАРОДНИХ ВІДНОСИН ХХІ СТОЛІТТЯ: ГЕОПОЛІТИЧНИЙ, ІНФОРМАЦІЙНО- КОМУНІКАЦІЙНИЙ ТА ІНСТИТУЦІОНАЛЬНИЙ ДИСКУРСИ

В умовах сьогодення особливо актуалізується питання дослідження особливостей теорії та практики дипломатії, її інформаційно-аналітичного забезпечення, зокрема – практичної дипломатії у сфері регіональної безпеки, інформаційно-політичної безпеки, міжнародно-політичних переговорів, політичної комунікації в поліцентричному (постбіполярному, багатополосному) світі ХХІ століття (Ціватий, 2022, С. 274–278).

Проблеми забезпечення та ефективного функціонування системи регіональної безпеки та системи національної безпеки держави на сьогодні є особливо актуальними для більшості держав світу в умовах поліцентричного (постбіполярного, багатополарного) світоустрою ХХІ століття. Особливо актуалізуються питання інформаційно-аналітичної діяльності та моделювання у сфері міжнародних відносин, зокрема – моделювання безпекових стратегій національних держав.

В умовах зростання міжнародно-політичної нестабільності у світі, підвищеної політичної конфліктогенності у світовому геополітичному просторі та повномасштабного вторгнення росії в Україну – постають нові виклики й загрози міжнародній безпеці в енергетичній, інформаційній, а особливо – у війсьній сферах. Дипломатія переорієнтовується на нові напрями діяльності

в умовах воєнного стану: культурна дипломатія, публічна дипломатія, кризова дипломатія.

Наукове обґрунтування і концептуалізація таких соціальних регуляторів сучасного світоустрою, як право, дипломатія, політика, міжнародна безпека – це новий перспективний напрям досліджень у сфері міжнародних відносин, і перш за все – у контексті світових інтеграційних та дезінтеграційних процесів, аналітично-інформаційного забезпечення зовнішньополітичних і дипломатичних практик в умовах поліцентричного світоустрою XXI століття (Tsviaty, 2017, Р. 16–26).

Одним із нових напрямів у теорії дипломатії та теорії міжнародних відносин на сьогодні є – кризова дипломатія (*disaster diplomacy*), модель кризової дипломатії та інституціональна політична безпека (Ritzer, Dean, 2019). Одним із об'єднувачих інституціональних векторів у світовій політиці є дипломатія, кризова дипломатія (*disaster diplomacy*) і міжнародно-політичні переговори як засіб нейтралізації конфліктогенних чинників та інструментарій урегулювання політичних, воєнних і політико-дипломатичних конфліктів XXI століття. Важливою складовою інституціоналізації цього процесу є створення відповідних антикризових аналітичних центрів («мозкових центрів») (Bassan, 2021).

Поняття гібридної війни виявилось теоретично й практично найбільш придатним для визначення характеру російсько-української війни 2022 року. Для опору й стримування агресора Україна разом з її міжнародними партнерами демонструє модель кризової дипломатії та модель політичної безпеки, чітке розуміння природи й характеру цієї війни. Гібридну війну в загальному вигляді розуміють як воєнні дії, що здійснюються шляхом поєднання мілітарних, квазімілітарних, дипломатичних, інформаційних, економічних та інших засобів з метою досягнення стратегічних політичних цілей. Специфіка такого поєднання полягає в тому, що кожний з військових і невійськових способів ведення гібридної війни застосовується у воєнних цілях і використовується як зброя (Перепелиця, 2003).

Перетворення на зброю (*weaponization*) відбувається не тільки в медійній та інформаційно-комунікативній сфері. Теорія

дипломатії та теорія міжнародних відносин XXI століття активно досліджує їх базову аксіоматику, здійснює типологічний аналіз воєн і конфліктів, причинно-наслідкову обумовленість воєн і міжнародно-політичних конфліктів, технології їх урегулювання, зокрема – моделі переговорного процесу, їх динаміку та управління конфліктами в умовах глобалізованого світоустрою та історичній ретроспективі (інституціональна політична конфліктологія) (Tsivaty, 2017, P. 16–26).

Гібридні конфлікти і гібридні загрози на сьогодні розглядають як важливу характеристику міжнародного безпекового довкілля і сучасної системи міжнародних відносин, що перебуває в стані системної кризи. Ситуація ведення бойових дій не позбавляє від потреби вирішення теоретичних питань, уважати так було б драматичною помилкою, оскільки в умовах війни правильна оцінка сутності воєнних явищ безпосередньо пов'язана з розробкою та перевіркою на практиці засобів оборони, захисту від агресії.

Для України на сьогодні це питання є ключовим. Новими теоретико-методологічними пріоритетами для моделювання конфліктів у сфері теорії дипломатії, зовнішньої політики і міжнародних відносин повинні стати – концепції теорії систем і системного аналізу, загальної теорії управління і кібернетики, синергетики, інформаційних технологій і логіколінгвістики, теорії хаосу й активних систем, діаспориальна аксіоматика (Марутян, 2022, С. 270-283).

Нові тенденції в розвитку сучасних політичних і політико-дипломатичних конфліктів вимагають і нових ефективних методів вивчення цих конфліктів на основі математичних, структурно-логічних, кібернетичних і імітаційно-комп'ютерних, історико-компаративних підходів. Політичні конфлікти сучасності – це клас (інституційний кластер) соціальних конфліктів. Політичні конфлікти відбуваються в соціальній сфері. Важливою рисою політичних і політико-дипломатичних конфліктів, в умовах трансформації сучасних міжнародних відносин, є використання для їх вирішення як силових, так і несилових способів. У першому випадку вони балансують на межі переходу у військові, у другому – найчастіше набувають юридичного (правового), договірної забарвлення.

У нових геополітичних умовах ХХІ століття, в умовах поліцентричної (багатополусною) моделі світоустрою, теорія і практика глобальної дипломатії, теорія зовнішньої політики і теорія міжнародних відносин акцентують свою дослідницьку парадигму на нових підходах у дослідженні політичних конфліктів та воєн – на основі використання сучасних методів математичного та комп'ютерного моделювання. Поряд з традиційними підходами до вивчення, моделювання та аналізу політичних конфліктів слід залучати і нові підходи: використовувати останні досягнення в області природознавства, математики, інформатизації та комп'ютеризації тощо. Публічна дипломатія та політика «м'якої сили» є одним із засобів реалізації зовнішньополітичної стратегії для будь-якої держави, що претендує на значиму роль у системі міжнародних відносин ХХІ ст. і реаліях підвищеної світової політичної конфліктогенності міждержавних відносин. З наданням міжнародної допомоги пов'язаний і особливий спосіб просування «м'якої сили» держави – кризова дипломатія (*disaster diplomacy*). Конфліктогенні чинники, тренди хаотизації та упорядкування мають свій вияв у всіх сферах міжнародних відносин, зовнішньої політики та дипломатії, з'являється новий дипломатичний інструментарій та моделі дипломатії (Weimann, 2004).

Отже, феномен гібридної війни має два головні модули існування – матеріальний (фізичний) і дискурсивний. Постановка проблеми кризової дипломатії (*disaster diplomacy*), інституціоналізації конфліктів, політичної безпеки, гібридних воєн та інституціональних механізмів їх урегулювання в сучасній міжнародній політико-дипломатичній системі є новою для історико-політологічних і політико-правових досліджень, що відтак вимагає застосування системного аналізу та відповідної термінології, яка необхідна для виконання наукових завдань. Модель кризової дипломатії, кризова дипломатія (*disaster diplomacy*), антикризові аналітичні центри («мозкові центри»), антикризові комунікації – є на сьогодні одним із нових напрямів у теорії дипломатії та теорії міжнародних відносин.

Ефективність управління у сфері міжнародних відносин, зовнішньої політики і дипломатії багато в чому визначають прийняття і реалізацію управлінських рішень, заснованих на

результативності використання сучасних інформаційних і комунікаційних технологій, зокрема – і у контексті моделювання міжнародних відносин і прогнозування зовнішньої політики держав, моделювання безпекових стратегій національних держав. Відповідно одержання, аналіз, видача й ефективне використання інформації – найважливіша умова ефективного забезпечення міжнародно-політичної, зовнішньополітичної діяльності України та впровадження ефективної моделі її дипломатії.

У напрямі інституціоналізації політичної конфліктології одним із об'єднавчих інституціональних векторів у світовій політиці є дипломатія, зокрема – кризова дипломатія (*disaster diplomacy*), як засіб нейтралізації конфліктогенних чинників та інструментарій урегулювання воєн, політичних і політико-дипломатичних конфліктів XXI століття ефективними засобами та інструментарієм кризової дипломатії (*disaster diplomacy*) та антикризової комунікації.

Література

Марутян, Р. Р. (2022) Воєнна фантастика як гуманітарна технологія гібридної війни. *Інформаційно-комунікаційна безпека: сучасні тренди*. Київ: Київський університет імені Б. Грінченка, 270–283.

Перепелиця, Г. М. (2003). *Конфлікти в посткомуністичній Європі*. Київ: ПЦ «Фоліант».

Ціватий, В.Г. (2022). Політика безпеки, гібридні війни і міжнародно-політичні переговори в теорії та практиці дипломатії: історико-інституціональний і політико-правовий дискурси. *Міжнародна безпека. Російсько-українська війна: право, безпека, світ*. Тернопіль: ЗУНУ, Західноукраїнський національний університет, V, 274–278.

Bassan, F. (2021). *Digital Platforms and Global Law*. Edward Elgar Publishing.

Ritzer, G., Dean, P. (2019). *Globalization: Conceptualization, Origins, and History*. 2nd ed. Oxford.

Tsivaty, V. (2017). National Security as a Component of Global Security: Lessons from Ukraine's Crises. *Eastern Europe Regional Studies*, 2 (4), 16–26.

Weimann, G. (2004). *Www.Terror.Net: How Modern Terrorism Uses the Internet*. Special Report. Washington, D. C.: U.S. Institute of Peace.

ОСНОВНІ СТРАТЕГІЧНІ НАПРЯМКИ КІБЕРБЕЗПЕКИ

Завгородня Юлія Володимирівна
кандидат політичних наук, доцент,
Національний університет «Одеська юридична академія»,
м. Одеса, Україна
ORCID: 0000-0003-3500-8638

ПОЛІТИЧНА КІБЕРКУЛЬТУРА ЯК ЕЛЕМЕНТ КІБЕРСТАБІЛЬНОСТІ

Політичні процеси у формі кіберпротиборств несуть суттєву небезпеку для стабільного функціонування кіберпростору та кібервзаємодії. Політична культура у кіберпросторі має стати одним із вагомих чинників щодо стабілізації процесів у кіберпросторі. З розвитком кіберможливостей відбувається розвиток кіберзагроз, які глобалізуються та стають небезпекою світового масштабу. Локальне врегулювання питань захисту кіберпростору не приносить ефективного результату, оскільки кіберпротиборство не має прив'язки до території, в той час як врегулювання проблемного питання нормативно обмежується межами території держави чи міжнародного об'єднання, котре по своєму принципу дії також обмежується межами країн учасниць.

Реальна політична дійсність фактично стирає межі кордонів держав, спираючись на цінність усіх націй, проте з метою ідентифікації народностей зберігається культура, як невід'ємний атрибут об'єднання людей по історичним, територіальним та біологічним ознакам. Для сучасних глобалізаційних процесів в політиці важливу роль повинна відігравати саме кіберкультура, як якісний атрибут поведінки та реалізації політичних дій у кіберпросторі.

В сучасному світосприйнятті поняття «кіберкультура» є міждисциплінарним поняттям, яке охоплює фундаментальні ознаки культури з використанням комунікацій та інформаційних технологій, які стрімко розвиваються та використовуються різними інститутами органів управління, як сучасний механізм у реалізації політичних рішень.

Так, на думку П.Леві під поняттям «кіберкультура» варто розуміти «набір методів (матеріальних та інтелектуальних), практик, підходів, способів мислення і цінностей в їх сукупному розвитку у кіберпросторі» (Lévy, 2001, P. 201). Думки автора направлені в більшій мірі на публікацію матеріалів в інформаційних ресурсах, їх авторській ідентичності. Якщо оцінювати кіберкультуру в політичних процесах, то це також використання певних методів, підходів щодо дій направлених на реалізації політичних інтересів в межах норм моралі та актуальних форм дипломатії та їх авторській політичній ідентичності.

Адже, специфіка політичної кіберкультури скоординована на дії суб'єктів політики, які вчиняють заходи направлени на досягнення політичних цілей (підвищення рейтингу, досягнення розвитку в якості впливового політичного діяча чи політичного оглядача/аналітика, вплив на політичного діяча в кіберпросторі з метою зниження його політичної ролі та ін.). Тому, підвищення рівня політичної кіберкультури сприятиме покращенню взаємодії суб'єктів політики в кіберпросторі. У зв'язку з цим, об'єднання націй навколо культурного чинника в кіберпросторі сприятиме з одного боку об'єднанню цінностей та зниженню рівня агресії, з іншого боку відсутності жорстких обмежень, які створюють умови закритого кіберпростору.

Тому, поведінка учасників політичної системи в інформаційному просторі є досить показовою та створює прецеденти до наслідування поведінки суб'єктів політики в кіберпросторі (Завгородня, 2022, С. 30). А кіберкультура створює певні умови для поведінки політичних діячів в кіберпросторі, їх популяризації, ефективності при політичних процесах та пришвидшенні політичної діяльності до викликів сучасності.

У зв'язку з науковими поглядами кіберкультура розвиває нову форму взаємодії, так звану «комунікативну мутацію», яка ґрунтується на:

- «новому режимі зв'язку, який не тільки є одним з аспектів сучасної культури, а й призводить до зміни семіотичних передумов самої культури;
- кіберкультурі - як дуже складній системі знаків, яка розподіляється симетрично і однорідно. При цьому кожен користувач більше не піддається ідентифікації по своєму відношенню до соціального прошарку. Кіберкультура передбачає «занурення»;
- кіберкультурі, яка надає можливість посилювати колективні мімічні і абстрактні реалії;
- кіберкультурі - як новому рівні семіотичної складності, безпрецедентному в історії людства» (Власенко, Левченко, 2019, С. 77).

Звичайно, такі елементи сприйняття кіберкультури демонструють здатність суспільства та суб'єктів політики швидко сприймати та практично реалізовувати на користь забезпечення своєї життєдіяльності як політичних діячів технології, нові знання, технічні засоби та інформаційні ресурси, які можна називати новітньою інформаційною культурою світу. Рівень розвитку такої культури, сприятиме важливим інтегральним показникам щодо рівня розвитку суспільства в глобальному сприйнятті інформаційного простору.

На думку Ф. Власенко та Є. Левченко «інформаційна культура являє собою комплексну характеристику особистісних, професійних якостей, що відповідають сучасним вимогам професійної діяльності, визначальним чинником якої виступає всебічна інформація та знання, що, в свою чергу, формують відповідну систему мислення та світорозуміння» (Власенко, Левченко, 2019, С. 78). Тому, показник рівня політичної кіберкультури це прояв професіоналізму політичних суб'єктів, їх цивілізованій діяльності в кіберпросторі та публічному відкритому обговоренні політичних процесів у формі конфліктів та кризових явищ.

Разом з тим, існуючі наукові концепції щодо поглядів на можливість розвитку кіберкультури виділяють можливість

існування утопічної форми сприйняття такого явища, що де мотивує усіх прибічників удосконалення взаємовідносин у кіберпросторі з розвитком потенційних можливостей. В такому аспекті аналізу кіберкультури перевага надається в більшій мірі розвитку кіберзагроз аніж кіберзахисту.

Звичайно тенденції інформаційного розвитку містять позитивні та негативні чинники, а тому кіберкультуру не потрібно ідеалізувати, як явище. Проте, оцінюючи лише негативні наслідки важко скоординувати позитивні складові діяльності кіберпроцесів, які використовуються політичними інститутами. Тому, з поміж позитивних напрямків варто визначити швидкість отримання політичної інформації, її використання та освідомлення політичних подій, доступність політичної інформації та вміння аналізувати послідовність політичних подій, що умовно сприяє бути дотичним до політичного життя, співпрацювати з політичними партіями чи громадськими об'єднаннями, фактично знаходячись територіально далеко.

Окрім цього, розширюються можливості щодо створення об'єднань, співтовариств вчених та політиків, які мають досвід управлінської діяльності з метою обміну практичним досвідом без територіальних обмежень. Якщо загальна політична культура все ж таки робить акцент на ціннісні орієнтири окремого народу, то кіберкультура об'єднує у спільні принципи дії для усього суспільства світу.

У свою чергу, негативними елементами кібернетичної діяльності є удосконалення проявів кіберзлочинів у різних його проявах, які націлені на політичний дисбаланс в окремих країнах, як прояв регіональної турбулентності в політичних системах держав. Тому, формування кіберкультури у політиці дозволить відшукати легкі форми попередження кіберзлочинів, а політичні діячі в методах діяльності знизять можливість використання таких методів впливу на опонента.

Криза у глобальних політичних процесах перекладає значний фронт впливу суб'єктів політики один на одного через кіберпростір, тому популяризація методик міжнародних порядків користування інформаційними ресурсами створює

умови для подальшого удосконалення кібернетичного простору та кіберкультури.

А тому, інформаційна культура стає своєрідним механізмом боротьби з злочинністю на основі принципово нового світогляду і наукової картини світу. Разом з цим, виникає новий рівень конкурентоздатності сучасної людини, яка наділена новим типом пізнання світу, культурою спілкування з людьми та технологічним мисленням. Оскільки, технологічні зміни не відворотні, люди з технологічним мисленням є сучасною новою суспільною формацією, то розвиток кіберкультури є вагомим чинником для стабілізації політичних процесів, які реалізуються в кіберпросторі, адже фактично найскладніші форми кіберзлочинів реалізуються з політичною та економічною цілями, які взаємопов'язані між собою.

Література

Lévy, P. (2001). *Cyberculture*. Univ. of Minnesota Press.

Завгородня, Ю. В. (2022). Особливості поведінки учасників політичного процесу під час конфронтації в інформаційному просторі. *Політикус*, 4, 29-34.

Власенко, Ф., Левченко, Є. (2019). Інформаційна культура та кіберкультура в контексті розвитку сучасного суспільства. *Українські культурологічні студії*, 2(5), 75-79.

Климчук Дмитро Олегович
*Донецький національний університет імені Василя Стуса,
м. Вінниця, Україна*

КІБЕРБЕЗПЕКА ПРОЦЕСУ ПРОВЕДЕННЯ ВИБОРІВ

У теперішній час важко переоцінити роль кібербезпеки у сучасному світі. Це пов'язано з тим, що з кожним днем посилюється розвиток цифрових технологій, які охоплюють велику кількість сфер нашого життя. Зважаючи на це існує небезпека негативного впливу на інформаційні системи шляхом здійснення кібератак. Не виключенням є і процес проведення виборів.

Держава-агресор періодично намагається впливати на проведення демократичних виборів як в Україні так і у світі, зокрема шляхом здійснення кібератак на державні ресурси.

Так, на сайті державної служби спеціального зв'язку та захисту інформації України зазначено, що під час одного з брифінгів заступник голови Держспецзв'язку Віктор Жора повідомив: «Україна протягом багатьох років була тестовим майданчиком атак російських хакерів. Підходи та технології, які були «відтестовані» на українській інформаційній інфраструктурі, вони використовують і в інших країнах». Як приклад він також зауважив, що у 2014 році російські хакери атакували сервери української Центральної виборчої комісії, а в 2016 та 2020 – наважились на втручання у вибори в США (Сайт Держспецзв'язку, 26.10.2023).

Крім того, у 2019 у межах виконання завдань із контррозвідувального забезпечення інтересів держави у сфері інформаційної безпеки, співробітники СБУ попередили спроби спецслужб рф організувати хакерські атаки на державні установи, які були задіяні в підготовці до виборчого процесу та його проведенні. Масове поширення шкідливого програмного забезпечення здійснювалось через направлення цільових електронних повідомлень на адреси держустанов, а також уразливі ділянки Інтернет-сайтів державних органів. За висновками фахівців, такі комп'ютерні віруси застосовуються

для блокування діяльності інформаційних ресурсів через підключення до державних реєстрів України, що могло створити загрозу для роботи серверів і персональних комп'ютерів виборчих комісій (Бондар & Ємельянов, 2019).

Вищезазначені приклади свідчать про неодноразові спроби ворога впливати на виборчий процес шляхом використання кібертехнологій. З метою боротьби зі спробами ворога втручатися у виборчі процеси основними суб'єктами національної системи кібербезпеки здійснюються активні дії, які спрямовані для протидії агресії у кіберпросторі.

Так, одним з напрямків формування безпеки у сфері проведення виборів можна виокремити забезпечення захисту державного реєстру виборців.

Відповідно до закону України «Про державний реєстр виборців» державний реєстр виборців це – автоматизована інформаційно-комунікаційна система, призначена для зберігання, обробки даних, які містять передбачені цим Законом відомості, та користування ними, створена для забезпечення державного обліку громадян України, які мають право голосу відповідно до статті 70 Конституції України (Про державний реєстр виборців).

Під час виборчого процесу у 2019 за даними прес-центру СБУ станом на 26.07.2019, співробітники СБУ у співпраці зі співробітниками Центральної виборчої комісії, Кіберполіції та Держспецзв'язку забезпечили належний рівень кібербезпеки та мінімізували загрози надійному та безпечному функціонуванню Єдиної інформаційної автоматизованої системи «Вибори» та автоматизованій інформаційно-телекомунікаційній системі «Державний реєстр виборців». (Бондар & Ємельянов, 2019).

У зв'язку із введенням в Україні воєнного стану та з метою захисту цілісності бази даних автоматизованої інформаційно-комунікаційної системи «Державний реєстр виборців», забезпечення захисту персональних даних, її захисту від несанкціонованого доступу, незаконного використання, незаконного копіювання, спотворення, знищення даних АІКС Реєстру, забезпечення її кіберзахисту 24.02.2022 Центральна виборча комісія своєю постановою тимчасово, на час дії воєнного

стану, припинила функціонування АІКС Реєстру, а також її ведення органами ведення Реєстру.

Водночас, у зв'язку з новими загрозами та викликами сьогодення, Центральна виборча комісія приділяє велику увагу питанню кіберзахисту та технологічній модернізації, яка до того ж визначена одним з стратегічних напрямків роботи Центральної виборчої комісії (Сайт ЦВК, 26.10.2023).

Таким чином можна зауважити, що уповноважені органи реагують на існуючі загрози та здійснюють покладений на них комплекс заходів щодо забезпечення кіберзахисту на професійному рівні. Проте роль цифрових технологій невпинно зростає та виникає потреба постійного удосконалення кіберзахисту для реагування на нові виклики та загрози. Оскільки держава-агресор неодноразово намагалася вплинути на виборчі процеси як в Україні так і в інших країнах цілком ймовірно, що вони будуть намагатися продовжувати робити подібні спроби і під час наступних виборів. Зважаючи на наведене, можна дійти до висновків, що перш за все слід поглиблювати співпрацю з іноземними партнерами у сфері кібербезпеки, вивчати досвід інших країн по протидії кіберзагрозам та впроваджувати законодавчі зміни щодо покращення рівня захисту від кіберзагроз, оскільки спроби ворога втрутитися у виборчі процеси можуть мати негативний вплив на рівень демократії.

Література

Бондар, Г. Л., Ємельянов, В. М. (2019). Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури. *Публічне управління та регіональний розвиток*, 5, 493-523.

Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua/news/ukrayina-neyedina-cil-rosiiskikh-khakeriv-prote-odna-z-golovnikh>

Офіційний сайт Центральної виборчої комісії. URL: <https://www.cvk.gov.ua/novini/tsvk-testovo-perevirit-sistemu-derzhavnogo-reiestru-vibortsiv.html>.

Закон про державний реєстр виборців 2007 (Верховна Рада України). Офіційний сайт Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/698-16#Text>.

Кучмій Олена Петрівна

кандидат політичних наук, доцент,

*Навчально-науковий інститут міжнародних відносин,
Київський національний університет імені Тараса Шевченка,*

м. Київ, Україна

ORCID: 0000-0002-2634-4114

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА СТРАТЕГІЇ ПРОТИДІЇ ГІБРИДНИМ ВИКЛИКАМ І ЗАГРОЗАМ ЄС

Сучасне середовище безпеки Європейського Союзу формується під впливом цілої низки чинників, виникнення яких обумовлене бурхливими геополітичними зрушеннями, зростанням нестабільності у регіоні і світі, трансформацією підходів до ведення війн, появою нових засобів протидії, удосконалення яких відбувається завдяки впровадженню досягнень науково-технологічного прогресу. Найбільш небезпечними для системи регіональної безпеки Європи нині виступають гібридні загрози, які завдяки своїй гнучкості, багатосуб'єктності (беруть участь держави і недержавні актори), багатомірності, поєднанню силових і несилових механізмів впливу, традиційних і нетрадиційних засобів протидії (військових, економічних, політичних, технологічних), що залишаються нижче порогу офіційно проголошеної війни, набувають критичного значення для подальшого поступального розвитку регіону.

Починаючи з 2014 р. Європейська Комісія започаткувала низку ініціатив, спрямованих на зміцнення безпеки і оборони європейського регіону у контексті появи нових гібридних викликів і загроз. У 2015 р. Рада ЄС ухвалила висновки щодо Спільної політики безпеки та оборони, в яких містився заклик до створення ефективної спільної структури для протидії гібридним загрозам і зміцнення стійкості ЄС, його держав-членів та міжнародних партнерів. У 2016 р. був оприлюднений перший політичний документ «Об'єднана структура протидії гібридним

загрозам - відповідь Європейського Союзу», що передбачав 22 напрями дій, починаючи від підвищення обізнаності до розвитку стійкості (European Commission, 2016). Важливу роль у боротьбі з гібридними загрозами у документі було відведено кібербезпеці, зокрема, зміцненню структур, до компетенції яких входять питання безпеки кіберсередовища ЄС, підвищення ефективності оперативного реагування на кіберінциденти, удосконалення методів боротьби з дезінформації в Інтернеті, запобігання втручання у вибори тощо.

Внаслідок швидкоплинної еволюції гібридних викликів і загроз для країн ЄС, у 2018 р. було представлено Спільне повідомлення Європейському Парламенту та Раді ЄС «Підвищення стійкості і зміцнення потенціалу для протидії гібридним загрозам», в якому зазначалося, що важливим досягненням у сфері протидії гібридним загрозам для кіберсередовища стало ухвалення усіма державами-членами ЄС правових документів, що регулюють базові підходи у сфері безпеки мереж та інформаційних систем. Основну увагу було приділено підвищенню стійкості ЄС до кібератак і створенню ефективних правових механізмів реагування в даній сфері (European Commission, 2018). У грудні 2019 р. у Висновках Ради ЄС щодо додаткових зусиль з посилення стійкості та протидії гібридним загрозам було запропоновано «скласти карту, яка б враховувала заходи, вжиті до цього часу, та відповідні документи, прийняті у всеосяжній формі, з метою сприяння виникненню нових ініціатив» (Council of the European Union, 2019). У документі також зазначалося, що з 2016 р. в рамках ЄС було впроваджено майже 200 ініціатив у сфері протидії гібридним загрозам, створено робочу групу East StratCom Task Force та онлайн-платформу для ознайомлення країн-членів з інструментами і заходами боротьби з гібридними загрозами.

У 2020 р. в рамках ЄС було оприлюднено документ під назвою «Картування заходів, пов'язаних з підвищенням стійкості та протидією гібридним загрозам», в якому, зокрема, йшлося про вироблення ефективних механізмів скоординованого реагування на великомасштабні інциденти та кризи у сфері кібербезпеки, у тому числі, через мережі європейських національних органів,

які відповідають за протидію кіберкризам (CyCLONe) за підтримки Агентства ЄС з кібербезпеки ENISA, удосконалення системи безпеки мереж 5G-зв'язку, створення об'єднаного центру дослідження кіберзагроз CERT-EU та мережі Груп реагування на інциденти (CSIRT) для моніторингу ситуації та підготовки оцінки кіберзагроз для критично важливих секторів, налагодження міжвідомчої співпраці у сфері кібербезпеки для надання експертної, оперативної та технічної підтримки ЄС та державам-членам; усунення ризиків кібербезпеки для широкого кола постачальників основних послуг у таких сферах, як енергетика, транспорт, водопостачання, банківська справа та цифрові технології; стимулювання розвитку науково-дослідних проєктів у сфері кібербезпеки через контрактне державно-приватне партнерство; створення Європейського центру компетенції з кібербезпеки (European Cybersecurity Industrial, Technology and Research Competence Centre); посилення мандату Агентства Європейського Союзу з кібербезпеки (ENISA), що має покращити оперативне співробітництво ЄС і держав-членів у сфері кібербезпеки, удосконалити підходи до врегулювання кризових ситуацій, продовжити розвиток інструментарію кібердипломатії з метою запобігання конфліктам, пом'якшення загрозам кібербезпеці та підвищення стабільності в міжнародних відносинах і, таким чином, сприяння посиленню стійкості ЄС до гібридних загроз у кіберпросторі (European Commission, 2020a).

Зазначимо, що у 2020 р. було ухвалено оновлену Стратегія кібербезпеки ЄС, яка мала зміцнити загальну стійкість Європи до кіберзагроз і допомогти гарантувати всім громадянам та підприємствам можливість повною мірою скористатися надійними послугами та цифровими інструментами, що заслуговують на довіру. У новій Стратегії йшлося не тільки про захист глобального і відкритого Інтернету, але й про захист європейських цінностей та фундаментальних прав і свобод кожного. Ґрунтуючись на досягненнях останніх років, у документ було включено конкретні пропозиції щодо регуляторних, інвестиційних та політичних ініціатив у трьох сферах діяльності ЄС: «Стійкість, технологічний суверенітет та лідерство»

(підвищення рівня кіберстійкості критично важливої інфраструктури); «Розбудова оперативного потенціалу для запобігання, стримування та реагування» (співпраця між органами ЄС та органами держав-членів, відповідальними за реагування на кібератаки, включаючи цивільні, правоохоронні, дипломатичні спільноти та спільноти кіберзахисту); «Просування глобального та відкритого кіберпростору шляхом посилення співпраці» (активізація роботи ЄС з міжнародними партнерами для зміцнення глобального порядку, заснованого на правилах, сприяння міжнародній безпеці та стабільності в кіберпросторі, а також захисту прав людини та основних свобод в Інтернеті). (European Commission, 2020b).

У практичній площині ініціативи ЄС у сфері кібербезпеки як складової протистояння гібридним загрозам зорієнтовані на формування ефективних механізмів захисту кіберпростору в умовах розбудови цифрового суспільства та Єдиного цифрового ринку від будь-яких спроб застосувати гібридні методи протиборства. Зокрема, для підвищення рівня стійкості до гібридних загроз у сфері кібербезпеки провайдери ключових цифрових послуг (наприклад, хмарних обчислень) повинні вживати відповідних заходів безпеки та повідомляти про серйозні інциденти державним органам, звертаючи увагу на будь-які гібридні характеристики. Держави-члени ЄС мають сприяти розвитку національного потенціалу кібербезпеки, зміцнюючи співпрацю шляхом обміну інформацією та передовим досвідом протидії гібридним загрозам, використовувати мережу CSIRT та CERT-EU для координації стратегічної співпраці. Для заохочення поглиблення державно-приватного партнерства та узгодження загальноєвропейських підходів до кібербезпеки було створено платформу NIS, яка містить інформацію про найкращі практики у зазначеній сфері. Особливої важливості протидія кіберзагрозам як складової гібридних війн набула в критично важливих сферах – енергетичній, індустріальній, транспортній та фінансовій.

Таким чином, важливим виміром гібридного протистояння нині виступає кіберпростір, в якому відбуваються масовані атаки на свідомість європейських громадян шляхом запуску кампаній з дезінформації через соціальні медіа і месенджери з метою

встановлення контролю над політичними наративами або радикалізації суспільних настроїв, підриву фундаментальних демократичних цінностей і свобод, впливу на ухвалення політичних рішень, стратегічні комунікації, вербування та скеровування діяльності так званих проксі-акторів тощо. Для протидії гібридним загрозам у кіберпросторі ЄС виробив ефективні механізми, які дозволяють поєднувати зусилля європейських країн, враховуючи національну специфіку стратегій кібербезпеки, приватного сектору та представників інтелектуальних кіл.

Література

Joint Framework on countering hybrid threats: a European Union response. Joint Communication to the European Parliament and the Council (2016). *European Commission.* URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018>.

Increasing resilience and bolstering capabilities to address hybrid threats. Joint Communication to the European Parliament, the European Council and the Council (2018). *European Commission.* URL: <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016>.

Council Conclusions on complementary efforts to Enhance Resilience and Counter Hybrid Threats (2019). *Council of the European Union.* URL: <https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf>.

Mapping of measures related to enhancing resilience and countering hybrid threats. Joint Staff Working Document (2020a). *European Commission.* URL: [https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/swd/2020/0152/COM_SWD\(2020\)0152_EN.pdf](https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/swd/2020/0152/COM_SWD(2020)0152_EN.pdf).

New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient (2020b). *European Commission.* URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391.

Кузьмич Вікторія Миколаївна

*Дніпропетровський державний університет внутрішніх справ,
м. Дніпро, Україна*

ОСНОВНІ СТРАТЕГІЧНІ НАПРЯМКИ КІБЕРБЕЗПЕКИ

Важливістю дослідження з даної теми є необхідність подолання суперечності між наявним станом стрімкого зростання важливості кібербезпекової проблематики та часткової готовності Української держави відповісти на новітні кібербезпекові виклики.

Основні виклики для України у сфері кібербезпеки:

➤ активно використовувати засоби мережі в міжнародній конкуренції;

➤ в умовах стрімкого прогресу інформаційно-комунікаційних технологій, особливо хмарних обчислень та квантових обчислень, мережі 5G, великих даних, Інтернету речей, штучного інтелекту тощо, конкурентний характер розробки засобів мережевої безпеки;

➤ мілітаризація кіберпростору та розвиток кіберзброї роблять можливим приховане проведення кібератак на підтримку бойових дій і розвідувальну диверсію в кіберпросторі;

➤ вплив пандемії COVID-19 на економічну діяльність і соціальну поведінку з широким використанням електронних сервісів та інформаційних комунікаційних систем, що призводить до швидкої трансформації та організації значної частини соціальних відносин дистанційним способом;

➤ запровадження нових технологій, цифрових сервісів та механізмів електронної взаємодії між громадянами та державою не здійснюється системно з точки зору заходів кібербезпеки та без належної оцінки ризиків.

На даний час заходи з організації кібербезпеки в Україні знаходяться у стані активної розробки та постійного удосконалення. Велику частину роботи з убезпечення громадян від найбільш розповсюджених кіберзлочинів здійснює МВС.

У даній структурі утворено спеціальне Управління боротьби з кіберзлочинністю. Основними завданнями Управління є організаційні та практичні забезпечення реалізації державної політики по попередженню та протидії злочинам і правопорушенням, які вчиняються з використанням інформаційної технології та телекомунікаційної мережі. Державна служба спеціального зв'язку та захисту інформації відповідно до своїх завдань безпосередньо включена до здійснення кібербезпеки держави.

Незважаючи на таку розгалуженість організаційних структур, які працюють у системі забезпечення кібербезпеки держави, вітчизняній кібербезпековій сфері притаманні певні стратегічні проблеми, які все ще потребують вирішення. У відповідь на політичну ситуацію, що склалась у кінці 2014 р. – на початку 2015 р. Президент України Петро Порошенко підписав указ «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» (Про Стратегію кібербезпеки України). Даним указом введена в дію розроблена фахівцями з кібербезпеки та затверджена на засіданні РНБОУ Стратегія кібербезпеки України. Стратегія вводить комплекс пріоритетів, заходів, та напрямів по забезпеченню кібербезпеки України, зокрема: вироблення і оперативну адаптацію державної політики, спрямованої на розвиток кіберпростору та досягненні сумісності з відповідними стандартами ЄС та НАТО; створення державної нормативно-правової та бази термінів у цій сфері; формування конкурентного середовища у сфері електронних комунікацій. Загалом, структура Стратегії визначає основні напрями організації кібербезпеки.

Правовий фундамент кібербезпеки України становлять Конституція України, закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» та інші закони, Конвенція Ради Європи про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України,

Доктрина інформаційної безпеки України, а також інші нормативно-правові акти. Проаналізувавши чинне законодавство, можна стверджувати, що основною проблемою правового забезпечення системи кібербезпеки України є відсутність розробленого та нормативно закріпленого понятійного апарату у сфері кібербезпеки на найвищому рівні. Насамперед, це стратегія забезпечення кібербезпеки, яка стане вітчизняним документом, що врегульовує відносини у кіберсфері та відповідно до якого буде забезпечуватись кібербезпека.

Пріоритети забезпечення кібербезпеки України: забезпечити, щоб кіберпростір захищав національний суверенітет і соціальний розвиток; захищати права, свободи та законні інтереси громадян України у кіберпросторі; європейська та євроатлантична інтеграція в кібербезпеці.

Для забезпечення інформаційної безпеки в Україні держава має вжити таких заходів:

- покращити інформаційне забезпечення державної політики, діяльності українських громадських організацій та закордонних суб'єктів господарювання;

- надати організаційну, технічну, інформаційну та ресурсну допомогу вітчизняним ЗМІ з метою формування позитивного іміджу України у світовому інформаційному просторі;

- посилити інформаційно-просвітницьку роботу щодо переваг членства України в ЄС, поглибити практичну співпрацю у сфері безпеки з НАТО, іншими міжнародними організаціями та країнами-партнерами, а також ефективні шляхи зміцнення національної безпеки України, в тому числі з урахуванням перспективи повноцінного членства в НАТО;

- об'єднання міжнародних інформаційно-комунікаційних систем і організацій на основі рівноправності, економічних інтересів, захисту мережі та підтримки інформаційного суверенітету;

- сприяти формуванню та дотриманню країнами міжнародних правил поведінки в інформаційній сфері; запобігати своєчасному виявленню зовнішніх загроз національному інформаційному суверенітету та усувати ці загрози, в тому числі за допомогою технологій кібербезпеки;

покращувати рівень міжнародного співробітництва у сфері інформаційна безпека на національному та відомчому рівнях;

- поширювати інформацію у світовому інформаційному просторі, формувати позитивний імідж України як надійного партнера в міжнародних відносинах та популяризувати позитивні надбання України.

Література:

Указ про Стратегію кібербезпеки України 2016 (Президент України). Офіційний сайт Президента України. URL: <http://www.president.gov.ua/documents/962016-19836>

Гарашенко, Ю. В. (2019). Державна політика у сфері кібербезпеки України. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Державне управління*, 30 (69), 1.

Задубний, А. (2021). Стратегія на тему кібербезпеки в Україні: цілі та пріоритети. *АрміяInform*. URL: <https://armyinform.com.ua/2021/08/27/strategiya-kiberbezpeky-ukrayiny-czili-ta-priorytety/>

Сімакова Світлана Іванівна
*кандидат юридичних наук, доцент,
Білоцерківський національний аграрний університет
соціально-гуманітарний факультет, м. Біла Церква, Україна*

АКТУАЛЬНІ ПИТАННЯ КІБЕРБЕЗПЕКИ В УКРАЇНСЬКОМУ СУСПІЛЬСТВІ

В сучасному суспільстві, яке є досить автоматизованим виникають нові види злочинів, які пов'язані із вчиненням шахрайства, крадіжок, вимагань із використанням транспортних телекомунікаційних мереж. Захист інформаційних даних, та програмного забезпечення, які розміщені в мережі Інтернет від втручання злочинців (ворога) є важливим питанням в контексті забезпечення кібербезпеки в українському суспільстві. Розвиток кібербезпеки, кіберзахист – пріоритетні напрямки нашої держави.

За статистичними даними, у 2022 р. комунікація між бізнесом та клієнтом у 72 % випадках вілбулась у цифровому форматі. В такому разі споживачі очікують більш високий контроль над своїми даними та прозорості політики організації. Про те, існує ризик втручання у особисті дані споживачів.

Наразі в українському суспільстві існує новий вид злочинця-кіберзлочинець. Це не просто злочинець, який вчиняє крадіжки, шахрайства, та інші види злочинів. Це злочинець, який володіє необхідними навичками роботи із транспортними телекомунікаційними мережами, програмним забезпеченням, різного роду обладнанням, тобто це особа, яка навчалась цьому, чи отримала такі знання працюючи на роботах пов'язаних із використанням транспортних телекомунікаційних мереж, Інтернетом.

Кіберзлочинці мотивовані жагою до легкої наживи, до збагачення за рахунок інших в найкоротші строки. Такі злочинці використовують банківські рахунки жерт злочину, намагаються отримати ідентифікаційні дані, дані банківських

карток. Дану інформацію злочинці можуть продати іншим особам, які зацікавлені в отриманні такої інформації, можуть викрасти кошти із банківських карток власника, можуть здійснювати прослідковування за життям власниками такого майна із корисних цілей, чи вчинити інші злочини. Такі злочини можуть стосуватись, як конкретної людини, так, і цілої сім'ї, чи навіть бізнесу. Захист бізнесу є пріоритетним завданням власників бізнесу, адже для них є надважливим їхні клієнти та відповідно їх репутація, а коли компанія не може захистити клієнта то і довіри до неї не буде. А клієнт буде обирати вже інших партнерів для ведення бізнесу.

Захист підключених до мережі Інтернет, системобладнання, та програмного забезпечення та даних від кіберзагроз, кіберзлочинців називають кібербезпекою. Такий захист є вкрай необхідним, адже кіберзлочинці можуть підривати економічну безпеку, як громадян, так і суспільства загалом вчиняючи злочини в даній галузі. Cybersecurity” це безпека у звичайному нашому житті – це коли ми закриваємо двері свого помешкання, обладнуємо його засобами охорони, використовуємо сигналізацію для захисту свого автомобілю, та інше, а також це є наш захист тільки в ІТ просторі.

За статистичними даними Tech Times, кібератаки зловмисного програмного забезпечення на мобільні пристрої у всьому світі зросли на 500% протягом перших кількох місяців 2022 р. Наразі існують передові методи зламу захисту даних споживачів, такі, як: програми-вимагачі, фішинг атаки, атаки Man-in-the-Middle, та шкідливі програми та вебсайти.

У 2023 р. зафіксовано новий вид шахрайства з використанням deepfake, який полягає у створенні реалістичних аудіо та відео матеріалів створених за допомогою штучного інтелекту і машинного навчання. А тому правоохоронним органам під час розроблення заходів боротьби із кіберзлочинцями варто враховувати новітні види кібератак, задля попередження та розкриття кіберзлочинів.

З початку війни повномасштабної війни РФ проти України Міністерство цифрової трансформації створило першу в нашій державі українську ІТ армію. Метою якої є захист даних

у національному, та цифровому просторі. Під час повномаштабної війни проти України у 2020 р. було зафіксовано 800 повномаштабних кібератак. У 2021 р. 1400, У 2022 – понад 4000.

Кіберборотьба й кіберзахист стали одними із ключових елементів гібридної війни. Наші фахівці та хакери-волонтери не лише успішно протистоять нападам, а й завдають значних ударів у відповідь. У 2023 р. зафіксовано понад 1,25 мільйона DDoS-атак на російську інфраструктуру (це 8,4% від усіх кібератак у світі). За оцінками керівника служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО Наталії Ткачук, Україна – єдина держава, яка змогла здобути перевагу у протистоянні кібератакам та інформаційній агресії РФ (Кириченко).

У Стратегії кібербезпеки України визначено, що «забезпечення кібербезпеки є одним з пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі» (Задубінний; Указ про Стратегію кібербезпеки України).

Стратегія кібербезпеки України визначає пріоритети національних інтересів у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави (Задубінний; Указ про Стратегію кібербезпеки України).

Слушно вказує Андрій Задубінний: «РФ залишається одним з основних джерел загроз національній та міжнародній кібербезпеці. Надана оцінка діям країни-агресора, адже «Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України». Прогнозується зростання інтенсивності міждержавного протиборства й розвідувально-підривної діяльності у кіберпросторі.

Розширюється коло держав, які намагаються сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної діяльності у кіберпросторі, посилюють державний контроль за національними сегментами мережі Інтернет. При цьому поширюється інструментарій та посилюється тенденція здійснення розвідувально-підривної діяльності у кіберпросторі шляхом залучення спецслужбами окремих держав, насамперед Російської Федерації, міжнародних хакерських угруповань для реалізації кібервпливу. У Стратегії також наголошується, що використання кіберпростору терористичними організаціями набуває глобального масштабу” ((Задубінний; Указ про Стратегію кібербезпеки України).

Висновок. Кібербезпека в українському суспільстві забезпечує поглиблення євроінтеграційних процесів шляхом уніфікації сучасних, дієвих методів забезпечення кібербезпеки із врахуванням практики ЄС і НАТО. В цьому нашій державі допомагають іноземні партнери, які розробляють спільні заходи спрямовані на посилення кіберстійкості України. Захист національних інтересів у кіберпросторі – пріоритетні напрямки українського уряду. Єдина, могутня, нездоланна українська спільнота покладає всі зусилля на убезпечення кіберпростору для захисту суверенітету держави та розвитку суспільства; покликана захищати права, свободи і законні інтереси громадян України у кіберпросторі.

Література

Кириченко, А. *Кібербезпека в Україні: шляхи розвитку та можливості*. URL: <https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html>.

Задубінний, А. (2021). *Стратегія кібербезпеки України: цілі та пріоритети*. URL: <https://armyinform.com.ua/2021/08/27/strategiya-kiberbezpeky-ukrayiny-czili-ta-prioritytety/>.

Указ про Стратегію кібербезпеки України 2021 (Президент України). *Офіційний сайт Верховної Ради України*. URL: <https://zakon.rada.gov.ua/go/447/2021>

Суський Георгій Валерійович
*Інститут програмних систем НАН України,
м. Київ, Україна*

КІБЕРБЕЗПЕКА У ПРОБЛЕМНОМУ ПОЛІ ГІБРИДНОЇ ВІЙНИ

З розвитком кібернетичних систем, що спричинило також бурхливий розвиток цифрових медіа, глобалізація інформаційних процесів стала повсякденним явищем. Проте «інформація без кордонів», що стало гаслом ХХІ ст., також має свій зворотній бік, свої плюси і мінуси. Втручання в інформаційний простір інших суверенних держав з метою здійснення кібератак або розповсюдження агресивної пропаганди (як це відбувалось перед початком і в перші тижні після повномасштабного вторгнення російських військ на територію суверенної України у 2022 році) роблять країни незахищеними та вразливими щодо втручання у їхній інформаційний та політичний простір з боку інших держав (Melykh, & Korbut, 2020). Треба взяти до уваги, що у власності державних і найбільших комерційних каналів мас-медіа ще й досі залишаються сконцентрованими основні фонди та технічні потужності, отже, вони автоматично отримують можливості охоплення територій та найбільші масштаби обсягів аудиторії. Місцевим мас-медіа, потужності яких є меншими, зберегти високопрофесійний кадровий склад та виробляти високоякісні власні програми під час повномасштабної російсько-української війни набагато складніше. Особливо це стосується прифронтових та деокупованих територій.

«Ефір був матір'ю усіх медіа» (Пітерс, 2004, С. 111), проте, коли навколо відбуваються обстріли, непередбачувані негативні події (іноді загрозливі для життя), коли в мас-медійному просторі інформація доноситься спотворено, коли негативні стереотипи можуть виявлятися у настановленнях, передусім конфронтаційних, можливості реципієнта протистояти таким впливам медіа звужуються, тим більш, коли це відбувається

внаслідок цілеспрямованих кібер- та інформаційних атак. За нестійкого інтернет-трафіку звужуються також можливості увійти в простір соціальних мереж і отримати інформацію від експертів, учасників (зокрема, військових) та очевидців подій. Залежно від масштабів мовлення та покриття максимального обсягу аудиторій на територіях, куди досягають технічні можливості цих каналів, ведеться справжня «гібридна війна» у мас-медійному просторі.

Сучасний інформаційний простір впливає не тільки на політичні, економічні та соціокультурні процеси, але й на розвиток ІТ-технологій та забезпечення ними військових. З погляду на мас-медійний контент та загальну ситуацію в інформаційному просторі України, саме питання кібербезпеки в умовах гібридної російсько-української війни (Суський, 2023, С.48-50) набувають особливої важливості. Одним з основних стратегічних напрямків кібербезпеки в сучасній ситуації, у якій перебуває Україна, є напрямок складових безпеки державних органів як таких, що опікуються державними даними. Специфіка державного кіберзахисту вимагає концентрації уваги на таких аспектах:

- контент інформації
- кількість користувачів
- архітектура підключення, що включає сітку розгалуження (щодо спектру громад)
- регламенти роботи
- менталітет користувачів.

Аналіз звітів Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту України свідчить, що від початку російсько-української війни тренд на зростання кількості кібератак зберігається. Основною метою таких кібератак є кібершпionаж, порушення доступності державних інформаційних сервісів та навіть знищення інформаційних систем за допомогою програмвайперів. З кінця 2022 року зафіксовано істотне зростання активності хакерських груп щодо розповсюдження шкідливого програмного забезпечення, серед якого є такі програми, що викрадають дані, й такі, що прямо спрямовані на знищення даних.

Важливою складовою національної системи кібербезпеки є організаційно-технічна модель кіберзахисту, яка забезпечує на організаційному, технологічному і базисному рівнях взаємодію між суб'єктами національної системи кібербезпеки на основі відповідно захищеної інформаційної інфраструктури. Дана модель складається з трьох вертикально та горизонтально інтегрованих рівнів кіберзахисту:

- організаційно-керуюча інфраструктура, до складу якої входять суб'єкти кіберзахисту, згруповані у державний, академічний, приватний, громадський та регіональний сектори;
- технологічна інфраструктура, в рамках якої забезпечується обмін інформацією, моніторинг, забезпечення сталої безпеки кіберпростору тощо;
- базисна інфраструктура, яка складається з двох шарів: захищена інформаційна інфраструктура та обізнане суспільство (громади та громадяни).

Велике значення має міжнародна підтримка України; зокрема, увагу світових кіберспільнот, які виступають на боці України, привертає низка заходів, які є дієвими щодо протидії злочинним російським кібератакам (EEAS, 2022). Так, агрегувавши свої зусилля, незалежні хакери з усього світу виявили та оприлюднили російські урядові документи (в тому числі електронні листи), фінансові дані та інформацію про банківську діяльність, виробництво енергії та пропагандистські кампанії тощо. За повідомленням ДСЄП (Дослідницької служби Європарламенту) така конфіденційна інформація потім передається міжнародним активістам, з метою покарати російських агресорів за військові злочини в Україні. Яскравим ефектом останніх дій таких кіберспільнот є їхній успіх стосовно створення хаосу в російських кіберсистемах і руйнування переконань про їхню захищеність.

Позиція Європарламенту є непохитною: у резолюції від 1 березня 2022 року Парламент закликав до негайного та повного впровадження всіх рішень, які посилять внесок ЄС у зміцнення оборонних спроможностей України, у тому числі у сфері кібербезпеки. Крім того, Парламент закликав ЄС, НАТО та інших зацікавлених партнерів посилити допомогу Україні

у сфері кібербезпеки. Євродепутати закликали до повного застосування режиму кіберсанкцій ЄС проти фізичних, юридичних осіб та установ, відповідальних за кібератаки проти України або причетних до них (Przetacznik, Tarova, 2022).

Також одним з найважливіших напрямків кіберзахисту і протидії злочинним кібератакам є – стратегія скоординованого захисту. Вона полягає у забезпеченні залучення зовнішніх фахівців для проведення цифрових розслідувань успішних кібератак на організацію. Організована координація захисту, що включає як технічну складову – обмін інформацією про кіберінциденти та загрози, так і організаційну – координація реагування та зв'язок з органами влади, антикризове управління. Впроваджується забезпечення багаторівневого захисту даних та інформаційно-комунікаційних систем, відповідно до карти кіберризиків і структури бізнес процесів.

Розвиток цифровізації та активізація переходу на цифрові системи управління сприяли входженню України у глобальне інформаційне суспільство, проте, спричинивши і ряд загроз в галузі кібербезпеки. Питання кібербезпеки в умовах гібридної війни набуває особливої гостроти як стосовно медіапростору, так і технологічної інфраструктури. Одними з основних стратегічних напрямків кібербезпеки є напрямок складових безпеки державних органів як таких, що опікуються державними даними, а також організаційно-технічна модель кіберзахисту, яка забезпечує на організаційному, технологічному і базисному рівнях взаємодію між суб'єктами національної системи кібербезпеки. Захист інформаційно-комунікаційних систем (зокрема, державного рівня), програмних комплексів і мереж постає як нагальне завдання ІТ-фахівців з кібербезпеки, адже загрози в кіберпросторі є величезним викликом для національної безпеки України. Сьогодні необхідне вибудовування основних стратегічних напрямків кібербезпеки країни і конкретних стратегій і засобів її досягнення.

Література

- Пітерс, Дж.Д. (2004). *Слова на вітрі: історія ідеї комунікації*. Київ.
- Суський, Г. В. (2023). Питання кібербезпеки та «інформаційного імунітету» країни в період гібридної війни. *Особливості*

трансформації комунікацій в умовах новітніх суспільних викликів. Київ, НаУКМА, 48-51.

A Strategic Compass for Security and Defence (2022). EEAS. URL: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

Melykh, O., Korbut, A. (2020). Entertainment media in the context of hybrid war in the post-Soviet countries: the case of Ukraine. *Economic Annals-XXI*, 182(3-4), 27-34. doi: <https://doi.org/10.21003/ea.V182-03>.

Przetacznik, J., Tarpova, S. (2022). Russia's war on Ukraine: Timeline of cyber-attacks. *EPRS: European Parliamentary Research Service*. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI\(2022\)733549_XL.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf)

Гуменюк Наталія Іванівна

старша викладачка кафедри

медицини катастроф та військової медицини

Вінницький національний медичний університет ім. М.І.Пирогова,

м. Вінниця, Україна

Ангельська Вікторія Юрївна

старша викладачка кафедри

медицини катастроф та військової медицини

Вінницький національний медичний університет ім. М.І.Пирогова,

м. Вінниця, Україна

ORCID: 0000-0001-6140-0807

Матвійчук Микола Васильович

к.мед.н., доцент, завідувач кафедри

медицини катастроф та військової медицини

Вінницький національний медичний університет ім. М.І.Пирогова,

м. Вінниця, Україна

Поляруш Влада Володимирівна

старша викладачка кафедри

медицини катастроф та військової медицини

Вінницький національний медичний університет ім. М.І.Пирогова,

м. Вінниця, Україна

БЕЗПІЛОТНІ ЛІТАЛЬНІ АПАРАТИ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ СЬОГОДЕННЯ

За час повномасштабного вторгнення росії в Україну застосування безпілотних літальних апаратів (надалі БПЛА) для здійснення бойових задач набуло неймовірних масштабів. БПЛА застосовуються обома воюючими сторонами і є дієвою зброєю як в бойових цілях так і в розвідувальних. Саме операції з БПЛА, відкрили нову сторінку в умовах сучасної війни. Вони не можуть гарантувати швидкого звільнення або ж захоплення території, але значно впливають на якість контрнаступів.

БПЛА – це мобільний безпілотний літальний апарат, запрограмований на виконання будь-яких задач. БПЛА може програмуватись заздалегідь, або пілотуватись оператором через пульт дистанційного керування. З початком XXI століття літаючі безпілотники і наземні БПЛА стрімко увірвалися в цивільне життя і навіть у побут людини (інтернет ресурс). Формально історія безпілотників починається з 1782 року, коли брати Етьєн і Жозеф Монгольф'є підняли в повітря кулю, наповнену димом, вона протрималась у повітрі 10 хв і піднялась майже на 300м, чим і був покладений початок застосування аеростатів та дережаблів в авіації, а також примінення цих засобів у військовій справі. Початок використання безпілотних літальних апаратів у бойових діях ввійшло в історію у 1849 р. (Італія) і на сьогодні стає все більш розповсюдженим в сучасних збройних конфліктах. БПЛА мають безліч переваг, які можуть виконувати у розвідуванні, тактичної операції, корекції артилерійського вогню, нейтралізації, ураженні живої сили (шляхом спрямування на телефон військового, а SIM-картка вказує на місцезнаходження). США використовували широко в бойових діях в Афганістані. США є лідером у розробці та використанні БПЛА в умовах війни. У військових США до 2030 р. планується до 30% використовувати безпілотні системи від загальної кількості бойових машин (Горошко, Гуменюк, 2020 С. 25). Безпілотна авіаційна система не позбавлена людської ланки (за винятком окремих випадків повної автоматизації), але створює для неї можливість керувати літальним апаратом дистанційно, виконуючи при цьому увесь комплекс завдань, типових для пілота або льотного екіпажу. Тому більш адекватна назва для таких апаратів, яка використовується у зарубіжній літературі – дистанційно пілотовані літальні апарати (ДПЛА- Remotely Piloted Aircraft). Існує широке різноманіття безпілотних літальних апаратів різного класу та призначення, які важко порівнювати за змістом та умовами діяльності операторів (Петренко, 2015, С. 448).

За загальним виглядом БПЛА можна класифікувати за: швидкістю польотів: малошвидкісні- 250 км/год., середньошвидкісні- 450 км/год, швидкісні- 900-980 км/год.; призначення: БПЛА (Unmanned Aerial Vehicle) – багаторазово

реалізує своє функціональне призначення без безпосереднього розміщення людини на борту з метою управління. Загальноприйняте поняття має досить широкий сенс і не завжди точно відображає специфіку літального апарата. Таким чином, у даний клас не включаються безпілотні модифікації серійних літаків, використовувані як повітряні мішені, а також всі види балістичних і крилатих ракет. ДПЛА (Дистанційно пілотований літальний апарат Remotely Piloted Aircraft) – безпілотний літальний апарат з безперервним управлінням, яке здійснюється тим або іншим способом з нерухомого або рухомого пункту управління. БПАЛА (Безпілотний автоматичний літальний апарат Unmanned automatic aircraft) – безпілотний літальний апарат, що реалізує своє функціональне призначення в автоматичному режимі відповідно до закладених у нього алгоритмів і програм функціонування (крилаті ракети, літаки-розвідники і т.п.); функціональністю: бойові, які в свою чергу поділяються на спеціалізовані ударні багаторазового використання та ударні одноразового застосування. БПЛА забезпечення-розвідувальні, транспортні, цільові (Гимочко, Голубничий, Третяк, Рубан, 2007). Більшість моделей здатні здійснювати регулярне стеження, передаючи дані та відео на наземну станцію. Але це не все, що вміють безпілотники. Багато моделей також можуть бути наповнені вибухівкою – тобто вони можуть врзатися у цілі, тому їх і називають «камікадзе» або «дрони-самогубці» (Майк Екел, 2020).

Серед різних видів поранень під час введення воєнних дій, поранення отримані внаслідок застосування безпілотних літальних апаратів займають перше місце за складністю. Нас зацікавило питання дослідити обізнаність майбутніх лікарів зі складністю травм та поранень отриманих при використанні БПЛА.

Цільовою аудиторією дослідження стали 269 здобувачів освіти ВНМУ ім. М.І. Пирогова віком від 17 і старших 24 років, I-V курсів, із них чоловічої статті – 39,8% та жіночої статті – 60,2%. Із загальної кількості опитуваних на питання: «Чи є на Вашу думку доцільним вивчення особливостей отриманих травм у поранених внаслідок застосування БПЛА в воєнних умовах

в медичному вузі?» респонденти відповіли наступним чином: «Так, доцільно» – 91,8%, «Ні, не доцільно» – 5,2%, «Байдуже» – 3%. За результатами опитування на питання: «Який рівень обізнаності, на Вашу думку, ви маєте в питанні застосування БПЛА в мирний та військовий час?» лише – 2,6% визнали, що мають достатньо високий рівень обізнаності, 16,7% – вважають достатній рівень, проте 52% – низький, в основному через відсутність доступної інформації, в той час як 28,6% – не цікавилися питанням взагалі. На запитання: «Чи є, на Вашу думку, відмінності в отриманих травмах та пораненнях від застосування звичайної вогнепальної зброї та від застосування БПЛА?» 58% респондентів погодились, що є значні відмінності, 38% – вважали, що є незначні відмінності і 1,9% – відповіли, що взагалі немає відмінностей, а 1,1% – висловили байдужість до цих різних видів зброї. Стосовно дієвості використання безпілотних літаючих апаратів в наданні невідкладної медичної допомоги: 49,8% – відповіли так, дієво, 47,2% – так, дієво, проте сумнівались і 3% – ні, не дієво. З приводу питання: «Чи потребує, на Вашу думку, застосування БПЛА в військових умовах подальшого поглибленого наукового вивчення?» 95,5% – дали стверджувальну відповідь, а 2,2% – визнали, що дана інформація не потребує вивчення.

Можемо відзначити про високу ефективність безпілотних систем на полі бою. Аналізуючи отримані відповіді, можемо зазначити, що 95,5% респондентів зацікавлені у знаннях щодо використання безпілотних літаючих апаратів в умовах війни через безліч переваг, та які займають перше місце за складністю поранення та надання медичної допомоги.

Література

Дрон. *Wikipedia*. URL: <https://uk.wikipedia.org/wiki/Дрон>

Гуменюк, К. В., Горошко, В. Р. (2020). Погляд із минулого в майбутнє: безпілотні літаючі дрони як елемент евакуації поранених у медичній службі Збройних сил України. *Медицина невідкладних станів*, 16, 5, 22-25. DOI:10.22141/2224-0586.16.5.2020.212220

Екел М. (2020). Війни дронів: використання безпілотників під час бойових дій у Нагірному Карабасі. *Радіо Свобода*. URL: <https://www.radiosvoboda.org/a/30889212.html>

Петренко, О. В. (2015). *Психологічні аспекти новітніх підходів до забезпечення нефективності наземних екіпажів безпілотних літальних апаратів*, 436-450. URL: <http://appspsychology.org.ua/data/jrn/v10/i27/43.pdf>.

Тимочко, О. І., Голубничий, Д. Ю., Третяк, В. Ф., Рубан, І. В. (2007). *Класифікація безпілотних літальних апаратів. Військово-технічні проблеми*, 1(9), 61-66. URL: https://openarchive.nure.ua/bitstream/document/3330/1/soivt_2007_1_19.pdf

Крошка Надія Володимирівна
*Національна академія внутрішніх справ,
капітан поліції, старший інспектор з особливих доручень,
Управління протидії кіберзлочинам в м. Києві*

ДІАГНОСТУВАННЯ ІНТЕРНЕТ-ЗАЛЕЖНОСТІ У ВОЄННИЙ ЧАС В КОНТЕКСТІ КІБЕРБЕЗПЕКИ

Інтернет-залежність є серйозною проблемою сьогодення, оскільки інтернет тією чи іншою мірою входить в життя багатьох людей. Якщо ще десять-двадцять років тому ним користувалися лише ті, кого цікавив інтернет як такий, то сьогодні інтернет-користувачами вимушено стають і люди, які не захоплюються всесвітньою мережею. Він потрібний для навчання, роботи, багато необхідних у повсякденному житті дій через інтернет можна зробити легше, швидше, зручніше.

Також масовій інтернетизації суспільства сприяли тривала пандемія коронавірусу та повномасштабне вторгнення. Ці події розірвали безліч соціальних зв'язків, порушили багато процесів, які стало надто важко або зовсім неможливо здійснювати без інтернету. Наприклад, купувати квитки на потяг або навіть їжу в супермаркеті тепер, у воєнний час, безпечніше дистанційно, ніж фізично приїздити на вокзал або йти до торгового центру. Деякі соціальні зв'язки зараз підтримуються лише через інтернет, оскільки друзі та родичі опинилися в різних країнах, зустрічатися наживо важко, телефонувати надто дорого, і спілкування через інтернет є найзручнішим. За таких обставин люди – як діти, так і дорослі – подекуди регулярно проводять онлайн години щодня. І багато з них стають інтернет-залежними, не помічаючи цього, адже їм здається, що кожна година в інтернеті виправдана, вони не марнують там час, а займаються важливими справами.

Також діагностуванню інтернет-залежності (яка визнана розладом ще в 90-х роках) заважає те, що на побутовому рівні саме поняття «інтернет-залежність» сприймається викривлено через різний досвід різних поколінь. Тут варто згадати ознаки

інтернет-залежності, які виокремила його провідна дослідниця К. Янг (K.Young):

- нав'язливе бажання перевірити e-mail;
- постійне чекання наступного виходу в Інтернет;
- скарги навколишніх на те, що людина проводить занадто багато часу в інтернет;
- скарги навколишніх на те, що людина витрачає занадто багато грошей на інтернет (Young, 1999).

Ці ознаки на сьогодні є відверто застарілими. По-перше, певні форми інтернет-залежності взагалі не передбачають постійного перевіряння e-mail, для інтернет-залежних може бути цілком достатньо постійно скролити стрічку в соцмережах або грати онлайн. По-друге, поняття «скарги навколишніх» є надто суб'єктивним. «Навколишнім», що належать до більш старших поколінь, може здаватися, що людина проводить в інтернеті надто багато часу, навіть коли насправді жодних ознак інтернет-залежності в неї немає, просто старші родичі чули про інтернет-залежність і хвилюються, не розуміючи, для чого потрібен інтернет. Авторів цих рядків відомі непоодинокі випадки, коли люди вважали, що їхні рідні надто багато часу проводять в інтернеті, але насправді йшлося про роботу чи навчання, для яких потрібен інтернет. Викривленим було саме сприйняття оточуючих, які не могли осягнути розумом, наскільки багато всього легко та зручно робити за допомогою всесвітньої мережі.

Тому задля діагностування інтернет-залежності варто використовувати інші, більш сучасні ознаки. Передусім варто застосовувати основний критерій, що розмежує Інтернет-залежність та звичайне захоплення комп'ютером та мережею, – наявність/відсутність шкоди фізичному та психічному здоров'ю, соціальному життю (Шугайло, 2015).

Український дослідник Т. Карабін (Карабін, 2005) аналізує поняття інтернет-залежності і називає такі його ознаки: нав'язливе бажання вийти в інтернет, будучи «offline», та нездатність вийти з інтернету, будучи «online». Психологічна роль адиктивної поведінки полягає в тому, що, прагнучи втекти від реальності, людина періодично намагається штучним

шляхом змінити свій негативний психічний стан на такий, що дає їй ілюзію безпеки, відновлення рівноваги. Користування інтернетом поглинає час, сили, емоції так, що узалежнений не може підтримувати рівновагу в житті, включатися в інші форми активності, отримувати задоволення від спілкування з людьми, розвивати інші сторони особистості, проявляти симпатії, співчуття, емоційну підтримку навіть найбільш близьким людям.

Воєнний час додатково утруднює діагностику, оскільки симптоми інтернет-залежності, такі як зниження емпатії, комунікативні проблеми, підвищена тривожність та потреба в ілюзії безпеки, загострюються у зв'язку з переживаннями, пов'язаними з війною. І збільшення часу, який людина проводить в інтернеті, здається виправданим, адже важливо читати новини, спілкуватися з друзями, пересвідчуючись, що всі благополучні. Тому варто передусім орієнтуватися на такі симптоми:

- час, який людина, проводить в інтернеті, постійно зростає або принаймні не зменшується практично за жодних обставин;

- людина нервує, якщо довго не може зайти до інтернету;

- людина не може знизити напругу, знайти розраду інакше, ніж в інтернеті;

- людина нехтує іншими, не пов'язаними з інтернетом аспектами життя: їй стає байдуже, як вона виглядає, вона уважніше ставить до друзів з інтернету та більш байдуже – до друзів поза інтернетом, справи, не пов'язані з інтернетом, відходять для неї на другий план;

- людині важко дозувати час перебування в інтернеті.

Таким чином, інтернет-залежність під час воєнного часу стає ще гострішою проблемою, ніж раніше, тим більше що багатьма сприймається другорядною, неважливою проблемою. Тому важливо використовувати сучасні способи діагностики та самодіагностики.

Література

Карабін, Т. В. (2005). *Вплив особливостей спілкування в мережі «Internet» на процес соціалізації студентської молоді*: дисертація кандидата психологічних наук. Івано-Франківськ.

Шугайло, Я. В. (2015). Інтернет-залежність та проблема її профілактики серед дітей та підлітків. *Вісник Запорізького національного університету. Педагогічні науки*, 2 (25), 17-24.

Young, K. S. (1999). *Internet Addiction: Symptoms, Evaluation, And Treatment*. University of Pittsburgh at Bradford.

Кондратенко Анастасія Олегівна
*Державний торговельно-економічний університет,
м. Київ, Україна*

ВАЖЛИВІСТЬ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ЛОГІСТИЦІ

Безпека в логістиці є однією з найважливіших складових успішного функціонування будь-якого сучасного господарського підприємства. Ця сфера вимагає детального планування, постійного контролю та впровадження найсучасніших технологій для забезпечення безпеки як під час транспортування товарів, так і в складському обліку. Все це відіграє критичну роль у забезпеченні надійності ланцюга постачання та задоволенні потреб споживачів. Використання сучасних технологій та інноваційних методів стало необхідністю для мінімізації ризиків та забезпечення надійності ланцюга постачання. Такий підхід допомагає не лише забезпечити постачання та перевезення товарів, але і зберегти безпеку та ефективність усього господарського процесу.

Українці під час воєнного стану, а особливо на його початку, як ніхто інший зрозуміли всю важливість логістики, безпеки постачання та перевезень, де зіштовхнулися зі відсутністю доступу до певних товарів, знищенням складів та інфраструктури, а також втратою деяких транспортних зв'язків, що мали катастрофічний вплив на життя та господарську діяльність країни. Війна в Україні призвела до серйозних економічних втрат, а збиток, завданий транспортній інфраструктурі країни, оцінюється в 100 мільярдів доларів (Sorochii, 2022). Найбільші втрати логістики України пов'язані з блокуванням морських портів. До війни через них здійснювалося близько 70% українського експорту та імпорту. Зараз порти заблоковані російськими військами, що призвело до зупинки експорту та імпорту багатьох товарів. Крім того, під час війни було пошкоджено або знищено значну кількість

логістичних об'єктів, таких як склади, термінали, транспортні засоби. Це також призвело до зниження ефективності логістичних операцій. Багато підприємств були змушені закритися або переїхати на захід України. Крім того, через дії Росії постраждали і транспортно-логістичні компанії. Окрім проблем, з якими стикається транспортна галузь (нестача водіїв, зруйнована дорожня інфраструктура, брак складських приміщень, небезпека для життя працівників), трапляються й надзвичайні випадки. Тому вміння ефективно планувати, керувати та забезпечувати безпеку логістичних процесів стало вирішальним фактором для забезпечення готовності до подібних ситуацій (Берестенко, 2023). Важливо враховувати, що безпека в логістиці впливає на всі аспекти бізнесу, від забезпечення робочих місць до відносин з клієнтами.

Забезпечення безпеки в логістиці є необхідним аспектом сучасних логістичних операцій. Логістика, як складний процес переміщення товарів та ресурсів від постачальника до споживача, стикається з різними ризиками і загрозами на кожному її етапі. Тому важливо мати чіткий план та систему заходів для забезпечення безпеки та надійності цього процесу. Можна виділити основні аспекти безпеки в логістиці: 1) забезпечення захисту від фізичних загроз, таких як крадіжки, вандалізм, аварії та стихійні лиха, є критичним для логістичних операцій. Це може включати в себе використання систем відеоспостереження на складах, сейфових перевезень та управління доступом; 2) через розвиток технологій і віддаленими системами управління, кібербезпека стала ключовою складовою безпеки в логістиці. Злочинці можуть спробувати використовувати кібератаки для викрадення даних, перерви в роботі систем або навіть керування транспортом. Тому важливо захищати комп'ютерні системи та мережі, використовувати сильні паролі, оновлювати програмне забезпечення та навчати персонал з питань кібербезпеки для проведення безпечних процесів транспортування, складування та захисту даних споживачів, які користуються логістичними послугами; 3) контингентування, що являє собою стратегічне планування для запобігання та керування ризиками в логістичному ланцюзі. Це може включати планування змінних

маршрутів, резервні джерела постачання, плани надзвичайних ситуацій і резервні об'єкти для забезпечення неперервності постачання під час негативних подій; 4) важливою завжди залишається безпека транспортування. Перевезення товарів може бути супроводжене ризиками, особливо при транспортуванні небезпечних матеріалів. Відповідне маркування, упакування, навчання водіїв та встановлення аварійних планів є важливими кроками для забезпечення безпеки під час транспортування; 5) безпека при зберіганні відіграє важливу роль для подальшого транспортування товарів, вони є місцями, де товари зберігаються перед подальшим розподілом. Тому склади повинні бути обладнані системами безпеки, такими як відеоспостереження, контроль доступу та сигналізація, щоб запобігти крадіжкам та пошкодженням.

Страховання є одним з основних засобів забезпечення безпеки в логістиці. Воно допомагає логістичним компаніям захиститися від фінансових збитків, які можуть бути завдані в результаті різних ризиків. Воно дозволяє компаніям захистити себе від фінансових втрат у разі негативних подій, таких як крадіжки, аварії, пошкодження товарів або втрати під час транспортування (3). За допомогою страхування можна мінімізувати ризики, пов'язані з небезпечними вантажами, природними лихами, крадіжками, політичною ситуацією та іншими потенційними загрозами. Це дозволяє компаніям зосередитися на своїй основній діяльності, не страхуючи кожен ризик окремо. Страховання відповідальності покриває випадки, коли логістична компанія несе відповідальність перед третіми сторонами за можливі збитки або шкоду. Це особливо важливо у випадках, коли виникають претензії від клієнтів або партнерів.

У підсумку варто зазначити, що безпека в логістиці – це складний та багатоаспектний процес, який вимагає постійного моніторингу, оцінки ризиків та прийняття заходів для запобігання потенційним загрозам. Безпека в логістиці не тільки передбачає захист активів і даних, але і забезпечує неперервність операцій та довіру споживачів до вашого бренду.

Література

Corochii, O. What's it like running a 3PL in war-affected Ukraine? We talk to the head of Zammler Group. *Trans.INFO*. URL: <https://trans.info/3pl-ukraine-war-288674>;

Берестенко, В. Уроки логістики під час війни / Порти України. *Порти України*. URL: <https://ports.ua/uroki-logistiki-pid-chas-vijni/>;

Страхування вантажів – провідна страхова компанія. *Провідна страхова компанія*. URL: <https://www.providna.ua/corp/strakhuvannya-vantazhiv>.

КІБЕРЗАХИСТ ТА НАЦІОНАЛЬНА БЕЗПЕКА: УКРАЇНСЬКИЙ ДОСВІД

Гринік Аліна В'ячеславівна

*Дніпропетровський державний університет внутрішніх справ,
м. Дніпро, Україна*

Ярошевська Тамара Василівна

*доктор юридичних наук, доцент,
Дніпропетровський державний університет внутрішніх справ,
м. Дніпро, Україна*

ORCID: <http://orcid.org/0000-0001-5525-1681>

ПРОБЛЕМНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Кібербезпека в сучасному світі стала однією з найбільш актуальних та важливих проблем. Україна не є винятком і стикається зі значними викликами у цій галузі. Пріоритетні питання забезпечення кібербезпеки України – це захист критично важливих інфраструктур, боротьба з кіберзлочинністю, зміцнення інформаційної безпеки сфери державного управління та особистої безпеки громадян. У цьому контексті важливо розвивати кіберзахист, сприяти освіті та підвищенню кваліфікації фахівців у цій сфері, а також співпрацювати з міжнародними партнерами для спільного реагування на кіберзагрози. Розв'язання цих проблем стане ключовим елементом забезпечення національної безпеки та стійкості України в цифровому віці.

Необхідність розв'язання проблеми кібербезпеки в сучасному суспільстві підтверджується широким спектром порушень у використанні обладнання, програмного забезпечення та інформаційно-комунікаційних технологій, особливо в банківському секторі, сфері захисту інтелектуальних прав,

економічної безпеки, національної безпеки тощо. Стратегія України спрямована на розв'язання цих питань у суспільстві. Зокрема, важливим кроком є прийняття Закону України № 2163-VIII від 5 жовтня 2017 року «Про основні засади забезпечення кібербезпеки України» (Закон України, 2017). Цей закон визначає правові та організаційні засади для забезпечення захисту ключових інтересів людини, громадянина, суспільства та держави в кіберпросторі.

Кібербезпека означає вживання заходів для забезпечення конфіденційності, цілісності та доступності даних у світі інформаційних технологій. Вона спрямована на захист різних ресурсів, включаючи інформацію, комп'ютери, сервери, підприємства та особисті дані. Кібербезпека важлива для забезпечення безпеки даних під час їх передачі та зберігання. Заходи безпеки включають контроль доступу, навчання, аудит та оцінку ризиків, тестування, керування та авторизацію.

Спеціалісти з кібербезпеки розробляють системи захисту для різних мереж зв'язку та електронних баз даних, тестують та вдосконалюють різні рішення, щоб уникнути витоку важливої інформації, такої, яка може містити державну або комерційну таємницю. Ця професія досить молода і стала широко розповсюдженою завдяки впровадженню комп'ютерних та мережевих технологій у різних організаціях, від невеликих комерційних фірм до державних органів безпеки. Створення безпечних комп'ютерних систем і програм є головною метою роботи мережевих інженерів та програмістів, а також об'єктом досліджень у галузі телекомунікацій, інформатики та економіки. Кібербезпека полягає в мінімізації можливих загроз для життєво важливих інтересів особистості, суспільства та держави, які виникають при використанні комп'ютерних систем і телекомунікаційних мереж, шляхом застосування відповідних заходів захисту та мінімізації ризиків, пов'язаних з інформаційними атаками та недозволенним доступом до даних (Баранов, 2014, С. 54).

Зараз все більше дослідників приділяють увагу концепції кібермогутності держави, що передбачає її здатність втілювати свою волю та захищати національні інтереси у кіберпросторі.

Наразі для України питання кібербезпеки та розвитку кібермогутності мають вирішальне значення. Україні необхідно самостійно розробляти шляхи та механізми забезпечення кібербезпеки в обличчі сучасних кіберзагроз, які постають перед нею. Важливо врахувати погляди науковця Д. Дубова, який розділяє кіберзагрози для України на два основних рівні: перший – «класичні» кіберзлочини, які можуть бути як абсолютно новими, так і вже відомими, але вони вимагають сучасних інформаційних технологій для реалізації. Другий рівень – це кібершпиунство та кібердиверсії, які характерні для геополітичних конфліктів (Дубов, 2014).

В сучасному світі досі існують передумови для поширення кіберзагроз. Деякі з цих передумов включають недосконалість нормативно-правової бази у сфері кібербезпеки та її застарілість у галузі захисту інформації. Також, відсутня система незалежного аудиту інформаційної безпеки та механізми розкриття інформації про вразливості, що важливо в умовах постійної цифровізації усіх сфер державного управління та життєдіяльності країни. Враховуючи це, необхідно строго дотримуватися відповідних стандартів.

Однією з основних актуальних загроз є розвідувально-підбивна діяльність в кіберпросторі проти України, яка здійснюється спецслужбами іноземних держав, особливо російською федерацією. Ця діяльність містить кібершпиунство та підбивні акції, спрямовані на порушення нормального функціонування об'єктів критичної інформаційної інфраструктури, таких як системи управління державою, об'єкти життєзабезпечення, електроенергетика, транспорт, ядерна та хімічна промисловість, а також банківська сфера (цивільні кібердиверсії).

Зокрема, Росія активно використовує кіберпростір у формі гібридної агресії проти України, проводячи деструктивні впливи на органи державної влади та системи військового управління та зброї. Ці фактори вимагають постійного розвитку засобів та можливостей у галузі забезпечення кібербезпеки органами безпеки та оборони.

Наразі спостерігається збільшення ризику застосування кібератак, включаючи фішингові атаки, поширення шкідливого

програмного забезпечення, включаючи програми-вимагачі. Ці атаки виконуються як фінансово мотивованими кіберзлочинними групами, так і хакерськими колективами, які можуть бути пов'язані з країнами-агресорами та іншими націями. Збільшення обсягу інформації в базах даних і інформаційних системах, а також посилення відповідальності за витік особистих даних громадян в розвинених країнах, призводить до зростання глобального ринку програм-вимагачів. Ці програми вимагають викупу за розблокування доступу до інформації або за нерозголошення викраденої інформації в Інтернеті. Нині кібератаки частіше спрямовані не безпосередньо на уряди та організації, а здійснюються через зараження популярних додатків, внесення змін до вихідних кодів і процесів оновлень.

Під час війни в Україні значно зросла загроза кібертероризму, що перш за все пов'язано з кіберможливостями російської федерації як держави-агресора, яка проводить ще й кібервійну. Спостерігається також тенденція використання кіберпростору для фінансування терористичних угруповань.

Проте, Україна недостатньо активно взаємодіє з міжнародними партнерами для розробки взаємовигідних механізмів протидії кібертероризму. Збільшення кіберзлочинності в національному сегменті кіберпростору є серйозною загрозою, яка завдає шкоди державним інформаційним ресурсам, суспільним процесам та особисто громадянам, порушуючи довіру громадян до інформаційно-комунікаційних технологій і призводячи до значних матеріальних збитків. Застосування кіберпростору для здійснення інших кримінальних правопорушень, таких як легалізація доходів, одержаних злочинним шляхом, торгівля людьми, незаконний обіг зброї, наркотиків та інших небезпечних речовин, також поширюється й ускладнюється через низький рівень кіберграмотності серед населення, зокрема серед звичайних користувачів електронних послуг (Горун, 2021, С. 102).

Слід зазначити, що головним пріоритетом державної політики з кібербезпеки в Україні є наступні складові:

1. Забезпечення безпеки кіберпростору з метою захисту суверенітету держави та сприяння розвитку суспільства.

2. Захист прав, свобод і законних інтересів громадян України в онлайн середовищі.

3. Інтеграція в європейську та євроатлантичну спільноти в галузі кібербезпеки.

Принципи основної державної політики України в галузі кібербезпеки повинні бути розроблені в комплексному підході, враховуючи національні інтереси та баланс інтересів громадян, суспільства і держави. Створення такої політики передбачає впровадження дієвих заходів у сферах організаційно-правового, технічного, фінансово-економічного, освітнього, наукового та зовнішньополітичного спрямування. Таким чином, пріоритетні питання забезпечення кібербезпеки України вимагають комплексного та національно орієнтованого підходу. Це включає захист кіберпростору для збереження суверенітету та розвитку суспільства, захист прав і інтересів громадян, а також інтеграцію в європейську та євроатлантичну спільноти у сфері кібербезпеки. Ця проблема вимагає не лише правового регулювання, але й наукових досліджень, технічних рішень та активної співпраці як на внутрішньому, так і на міжнародному рівнях для ефективного захисту від сучасних кіберзагроз.

Література

Закон про основні засади забезпечення кібербезпеки України 2017 (Верховна Рада України). Офіційний сайт Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/card/2163-19>

Баранов, О. (2014). Про тлумачення та визначення поняття «кібербезпека». *Інформація і право*, 2 (42), 54-62.

Дубов, Д. В. (2014). *Кіберпростір як новий вимір геополітичного суперництва*: монографія. Київ: НІСД, 328.

Горуш, О. Ю. (2021). Пріоритетні засади державної політики кібербезпеки: організаційно-правовий аспект. *Інформація і право*, 2 (37), 93-102.

Дубель Михайло Володимирович
доктор філософії,
Донецький національний університет імені Василя Стуса,
м. Вінниця, Україна
ORCID: 0000-0003-2229-0419

ЦИФРОВІ ВІРУСИ ЯК СУЧАСНА ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

Перші комп'ютерні віруси не несли загрозу пристроям, на які потрапляли. Один з таких прикладів називався Creeper і не завдавав комп'ютеру-носію ніякої шкоди. Creeper був створений у 1970-х роках, і про зараження цим вірусом користувачі дізнавалися з повідомлення на дисплеї комп'ютера або з роздрукованого на принтері аркуша: I'M THE CREEPER. Вірус просто існував у пам'яті комп'ютера та ніяким чином не впливав на його роботу. Це був свого роду жарт – не більше. Швидше за все, вірус Creeper і не замислювався як програма, яка має деструктивний характер. Згідно з легендою, співробітник BBN Боб Томас створив Creeper, щоб перевірити: чи можливе існування програм, що самовідтворюються, в принципі (Metcalf, 2014).

Комп'ютерні віруси, які цілеспрямовано руйнують комп'ютерну систему, почали масово розроблятися лише у 80-ті роки ХХ століття. Проте творці вірусу, який спровокував справді масштабну епідемію в середині того ж десятиліття, не ставили за мету завдати шкоди. Братам Алві, які тримали комп'ютерний магазин у Пакистані, просто набридло, що клієнти створюють копії їхніх продуктів, що не ліцензуються. Їхній вірус не знищував дані, але заражав завантажувальні сектори дискет і записував на нову дискету мітку ©Brain (назва магазину братів). Завдяки цьому вирахувати авторів вірусу, який випадково заразив не лише «піратів», а й «невинні комп'ютери», виявилось не дуже складним завданням (Avoine, Oechslin, & Junod, 2007).

З часом віруси стали переходити з категорії зброї у відносинах між злочинцями та окремими користувачами до рівню загроз

безпеці певних держав. Одним з перших таких випадків був вірус Stuxnet. The Stuxnet Worm був розроблений у першому десятилітті XXI ст. і є шкідливим програмним забезпеченням, яке «спочатку створене для промислових систем управління або групи аналогічних систем», що використовуються, наприклад, в газопроводах і електростанціях. Кінцевою метою вірусу є «перепрограмування промислових систем управління за допомогою зміни коду на програмованих логічних контролерах (ПЛК), щоб змусити їх працювати так, як задумав зловмисник, і приховати ці зміни від оператора обладнання». Stuxnet став першим відомим комп'ютерним вірусом, здатним цілеспрямовано виводити з ладу промислові системи.

В Ірані в 2010 р. (а можливо і раніше) вірус був застосований в атаці на операційну систему комп'ютерів шляхом доступу до програмного логічного контролера, який керує механізмом для включення центрифуг, призначених для виділення та збагачення урану. Доступ до системи було отримано через операційну систему Microsoft Windows та внутрішні комп'ютерні мережі, які, у свою чергу, забезпечили доступ до програмного забезпечення концерну Siemens, що використовується в іранському ядерному науковому центрі в Натанзі. Центрифуги під впливом вірусу розвинули дуже велику швидкість обертання, що призвело до їхнього руйнування. Внаслідок цієї кібердиверсії було знищено близько 20 відсотків усіх центрифуг на заводі загальним числом не менше ніж 1000 (Langner, 2013).

Наша держава теж зазнавала витрат, що були пов'язані з кібератаками за допомогою комп'ютерних вірусів. Найвідоміший подібний випадок трапився у 2017 році.

У 2017 році інформаційні системи України вразив комп'ютерний вірус-вимагач Petya.A. Вірус використовував недоліки в системі безпеки Windows, блокував і шифрував сектор завантаження системи, і, таким чином, змінив його на власний.

Під впливом дії вірусу було відключено та порушено роботу сайтів Міністерства внутрішніх справ, Чорнобильської АЕС, Секретаріату Кабінету міністрів, сайтів «Нової пошти», «Укртелекому», «Ощадбанку», «ТАСкомбанку», «ДТЕК», «Київенерго», сайтів заправки «Вог», оператора «Київстар»,

«Укргазбанк», «Епіцентр» та інших. Крім зовнішніх веб-сайтів, була порушена робота платіжних систем кількох банків, також поразки зазнали роздрібні мережі та страхові компанії. Було вражено вірусом системи Міністерства інфраструктури, Укртелекому, Укрпошти, Укрзалізниці, аеропорту "Бориспіль", "Нової пошти". Фахівці з кібербезпеки надають пояснення, що поразка систем вірусом Petya.A, як і здебільшого поразка іншими аналогічними вірусами, здійснюється через користування електронною поштою, і рекомендують не відкривати вкладення, якщо вони надійшли від невідомих адресатів. Адже ігнорування правил безпеки привело до такого масштабного зараження.

Як певна відповідь на цю вірусну атаку було прийняття закону, який у травні 2018 року набув чинності, «Про основні засади забезпечення кібербезпеки України» (Радіо Свободи).

У документі були визначені повноваження та обов'язки як державних, так і приватних установ, організацій та громадян у сфері кібербезпеки, а також визначені базові терміни, які з'явилися в українському законодавстві вперше: кіберзагроза, кібершпигунство, кіберзлочинність та інші.

Законом передбачене створення Національної телекомунікаційної мережі та Державного центру кіберзахисту.

Перед початком повномасштабного вторгнення у лютому 2022 року, з боку Росії відбувалися декілька кібератак на українські державні сайти у січні та лютому 2022 року. На підставі даних дослідження, що було проведене компанією ESET, після DDoS атаки 23 лютого на сайтах, що були пошкоджені, почали працювати шкідливі програмні засоби HermeticWiper, названий за цифровий сертифікат підпису коду від кіпрської компанії Hermetica Digital Ltd. Мета впливу цих шкідливих програм – знищення інформації з баз даних. Вірус було виявлено близько 17:00 23 лютого, однак мітка часу вказує, що він був скопійований 28 грудня 2021 року (ESET).

Ще більше атак на ресурси України було здійснено у період з 24 лютого 2022 року. Все це підкреслює, що лише постійні оновлення кібербезпеки можуть зберегти інформаційну цілісність простору нашої держави і, як наслідок, повноцінне функціонування інфраструктури.

Література:

Metcalf, J. (2014). Core War: Creeper & Reaper.
URL: <https://corewar.co.uk/creeper.htm>

Avoine, G., Oechslin, P., Junod, P. (2007). *Computer System Security: Basic Concepts and Solved Exercises*. EPFL Press.

Kushner, D. (2013). The Real Story of Stuxnet. *IEEE Spectrum*.
URL: <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>

Рік після атаки вірусу Petya: що змінилося в кібербезпеці України. *Радіо Свобода*. URL: <https://www.radiosvoboda.org/a/29336511.html>

HermeticWiper: New data-wiping malware hits Ukraine.
URL: <https://www.eset.com/gr-en/about/newsroom/press-releases/hermeticwiper-new-data-wiping-malware-hits-ukraine/>

Горошко Олександр Леонідович
Ніжинський державний університет імені Миколи Гоголя,
м. Ніжин, Україна
ORCID: 0009-0003-6518-4832

ПЕРСПЕКТИВИ НАВЧАННЯ КІБЕРБЕЗПЕКИ В ОСВІТНІХ ІНСТИТУЦІЯХ

У сучасному світі, цифрові та інтерактивні технології впливають практично на всі аспекти нашого життя. Мабуть не має такої галузі, де цифрові технології не відіграють роль. Зі зростаючою кількістю кіберзлочинів, навчання кібербезпеці стає надзвичайно важливим завданням для освітніх закладів. Ця проблема неодноразово згадується в різних контекстах та є ключовою для забезпечення безпеки в цифровому світі.

В основні поняття кібербезпеки або cyber security лежить здатність запобігати кібератакам через активні заходи для передбачення можливих кіберзагроз з боку зловмисників та протидія їх вторгненням. Всі стратегії та тактики кіберзахисту спрямовані на одну загальну мету – запобігати подібним загрозам, виявити їх та реагувати на них (Що таке кібербезпека).

Кібербезпека, визначена як заходи та стратегії для захисту інформації, комп'ютерних систем та мереж від кібератак. Вона охоплює велику кількість аспектів, включаючи захист даних, мереж, програмного забезпечення, інфраструктури та протидії кіберзлочинності. Враховуючи безперервне зростання обсягу загальної інформації, інформаційна безпека стає край важливою.

Навчання з кібербезпеки, що пропонуються в освітніх інститутах, відіграють важливу роль у розвитку необхідних компетентностей громадян та фахівців у галузі кібербезпеки. Воно допомагає розуміти потенційні загрози, розрізнити їх та приймати відповідні заходи для їх запобігання. Знання та навички, набуті під час навчання, створюють базу для безпеки суспільства в цілому.

Сучасні освітні заклади, спеціалізовані у навчанні кібербезпеки, пропонують різноманітні навчальні програми в цій

галузі. Важливо відзначити, що для успішної підготовки фахівців у цій сфері важлива матеріально-технічна база, яка відіграє досить важливу роль. Деякі інституції надають комплексні курси, з фокусом на практичному досвіді та лабораторних роботах, тоді як інші можуть обмежуватися базовим теоретичним навчанням.

Безсумнівно, навчання кібербезпеці важливо, проте існують обмеження, які суттєво впливають на його ефективність та поширення. Одна із основних проблем полягає в недостатньому фінансуванні. Розвиток та підтримка програм навчання вимагають значних інвестицій, які не завжди доступні в сучасних умовах. Для успішної реалізації навчальних програм з необхідна належна матеріально-технічна база. Студенти потребують доступу до сучасних комп'ютерних систем, спеціалізованого програмного забезпечення та лабораторних засобів для вдосконалення своїх навичок у практичних завданнях. Також заклади освіти можуть стикатися з проблемами, пов'язаними з відсутністю кваліфікованих викладачів, оскільки – це динамічна галузь, і викладачі повинні мати актуальні знання та досвід у цій сфері, щоб ефективно передавати їх студентам. Доступ до сучасних технічних ресурсів також є ключовим обмеженням. Без доступу до яких, студенти можуть бути обмежені в можливостях набувати практичний досвід та навички, які є важливими в галузі кібербезпеки.

Для подолання цих обмежень, освітні заклади повинні активно співпрацювати з індустрією, залучати фінансову підтримку та розробляти стратегії для забезпечення належної матеріально-технічної бази та викладачів з відповідними знаннями та досвідом.

Переваги навчання кібербезпеки в освітніх інституціях сприяє підвищенню рівня кіберграмотності серед студентів та учнів. Вони набувають знань та навичок, які допомагають розпізнавати потенційні загрози та застосовувати заходи для їх запобігання. Це важливо для особистої безпеки і безпеки їхніх даних в цифровому середовищі. Крім того, науковий предмет кібербезпеки важливо впроваджувати не лише в спеціалізованих освітніх закладах, але й у загальноосвітніх навчальних закладах. Інтеграція курсів кібербезпеки в загальну освітню програму дозволяє більшій

кількості студентів отримувати базові знання та навички з цієї сфери, сприяє формуванню загальної грамотності серед населення щодо потенційних загроз та вміння захищати свої особисті дані, що сприяє підготовці більш свідомих громадян, які можуть більш ефективно захищати себе та свої дані в цифровому світі.

Освіта в галузі кібербезпеки створює можливості для студентів та випускників розглядати кар'єру в цій галузі. Зростаючий попит на фахівців з кібербезпеки відкриває широкі перспективи для молодих спеціалістів. Вони можуть працювати в різних галузях, включаючи корпоративну безпеку, урядові структури, фінансову та медичні сфери, сфери енергетики, освіти та сфери інтернету речей – що в свою чергу зачіпляє IoT-технології в енергетиці, системи «розумне місто», медичними IoT-пристрої, безпілотні автомобілі та інше (10 найпопулярніших сфер).

Навчання кібербезпеки сприяє зміцненню цифрового суспільства в цілому. Громадяни, які розуміють загрози та ризики в цифровому середовищі, стають активними учасниками в створенні безпечного та стійкого інтернет-середовища. Вони можуть брати участь у цифровому громадянському суспільстві та впливати на політику безпеки в цифровому просторі.

Порівняння освітніх програм показало наявність спільних та відмінних аспектів у підготовці бакалаврів з кібербезпеки в університетах України та США. Оцінка змісту та вимог до результатів навчання дозволили визначити сильні та слабкі сторони кожної програми. Застосування наукових здобутків та передового досвіду з підготовки фахівців з кібербезпеки в США може допомогти вдосконалити систему підготовки фахівців в Україні. Рекомендується впровадження стандартизації, дуального та змішаного видів навчання, використання новітніх технологій та мотивування професорсько-викладацького складу. Загальний результат дослідження підкреслює необхідність розвитку галузі кібербезпеки, а також вдосконалення підготовки фахівців в Україні з урахуванням міжнародного досвіду та вимог ринку праці (Бистрова, 2017).

Інформаційна безпека завжди була об'єктом вивчення та викладання в контексті різних комп'ютерних дисциплін у вищій освіті з самого початку епохи сучасних обчислювальних систем. Протягом цього часу зростає необхідність в забезпеченні безпеки обчислювальних систем, що постійно посилювалася.

Внаслідок глобальних криз відбулося посилення уваги до безпеки інформаційної інфраструктури, саме так і з'явилася галузь "кібербезпеки", яка викликає міжнародну зацікавленість і підтримку. Еволюція кібербезпеки останнім часом свідчить про її становлення як справжньої академічної галузі, а не лише області навчання для фахівців у певних спеціалізованих сферах. Кібербезпеку можна офіційно визначити як метадисципліну з різними спеціалізованими напрямками, кожен із яких характеризується загальною моделлю компетентності, що сприятиме покращенню розуміння того, як кібербезпека розвивається, і сприятиме створенню стандартів і цілей для різних програм навчання в галузі кібербезпеки.

Навчання кібербезпеки в освітніх інституціях є кроком до створення безпечного, цифрового світу. Допомогає підвищити кіберграмотність, готувати майбутніх фахівців та зміцнювати наше суспільство. Незважаючи на виклики, які стоять перед освітніми закладами, навчання кібербезпеки повинно залишатися пріоритетом. Для подальшого розвитку цієї галузі важливо проводити дослідження та впроваджувати найкращі практики, співпрацювати з галузевими компаніями та розробляти стандарти навчання. Співпраця між освітніми інститутами та індустрією кібербезпеки сприятиме покращенню якості практичного навчання. Слід підкреслити важливість уваги до педагогічних аспектів навчання кібербезпеці. Забезпечення якості підготовки фахівців з кібербезпеки є актуальним завданням. Перспективи розвитку полягають у впровадженні передових педагогічних методик та стандартів забезпечення якості в освітній процес. Це сприятиме підвищенню рівня підготовки фахівців у галузі кібербезпеки та відповідатиме

вимогам сучасного інформаційного суспільства, яке потребує компетентних спеціалістів у цій області для забезпечення безпеки та захисту інформації.

Література

10 найпопулярніших сфер використання інтернету речей. *Blog Imena.UA*. URL: <https://www.imena.ua/blog/top-10-score-iot/>

Parrish, A., Impagliazzo, J., Raj, R., Santos, H., Asghar, M. R., Jøsang at al. (2018). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. 36-54

Бистрова, Б. В. (2017). Модернізація освітньої програми "Кібербезпека": реалії та перспективи. *Науковий вісник Мукачівського державного університету. Серія: Педагогіка та психологія*, 2, 22-24. URL: http://nbuv.gov.ua/UJRN/nvmdupp_2017_2_5.

Бистрова, Б. (2017). Основні поняття досягнення та концептуальні засади професійної підготовки фахівців із кібербезпеки. *Педагогічні науки: теорія, історія, інноваційні технології*, 8, 58-70.

Що таке кібербезпека - Заходи забезпечення кібербезпеки. URL: <https://dan-it.com.ua/uk/blog/chto-takoe-kiberbezopasnost-mery-obespechenija-kiberbezopasnosti/>

Обіход Тетяна Вікторівна

*кандидат фізико-математичних наук, доцент,
Київський університет ринкових відносин, Київ, Україна
старший науковий співробітник
Інституту ядерних досліджень НАН України
ORCID: 0000-0003-1103-4006*

Біленчук Петро Дмитрович

*кандидат юридичних наук, доцент,
професор Європейської академії прав людини
ORCID: 0000-0002-9599-0347*

КІБЕРБЕЗПЕКА УКРАЇНИ: ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ЇЇ ЗАБЕЗПЕЧЕННЯ

Кібербезпека (КБ) в Україні є важливим питанням, яке постійно еволюціонує. У країні були досягнуті певні перемоги у сфері КБ, але є й недоліки, які потребують уваги. Деякі досягнення включають створення національних кібербезпекових організацій, удосконалення законодавства. Створено Стратегію кібербезпеки України (2021–2025 роки) під назвою БЕЗПЕЧНИЙ КІБЕРПРОСТІР – ЗАПОРУКА УСПІШНОГО РОЗВИТКУ КРАЇНИ (Указ Президента України, 2021). Також було зроблено кроки для забезпечення КБ критично важливої інфраструктури, такої як енергетика, транспорт і фінанси. Проведено заходи щодо зберігання, передачі та оброблення баз даних із застосуванням сучасних інформаційно-комунікаційних технологій, а також приділено увагу відповідній підготовці фахівців для забезпечення КБ нашої країни. Такі заходи сприяють зміцненню обороноздатності країни проти кібератак. Однак, недоліки існують і вимагають подальших зусиль. Один з головних недоліків полягає у низькій кіберосвіченості населення. Багато людей не мають достатніх знань про КБ і стають жертвами кіберзлочинців. Тому необхідно працювати над підвищенням свідомості людей про цілеспрямовані атаки, фішинг, розповсюдження шкідливих програм і т.д. Також важливим є завдання з посилення захисту

державних і корпоративних інформаційних систем. Україна є метою кібератак з боку інших країн та груп хакерів, тому системи захисту повинні бути постійно оновлювані й вдосконалювані для протидії таким загрозам. Для протидії протиправній діяльності спецслужб іноземних держав необхідно збільшити роль спеціальних служб і правоохоронних органів в системі КБ України. Отже, хоча українська КБ розвивається, важливо продовжувати працювати над усуненням недоліків та посиленням заходів безпеки, щоб забезпечити захист національної інформації та інфраструктури.

Однією із складових КБ є її *правове забезпечення* на інфраструктурних об'єктах, оскільки воно є важливим аспектом для захисту від кібератак та забезпечення стабільності роботи критичних систем (Даник, 2019, С. 142). У багатьох країнах існують закони, положення та регуляції, які стосуються КБ на інфраструктурних об'єктах. Наприклад, в США діє Закон про кібербезпеку Інформаційних систем Критичної Інфраструктури (CISA), який визначає правила для захисту критичних інфраструктурних об'єктів від кіберзагроз. Ця організація має провідний досвід у питаннях захисту об'єктів критичної інфраструктури (ОКІ). Україна намагається співпрацювати з цією організацією через меморандум про співпрацю між Держспецзв'язком як уповноваженим органом у сфері захисту критичної інфраструктури України. Відповідно, в Україні створені секторальні переліки ОКІ, були проведені навчання відповідно до методики CISA, напрацьовується необхідна нормативно-правова база, прийнята постанова КМУ "Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього" від 28 квітня 2023 р. № 415. Проведено диференціацію захисту ОКІ за формою і рівнем відповідальності:

- захист об'єктів критичної інфраструктури виконується її операторами;
- ЗСУ здійснюють безпеку від ракетних обстрілів;
- СБУ - проти диверсій;
- Держспецзв'язку - проти кібератак.

Основні елементи забезпечення КБ на інфраструктурних об'єктах повинні включати:

1. Законодавчі акти: Уряд може ухвалити закони та положення, які визначають вимоги до кібербезпеки для певних секторів, таких як електроенергетика, транспорт, фінанси тощо;

2. Регуляторні рішення: органи регулювання можуть ухвалювати рішення щодо кібербезпеки, наприклад, вимагати встановлення певних заходів безпеки або здійснювати перевірки впровадження цих заходів;

3. Інформаційний обмін: Уряд може створити спеціальні механізми для обміну інформацією про кіберзагрози та ризики між державними органами та операторами інфраструктури;

4. Санкції та штрафи: у разі порушення вимог кібербезпеки, органи державного контролю можуть застосовувати адміністративні штрафи або приймати судові рішення проти операторів інфраструктури.

Правове забезпечення повинно бути комплексним та актуальним і враховувати специфіку кожного сектору, оскільки загрози КБ постійно змінюються.

Важливою складовою захисту України є *кіберосвіченість населення*, оскільки вона виступає показником готовності та здатності людей використовувати інформаційно-комунікаційні технології (ІКТ) в повсякденному житті. Розвиток людської спільноти пов'язаний з необхідністю безпеки від загрози збройних соціальних конфліктів. Тому проблеми безпеки розглядалися ще античними філософами Платоном й Аристотелем, Т. Гоббсом, Н. Макіавеллі та ін. Сучасна політична ситуація у світі відзначається високим рівнем конфліктності, що стимулює інтерес до КБ. Кіберосвіченість населення охоплює різні аспекти, такі як доступ до Інтернету, володіння навичками використання комп'ютерів та програмного забезпечення, цифрова грамотність та безпека в Інтернеті. Заходи щодо кіберосвіченості населення можуть включати проведення навчальних програм та тренінгів з цифрової грамотності, створення громадських центрів доступу до Інтернету, підтримку розвитку інфраструктури для бездротового Інтернету, сприяння доступності та використанню електронних послуг та інтернет-ресурсів, а також забезпечення

безпеки та конфіденційності в Інтернеті. Так, у складі Департаменту внутрішньої безпеки (Department of Homeland Security's (DHS)) США сформовано відділ освіти та підвищення освіченості з питань КБ і прийнято ряд документів:

1. Національна програма підвищення освіченості з питань КБ.
2. Національна програма розвитку професіоналізму та розвитку персоналу.
3. Національна програма освіти та тренінгу у галузі КБ (National Cybersecurity Education and Training Program (NCTEP)).

Кіберосвіченість населення є важливою, оскільки вона допомагає забезпечити рівний доступ до інформації та можливостей, сприяє освіті та розвитку, полегшує комунікацію та спілкування, а також сприяє цифровому розвитку суспільства.

Ще однією ланкою КБ є *захист державних і корпоративних інформаційних систем*. Ось кілька основних засобів, які можуть допомогти посилити захист таких систем:

1. Криптографічне шифрування;
2. Аутентифікація та авторизація: Використання механізмів аутентифікації (наприклад, паролі, біометричні дані, двофакторна аутентифікація) для перевірки ідентичності користувачів, а також систем авторизації для контролю рівня доступу до системи та даних;
3. Фізичний захист: Забезпечення фізичної безпеки серверних кімнат, дата-центрів та інших приміщень, в яких знаходяться обладнання та системи збереження даних;
4. Захист мережі: Встановлення мережевих брандмауерів, розгалужувальників та інших пристроїв для моніторингу, перехоплення та блокування потенційно шкідливого трафіку, який може завдати шкоди системам або даним;
5. Системи виявлення та запобігання вторгнення: Використання спеціалізованих програмних продуктів, які дозволяють відслідковувати та реагувати на спроби несанкціонованого доступу до системи та зловживання правами користувачів;
6. Резервне копіювання та відновлення даних для забезпечення можливості швидкого відновлення інформації у разі втрати або пошкодження;

7. Навчання та освіта: Освіта користувачів щодо безпеки ІТ, навчання співробітників про правила безпеки та захисту даних, свідоме використання паролів та обізнаність про загрози безпеки.

Ці засоби варто використовувати в комплексі та регулярно оновлювати для оптимального захисту державних і корпоративних інформаційних систем від потенційних загроз.

Література

Даник, Ю. Г., Воробієнко, П. П., Чернега, В. М. (2019). *Основи кібербезпеки та кібероборони: підручник*. Одеса: ОНАЗ ім. О.С. Попова.

Указ про Стратегію кібербезпеки України 2021 (Президент України).

Галюга Катерина Миколаївна
*ВСП «Ніжинський фаховий коледж
Національного університету біоресурсів
та природокористування України»,
м. Ніжин, Україна*

Орел Ольга Володимирівна
*кандидат педагогічних наук,
ВСП «Ніжинський фаховий коледж
Національного університету біоресурсів
та природокористування України»
м. Ніжин, Україна*

ЯК ЗАХИСТИТИ СВОЇ ОСОБИСТІ ДАНІ ВІД КІБЕРАТАК

У сучасному світі особисті дані є цінним товаром. Вони можуть бути використані для крадіжки грошей, маніпуляції людьми, а також для порушення приватності. Кібератаки на особисті дані є одним із найпоширеніших видів кібератак (Петков, Журавльов, Дрозд, Дрозд, 2022).

Кібератака – це зловживання або несанкціоноване використання комп'ютерних систем, мереж або електронних пристроїв з метою отримання несанкціонованого доступу до даних, перешкоджання нормальному функціонуванню системи або завдання шкоди власнику системи. Кібератаки можуть бути спрямовані на різні цілі, включаючи урядові організації, корпорації, фінансові установи, медичні установи та приватних користувачів (Перелік кібератак).

Кібератаки можуть містити такі види загроз, як віруси, черви, троянські програми, фішингові атаки, DoS (Denial of Service) або DDoS (Distributed Denial of Service) атаки, рейдерство аккаунтів, крадіжку особистих даних та багато інших. Внаслідок кібератак може бути скомпрометована цілісність, конфіденційність та доступність особистих даних користувача (Перелік кібератак).

Види кібератак на особисті дані

Аналізуючи підручник з Кібербезпеки (Петков, Журавльов, Дрозд, Дрозд, 2022), можна виділити терміни, які належать до кібератак на особисті дані:

- Фішинг – це вид шахрайства, при якому зловмисники надсилають підроблені електронні листи або повідомлення, які видаються за законні. У цих листах або повідомленнях користувачів просять ввести свої особисті дані, такі як ім'я, пароль, номер банківської картки тощо.

- Зловмисне програмне забезпечення – це програмне забезпечення, яке розроблено для завдання шкоди комп'ютеру або мережі. Зловмисне програмне забезпечення може бути використане для крадіжки особистих даних, а також для порушення роботи комп'ютера.

- Взлом – це процес несанкціонованого доступу до комп'ютера або мережі. Зловмисники, які зламали комп'ютер або мережу, можуть отримати доступ до особистих даних, які зберігаються на цих пристроях.

Кібератаки можуть мати серйозний вплив на особисті дані користувача. Це може призвести до втрати грошей або крадіжки особистої, фінансової та медичної інформації. Крім того, такі атаки можуть пошкодити вашу репутацію та безпеку (9 Cybersecurity Tips).

Наприклад, у червні 2023 року було повідомлено про кібератаку на уряд США, яка стала причиною витоку особистих даних мільйонів американців (Cybersecurity).

Щоб захистити свої дані від кібератак, рекомендується використовувати сильні паролі, оновлювати програмне забезпечення та не давати доступ до своїх даних невідомим особам (9 Cybersecurity Tips).

Щоб захистити свої дані від кібератак, рекомендується використовувати сильні паролі, оновлювати програмне забезпечення та не давати доступ до своїх даних невідомим особам (9 Cybersecurity Tips).

Ось кілька додаткових порад (Cybersecurity):

1. Використовуйте двофакторну автентифікацію (2FA) для додаткового захисту своїх облікових записів.

2. Використовуйте віртуальну приватну мережу (VPN), коли ви користуєтеся публічним Wi-Fi.

3. Не зберігайте конфіденційну інформацію на пристроях, якщо це необхідно, то використовуйте шифрування.

4. Використовуйте програми, які забезпечують конфіденційність та безпеку вашої інформації.

Шкода від кібератак на особисті дані

Кібератаки на особисті дані можуть призвести до наступних наслідків (Гончарова, 2022):

- Фінансові збитки – зловмисники можуть використовувати особисті дані для крадіжки грошей, наприклад, для здійснення шахрайських операцій з банківською картою.

- Порушення приватності – зловмисники можуть використовувати особисті дані для маніпуляції людьми, наприклад, для поширення дезінформації або для здійснення шантажу.

- Порушення роботи комп'ютера або мережі – зловмисне програмне забезпечення може призвести до порушення роботи комп'ютера або мережі, що може призвести до фінансових втрат або до порушення діяльності організації.

Заходи щодо захисту особистих даних

Для захисту особистих даних від кібератак можна вжити наступних заходів (Protecting yourself from cyber attacks):

- Створіть сильні паролі – паролі повинні бути складними і містити як мінімум 12 символів, у тому числі цифри, букви та спеціальні символи.

- Використовуйте двофакторну аутентифікацію – двофакторна аутентифікація додає додатковий рівень безпеки до вашого облікового запису.

- Будьте обережні з тим, яку інформацію ви вводите в Інтернеті – ніколи не вводьте особисті дані на ненадійних сайтах.

- Завантажуйте антивірусне програмне забезпечення – антивірусне програмне забезпечення допомагає захистити ваш комп'ютер від зловмисного програмного забезпечення.

- Регулярно оновлюйте програмне забезпечення – оновлення програмного забезпечення часто містять виправлення безпеки, які можуть допомогти захистити ваш комп'ютер від кібератак.

Додаткові заходи щодо захисту особистих даних

Ось кілька додаткових заходів, які можна вжити для захисту особистих даних (Гончарова, 2022):

- Будьте обережні з тим, як ви використовуєте соціальні мережі – не надсилайте особисту інформацію, таку як номер телефону або адресу, незнайомим людям.
- Користуйтеся безпечними Wi-Fi-мережами – не вводьте особисті дані на незахищеному Wi-Fi-роутері.
- Будьте обережні з тим, що ви зберігаєте на своєму комп'ютері – регулярно робіть резервні копії важливих файлів.
- Вчіть своїх дітей про безпеку в Інтернеті – поговоріть з ними про ризики кібератак і про те, як їх уникнути.

Важливість освіти в галузі кібербезпеки

Освіта в галузі кібербезпеки є важливим фактором для підвищення рівня захисту особистих даних. Люди, які знають про кібератаки та про те, як їх уникнути, менш схильні стати жертвами цих атак (Гончарова).

Уряди, підприємства та організації можуть відігравати важливу роль у поширенні освіти в галузі кібербезпеки. Вони можуть проводити інформаційні кампанії, розробляти навчальні програми та навчати людей про кібератаки та про те, як їх уникнути (Protecting yourself from cyber attacks).

Хотіла вам запропонувати кілька додаткових рекомендацій, які можуть допомогти захистити ваші особисті дані:

- Використовуйте різні паролі для різних облікових записів – це допоможе захистити ваші дані, якщо один із ваших облікових записів буде скомпрометований.
- Уникайте використання слабких паролів – паролі не повинні бути легко відгадати, наприклад, "123456" або "password".
- Не надсилайте особисті дані електронною поштою – якщо вам потрібно надіслати особисту інформацію, використовуйте безпечний сервіс, наприклад, шифрування.
- Будьте обережні з тим, як ви користуєтеся публічними Wi-Fi-мережами – ці мережі можуть бути не захищені, що може дозволити зловмисникам отримати доступ до ваших даних.
- Регулярно перевіряйте свої облікові записи на наявність несанкціонованого доступу – якщо ви помітите будь-які підозрілі активності, негайно змініть паролі.

Ці рекомендації допоможуть вам захистити свої особисті дані від кібератак.

Особисті дані є цінним товаром, і їх захист від кібератак є важливим завданням.

Отже, кібератаки загрожують цілісності особистих даних користувача, завдяки чому несанкціоновані особи можуть отримати доступ до конфіденційної інформації та використовувати її злочинним чином. Для захисту своїх особистих даних важливо використовувати надійні паролі, оновлювати програмне забезпечення, бути обережними при відкритті невідомих посилань та використанні публічних Wi-Fi мереж, ащоб додатково захистити свої дані, можна розглянути використання шифрування, двофакторної аутентифікації та виконувати регулярні резервні копії важливих даних. Важливо також бути обережним із розкриттям особистих даних в Інтернеті та уникати недовірливих джерел та неперевірених додатків.

Якщо ви стали жертвою кібератаки або підозрюєте, що ваші особисті дані були скомпрометовані, рекомендується негайно повідомити про це відповідні організації або локальну поліцію, змінити паролі на всіх важливих облікових записках та вжити заходів для запобігання подальшим атакам.

Література

Петков, С. В., Журавльов, Д. В., Дрозд, О. Ю., Дрозд, В. Г. (2022). *Кібербезпека в Україні: нормативна база, коментарі та роз'яснення, актуальна судово практика*. Київ: ЦУЛ.

Cybersecurity Ready.gov. URL: <https://bing.com/search?q=how+to+protect+personal+data+from+cyber+attacks>

9 Cybersecurity Tips to Stay Protected in 2023. *How-To Geek*. URL: <https://www.howtogeek.com/778547/cybersecurity-tips-to-stay-protected/>

Перелік кібератак. URL: https://uk.wikipedia.org/wiki/Перелік_кібератак

Protecting yourself from cyber attacks - Washington State Department of URL: <https://dfi.wa.gov/consumers/cyber-attacks-tips>

Гончарова, І. П. (2022). *Кібербезпека в цифровому освітньому середовищі закладів професійної освіти: електронний навчальний курс*. Біла Церква, БІНПО ДЗВО «УМО» НАПН УКРАЇНИ.

Кондратьєва Крістіна Авінашівна
*Донецький національний університет імені Василя Стуса,
м. Вінниця, Україна*

МІСЦЕВА ЕЛЕКТРОННА ДЕМОКРАТІЯ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ: ПИТАННЯ ЕФЕКТИВНОСТІ

В сучасному світі, де демократія та цифрові технології залишаються невід'ємною частиною суспільного життя, питання забезпечення демократичних процесів в умовах воєнного стану набувають особливої актуальності. Особливо гостро дане питання стоїть в Україні, на території якої тривають воєнні дії.

Воєнний стан, який запроваджено в Україні з 24 лютого 2022 року у зв'язку з повномаштабним вторгненням РФ, накладає серйозні обмеження на звичайні демократичні процеси та права громадян. Але в той же час, він створює підвищену потребу в засобах участі громадян у прийнятті важливих рішень, що стосуються їхнього життя, безпеки та майбутнього. Місцева електронна демократія є одним із таких засобів. Так, електронні технології, включаючи Інтернет та мобільні додатки, можуть надати громадянам можливість висловлювати свої думки, брати участь у громадських обговореннях та впливати на рішення, що стосуються їхніх життєвих інтересів.

Сьогодні місцева електронна демократія представлена передусім сайтами місцевих рад та низкою місцевих спеціалізованих сервісів, серед яких Контактний центр Києва (в 2022 році було зареєстровано 22 380 електронних звернень громадян, з яких 9 242 було вирішено (Контактний центр Києва, 2023), «Цілодобова варта» Вінниці (в 2022 році було зареєстровано 2 293 е-звернення, з яких було виконано 1859) (Вінницька міська рада, 2023). Подібні звернення обробляються та виконуються протягом робочого тижня. Так, питання про відсутність газу та гарячої води вирішуються протягом 3-4 днів.

Потребує уваги й такий портал як «Відкрите місто», що існує на веб-платформі «Єдина платформа місцевої електронної демократії» (або e-DEM) та направлений на вирішення комунальних та інфраструктурних проблем. В жовтні 2023 р. сервісом користувалося вже 101 місто. За його допомогою було вирішено понад 30389 місцевих проблем (Відкрите місто, 2023).

Громади також використовують послугу “Громадські консультації” для обговорення проєктів нормативно-правових актів. Поряд з тим на платформі e-DEM зазначено про проведення 2070 консультацій, проте детальна інформація відсутня, що може свідчити про обмеженість даної функції під час воєнного стану (DEM консультації з громадськістю, 2023). Окрім того, проведений аналіз сайтів Вінницької ОВА та районних військових адміністрацій показує, що тільки на сайтах Вінницької, Хмельницької, Гайсинської та Жмеринської районних військових адміністраціях присутні форми електронних консультацій з громадськістю. Після аналізу звітів за результатами проведення консультацій, в тому числі й електронних, було виявлено, що майже всі звіти (99%) містять формулювання „Пропозиції та зауваження від громадськості не надходили” (Вінницька обласна Вінницька обласна військова адміністрація, 2023).

Іншим механізмом е-демократії є “Громадський бюджет”, яким в 2023 році скористалися в 245 громадах. Через цей сервіс було реалізовано 9025 проєктів місцевих активістів та ініціативних груп, серед яких 470 у Вінницькій області (Громадський бюджет, 2023). Проте варто зазначити, що в 2022 та 2023 роках багато муніципалітетів України, зокрема і Вінницької області, фактично втратили так звані “бюджети участі”. Цільові кошти, які закладалися в бюджетах міст та громад для реалізації низових ініціатив були перенаправленні на військові потреби.

Ефективним механізмом е-демократії, навіть в час війни, є електронні петиції, які стали для громад одним з основних способів впливу на місцеву владу. Сьогодні на місцевому рівні ефективно функціонує дві системи е-петицій: Єдина система місцевих е-петицій та сервіси е-петицій на сайтах місцевих рад. Єдина система місцевих петицій включає 338 громад в Україні. Станом на жовтень 2023 року було подано 24504 е-петицій

(Місцеві петиції, 2023). Серед сервісів е-петицій на сайтах місцевих рад успішно зарекомендував себе портал е-петицій Київської міської ради, де, для прикладу, з 2015 р. було опубліковано 7 922 електронних петицій, за які було віддано 4 782 122 голосів та реалізовано владою 103 (Електронні петиції, 2023). Основні теми, які піднімаються в петиціях доцільно розділити на такі групи: дерусифікація, патріотична тематика, продаж алкоголю, транспорт, благоустрій, освіта та інші.

Про ефективність е-демократії можемо говорити, дивлячись на показники індексу е-участі. Так, в 2022 р., Україна посіла 57 місце в рейтингу, отримавши 0,60 балів з 1. Для порівняння її результат. в 2020 р. склав 0,81 бали і 46 місце в рейтингу (Ukraine E-Government, 2020; Ukraine E-Government, 2022). Тут, варто зауважити, що основною з причин падіння рейтингу е-участі є централізація влади, спричинена воєнним станом. Поряд з тим, слід відмітити позитивні тенденції Індексу місцевого онлайн-сервісу LOSI. Так, на прикладі Києва помітний стрімкий розвиток місцевого онлайн-сервісу в Україні – 50 місце за рейтингом 2020 року і 21 за рейтингом 2022 року (UN E-Government. City Data, 2020; UN E-Government. City Data, 2022).

Отже, як бачимо, воєнний стан вніс свої корективи в систему взаємодії між владою та суспільством не тільки на загальнонаціональному рівні, а й на місцевому. Ефективними механізмами електронної участі стали е-петиції та е-звернення. Поряд з тим, в рамках безпеки, значно обмежився доступ до публічних даних, рідшою стала практика проведення публічних консультацій, кошти призначені на реалізацію «бюджетів участі» перенаправляються на військові потреби.

Література

Платформа електронної демократії (2023). *Відкрите місто*. URL: <https://opencity.e-dem.ua/about>

Вінницька обласна військова адміністрація (2023). *Офіційний веб-сайт Вінницької обласної військової адміністрації*. URL: <https://www.vin.gov.ua/>

Громадський бюджет (2023). *Платформа електронної демократії*. URL: <https://budget.e-dem.ua/landing>

DEM консультації з громадськістю (2023). *Платформа електронної демократії*. URL: <https://consult.e-dem.ua/>

Електронні петиції (2023). *Київська міська рада*.
URL: <https://petition.kyivcity.gov.ua/>.

Контактний центр Києва. 1551 (2023). URL: <https://1551.gov.ua/>.

Місцеві петиції (2023). *Платформа електронної демократії*.
URL: <https://petition.e-dem.ua/>

«Цілодобова варта». (2023). *Вінницька міська рада*.
URL: <https://www.vmr.gov.ua/1560>.

Local E-Government Development (2020). *Chapter 3. United Nations E-Government Survey*. URL: <https://publicadministration.un.org/egovkb/en-us/Data/City/dataYear/2020>

Local E-Government Development (2022). *Chapter 3. United Nations E-Government Survey*. URL: <https://publicadministration.un.org/egovkb/en-us/Data/City/dataYear/2022>

Ukraine E-Government (2020). *UN E-Government Survey*.
URL: <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine/dataYear/2020>

Ukraine E-Government (2022). *UN E-Government Survey*.
URL: <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine/dataYear/2022>

Харинович Марта-Марія Сергіївна
*Київський національний університет імені Тараса Шевченка,
м. Київ, Україна*

ПРОТИДІЯ ЗАГРОЗАМ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ В ІНФОРМАЦІЙНОМУ ПРОСТОРИ: ДОСВІД УКРАЇНИ

З 2014 року Україна стала об'єктом зовнішньої експансії та руйнівного вторгнення з боку Російської Федерації, тому загрози інформаційній безпеці постійно були присутні в інформаційному та кіберпросторі. Після 24 лютого 2022 інформаційний простір взагалі перетворився на ще одне поле бою, адже росіяни почали масові кібератаки, щоб шпигувати, сіяти паніку та виводити з ладу українські інфраструктурні об'єкти.

За роки Україна встигла напрацювати алгоритми та законодавчу базу, щоб протидіяти таким загрозам національній безпеці. В даній роботі проаналізовано дії України для захисту національної безпеки в інформаційному просторі.

Перші спроби систематизувати і впорядкувати законодавство були хаотичними, проте заклали фундамент для подальших дій. Ще у 2014 році було прийнято закон "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України". Він зокрема передбачав розробку Закону України про кібернетичну безпеку України.

Закон "Про основні засади забезпечення кібербезпеки України" врешті було розроблено і затверджено. Він набув чинності у 2018 році, через 4 роки після початку обговорень. Це був перший профільний закон у сфері кібербезпеки, який нарешті врегулював термінологію галузі.

У 2016 році затвердили Стратегію кібербезпеки України на 2016-2020 роки. Цей документ був важливим з точки зору накопичення досвіду та створення правового підґрунтя для розбудови національної системи кібербезпеки, проте зміст був доволі абстрактним.

Більш конкретною була її наступниця, нині діюча Стратегія кібербезпеки України на 2021-2025 роки. Її метою визначено створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства, держави. Документ ґрунтується на засадах стримування, кіберстійкості та взаємодії (Ткачук, 2021).

Щодо розподілу обов'язків у сфері захисту інформаційного простору між державними інституціями, то для цього з 2017 року діє Доктрина інформаційної безпеки України.

Також варто згадати Концепцію розвитку сектору безпеки і оборони України 2016 року, в якій уточнено, що протидія інформаційним загрозам покладається зокрема на розвідувальні органи України – однією з основних їхніх функцій є виявлення та визначення ступеня зовнішніх загроз національній безпеці України, у тому числі у кіберпросторі.

Останнім ключовим документом у сфері інформаційної та кібербезпеки є Стратегія інформаційної безпеки України, яка зокрема офіційно визначає, що інформаційна безпека – складова частина національної безпеки України.

Після початку повномасштабної війни також оновили та покращили і наявне законодавство у сфері кібербезпеки. Основні зміни внесли у Кримінальний кодекс України та Кримінальний процесуальний кодекс України (Мальцева, Черниш, Штонда, 2022).

Крім законодавчої бази Україна покращувала і практичний захист. З 2018 року функціонує окремий Ситуаційний центр забезпечення кібербезпеки при СБУ. Там працює система моніторингу подій в реальному часі, що дає змогу аналізувати стан інформаційної безпеки і швидко помічати та реагувати на загрози.

Також варто відзначити діяльність Державної служби спеціального зв'язку та захисту інформації України. Держспецзв'язку звітує про роботу мобільного зв'язку, інтернету та цифрового телебачення в Україні, управляє мережами телекомунікацій, а після повномасштабного вторгнення взяла на себе координацію роботи з їх відновлення після ворожих атак.

Окремо варто звернути увагу на CERT-UA – урядову команду реагування на комп'ютерні надзвичайні події України, яка функціонує в складі Держспецзв'язку. CERT-UA аналізує

кіберзагрози, зокрема, віруси та DDOS-атаки, та надає практичну допомогу з питань запобігання, виявлення та усунення наслідків кіберінцидентів.

Після 24 лютого 2022 року до кіберзахисту почали залучати більше людей. Так, було створено спільноти волонтерів, які допомагають захищати інформаційний простір та боротися з інформаційними загрозами. Міністр цифрової трансформації України Михайло Федоров оголосив про створення IT-армії, куди долучилась низка спеціалістів з цифрової сфери. Метою спільноти стала боротьба на кіберфронті, при чому не лише захист, а й атаки – з моменту створення учасники регулярно виводили з ладу вебресурси Росії та Білорусі. Паралельно існують об'єднання волонтерів, які організують і проводять ДдоС атаки на ворожі ресурси (Гусак, Лаштовічка, Плеснік, 2022).

Бачимо, що для протидії загрозам національній безпеці в інформаційному просторі Україна діє різноманітно. Вона оновила, а подекуди і створила законодавчу базу у сфері інформаційної та кібербезпеки та розподілила обов'язки між урядовими структурами.

Деякі установи, як Ситуаційний центр забезпечення кібербезпеки при СБУ, були створені з нуля. Інші, як-от Держспец'язку та CERT-UA, були оптимізовані під нові виклики. Окремі угруповання, що підтримують інформаційну та кібербезпеку, були створені із волонтерів та майже чи повністю не пов'язані із державним сектором.

Література

Ткачук, Н. А. (2021). Щодо підготовки нової редакції стратегії кібербезпеки України. *Актуальні проблеми управління інформаційною безпекою держави*, 130–132.

Husák, M., Laštovička, M., Plesník, T. (2022). Handling Internet Activism during the Russian Invasion of Ukraine: A Campus Network Perspective. *Digital Threats: Research and Practice*. <https://doi.org/10.1145/3534566>

Maltseva, I., Chernish, Y., Shtonda, R. (2022). Analysis of some cyber threats in war. *Cybersecurity: Education, Science, Technique*, 16(4), 37–44. URL: <https://doi.org/10.28925/2663-4023.2022.16.3744>

Снитко Валерія Володимирівна

*Дніпропетровський державний університету внутрішніх справ,
м. Дніпро, Україна*

КІБЕРЗАХИСТ ТА НАЦІОНАЛЬНА БЕЗПЕКА: УКРАЇНСЬКИЙ ДОСВІД

Протягом двох останніх десятиліть стрімко розвивалися цифрові технології. Це викликало великий ажіотаж з приводу можливостей, які відкриває нова епоха цифрових гаджетів. Перехід від аналогових технологій до цифрових, тобто ера цифрової революції, передумовами якої є широке розповсюдження інформаційно-комунікаційних технологій, вже настала і дуже активно прогресує (Десятко, 2020, С. 12). У сучасному світі, де технології грають ключову роль у всіх сферах життя, кіберзахист та національна безпека стають важливими складовими для кожної держави. Україна не виняток, і досвід країни в галузі кіберзахисту має велике значення для розуміння викликів і можливостей у цій сфері.

Забезпечення кібербезпеки у 21 столітті є нагально важливим напрямком національної безпеки України та потребує надзвичайного зосередження зусиль по її забезпеченню усіх органів державної влади, які складають основу національної системи кібер-безпеки (Ємельянов, Бондар, С. 12).

З початку 2014 року Україна стала ареною для інтенсивних кібератак, спрямованих як проти урядових інституцій, так і проти громадянського суспільства. Ці атаки включали в себе спроби дефейсу веб-сайтів, розповсюдження шкідливих програм та втручання в роботу критично важливої інфраструктури. Для України ця ситуація стала справжнім викликом для національної безпеки.

На думку окремих авторів, система кіберзахисту, створена відповідно до вище- зазначених вимог, не забезпечує повною мірою кібербезпеки об'єкта інформатизації і, в першу чергу, органів державної влади та оборони. Забезпечення кібербезпеки

цих органів має здійснюватися єдиною інтелектуальною системою кібербезпеки, що є частиною системи інформаційної безпеки (Бакалинський, 2019, С. 102).

Один з ключових аспектів українського досвіду в цій галузі – постійне вдосконалення законодавства та регулювання в сфері кібербезпеки. Уряд України активно працює над створенням ефективних нормативних актів, які б дозволяли протидіяти кіберзагрозам та карати злочини в цій сфері. Це включає в себе не лише покращення законодавства, але і розробку стратегій кіберзахисту, створення інцидент-відгукових центрів та інфраструктури для аналізу кіберзагроз.

До того ж, співпраця з міжнародними партнерами та організаціями з кібербезпеки стає невід’ємною частиною стратегії України в галузі кіберзахисту. Уряд співпрацює з партнерами з Європи, США та інших країн для обміну досвідом та інформацією, а також для проведення спільних навчальних та тренувальних заходів. Це допомагає підвищити рівень готовності до кіберзагроз та ефективно реагувати на них.

Висновок полягає в тому, що український досвід в галузі кіберзахисту та національної безпеки є важливим в контексті сучасних кіберзагроз. Постійне вдосконалення правового поля та співпраця з міжнародними партнерами допомагають забезпечити ефективний захист кіберпростору та важливих інформаційних ресурсів для забезпечення стабільності та безпеки країни в умовах сучасного світу. Кіберзахист стає важливою складовою національної безпеки, і Україна вивчає цей аспект свого досвіду для забезпечення стійкості та захисту свого національного інформаційного простору.

Література

Десятко, А. М. (відп. ред.) (2020). *Кібергігієна. Кібербезпека. Безпека держави*: матеріали наукових семінарів. Київ: Київ. нац. торг.-екон. ун-т. URL: <https://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf>

Ємельянов, В. М., Бондар, Г. Л. *Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України*. Миколаїв. URL: https://www.google.com/url?sa=t&rcct=j&q=&esrc=s&source=web&cd=&ved=2ahUKewj_w6Sh2P2BAxXiQuUKHdeTCuEQFnoECAkQA

Q&url=https://pard.mk.ua/index.php/journal/article/download/141/106/&usg=AOvVaw3vjbyyPTJs2gaghwTuaGq7&opi=89978449

Бакалинський, О. (2019). Правове забезпечення кібербезпеки в Україні. *Адміністративне право і процес*. URL: <http://pgr-journal.kiev.ua/archive/2019/9/18.pdf>

Літинська Валентина Анатоліївна
кандидат економічних наук, доцент,
Хмельницький національний університет,
м. Хмельницький, Україна
ORCID: 0000-0001-9272-4118

АКТУАЛЬНІСТЬ КІБЕРБЕЗПЕКИ У МАРКЕТИНГОВІЙ АНАЛІТИЦІ

З початку війни Україна стала цілпо чисельних кібератак, які охопили державні установи, приватні організації та пересічних громадян. Підприємства, які є частиною критичної інфраструктури, зокрема енергетичні, телекомунікаційні, медіа та фінансові компанії, також мають бути у режимі підвищеної готовності, оскільки саме ці галузі часто вважаються пріоритетними цілями у період війни. Бізнес має бути готові протидіяти цим викликам – компанії повинні оцінити свою готовність до кіберінцидентів і свою здатність відновити діяльність.

Більшість хакерів і кіберзлочинців – безпринципні люди. Вони постійно змінюють тактику, щоб скористатися вразливими місцями в інтернеті. Саме тому, щоб протистояти цьому, установлюйте лише надійне програмне забезпечення з ефективними функціями безпеки. Постачальник програмного забезпечення повинен регулярно надсилати оновлення, щоб захистити своїх клієнтів від загроз (Гнатюк, 2016, С. 58).

У сучасному цифровому світі використання аналітики великих даних для вдосконалення стратегій цифрового маркетингу стає все більш популярною тактикою. Використовуючи статистику на основі даних, компанії можуть створювати персоналізований досвід для своїх клієнтів і отримати конкурентну перевагу на ринку.

Аналітика великих даних пропонує низку переваг для стратегій цифрового маркетингу, включаючи можливість краще орієнтуватися на клієнтів, визначати потенційних потенційних

клієнтів і розуміти поведінку клієнтів. Завдяки великим даним компанії можуть отримати повнішу інформацію про вподобання клієнтів і розробити більш ефективні стратегії для зв'язку зі своєю цільовою аудиторією. Водночас дані компанії залишають незахищеними від кібератак, що потребує вирішення цієї нагальної проблеми (Богущ, 2020, С. 216).

Компанії також можуть використовувати великі дані, щоб отримати цінну інформацію про інтереси, поведінку та вподобання своїх цільових клієнтів. Ці дані можна використовувати для створення цільових кампаній, адаптованих до потреб та інтересів кожного клієнта. Підприємства також можуть використовувати дані для виявлення потенційних потенційних клієнтів і оптимізації взаємодії з клієнтами, допомагаючи підвищити ефективність своїх цифрових маркетингових зусиль.

Аналітика великих даних також пропонує компаніям можливість розробляти більш складні стратегії сегментації клієнтів. Використовуючи статистику на основі даних, компанії можуть створювати більш індивідуальний досвід для своїх клієнтів, допомагаючи покращити взаємодію та задоволеність клієнтів.

Нарешті, компанії можуть використовувати аналітику великих даних для вимірювання ефективності своїх цифрових маркетингових кампаній. Відстежуючи залучення клієнтів, коефіцієнти конверсії та інші ключові показники, компанії можуть отримати краще розуміння того, які стратегії працюють, а які потрібно вдосконалити.

Загалом використання аналітики великих даних може стати потужним інструментом для вдосконалення стратегій цифрового маркетингу. Використовуючи статистику на основі даних, компанії можуть створювати більш персоналізований досвід клієнтів, краще націлювати своїх клієнтів і вимірювати ефективність своїх кампаній. У сучасному цифровому світі використання аналітики великих даних стає все більш популярною тактикою для компаній, які прагнуть отримати конкурентну перевагу на ринку.

Враховуючи все вище зазначене, можна стверджувати, що є сенс переглянути ключові набори контролів кібербезпеки, які

можуть допомогти знизити ймовірність успішності атак, зокрема тих, які допомагають захиститися від загроз від держави-агресора або організованих угруповань, які активізували свою діяльність під час війни. Для цього необхідно надати пріоритет задачам з встановлення виправлень усіх критичних вразливостей у системах – особливо для тих, які зараз активно використовуються зловмисниками. Крім того, доцільно переглянути контролю доступу до ключових систем, зосереджуючи увагу на багатофакторній аутентифікації, видаленні облікових записів, що не використовуються або термін дії яких закінчився, а також необхідності ізоляції систем, що мають високий ризик (Cornish, 2009, С. 28).

Окрім превентивного захисту ефективний моніторинг безпеки є також важливим з огляду на своєчасне виявлення та реагування на вторгнення. Середній час між початковою компрометацією і запуском деструктивного шкідливого програмного забезпечення тепер вимірюється днями, а не тижнями або місяцями, як було раніше. Також необхідно зрозуміти поточні можливості з моніторингу кібербезпеки у мережевій інфраструктурі організації, щоб переконатися в існуванні можливостей з виявлення та запобігання інцидентів кібербезпеки та охопленні ними бізнес послуг, систем та даних (Mat, 2019, С. 118).

Якщо в компанії є команда з полювання на загрози, доручити їм пошук індикаторів компрометації, заснованих на тактиках, техніках та процедурах, пов'язаних з групами, що асоціюються з державою-агресором або її партнерами, або організованими злочинними групами, які залучені до війни на кіберфронті.

Отже, підприємствам слід планувати можливу зупинку своєї діяльності в регіонах бойових дій та у деяких випадках організувати тимчасову кадрову підтримку для забезпечення функціонування своїх критичних сервісів, доки їхні співробітники не зможуть повернутися до офісу або в країну. Окрім підтримки співробітників та їхніх сімей, організації також мають знати про ризики організованих злочинних груп. Ці групи намагаються скористатися кризою на свою користь, створюючи підроблені веб-сайти, які нібито пропонують допомогу чи

корисну інформацію, або приймають пожертвування. Є велика ймовірність фішингових кампаній, орієнтованих на тематику війни в Україні і спрямованих на високопоставлених осіб, які відкрито висловлюють свою позицію стосовно війни.

Література

Гнатюк, С. (2016). Рекомендації щодо розробки стратегії забезпечення кібербезпеки України. *Захист інформації*, 18, 1, 57-65. URL: <http://jrn1.nau.edu.ua/index.php/ZI/article/viewFile/10113/13301>

Cornish, P. (2009). Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks. *Directorate-General for External Policies of the Union, Policy Department*. 34. URL: https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf

Богуш, В. М. (2020). *Основи кіберпростору, кібербезпеки та кіберзахисту*. Видавництво Ліра-К. URL: <https://lira-k.com.ua/preview/12696.pdf>

Mat, B., Pero, S., Wahid, R., & Sule, B. (2019). Cybersecurity and Digital Economy in Malaysia: Trusted Law for Customer and Enterprise Protection. *International Journal of Innovative Technology and Exploring Engineering*. URL: <http://www.ijitee.org/wpcontent/uploads/papers/v8i8s3/H10610688S319.pdf>

ЦИФРОВА ДИПЛОМАТІЯ В УМОВАХ ТРАНСФОРМАЦІЇ СИСТЕМИ МІЖНАРОДНОЇ БЕЗПЕКИ

Хорішко Лілія Сергіївна

доктор політичних наук, професор,

Запорізький національний університет, м. Запоріжжя, Україна,

ORCID: 0000-0002-0618-976X

ОСОБЛИВОСТІ СПІВПРАЦІ УКРАЇНИ ТА НАТО У СФЕРІ КІБЕРБЕЗПЕКИ

Гібридні виклики сьогодення актуалізують потребу активізації політичного діалогу та синхронізації зусиль суб'єктів політики у формуванні дієвої системи кіберзахисту. Повномасштабне вторгнення російських військ ще більшою мірою актуалізувало питання кібербезпеки для України. Йдеться не тільки про здатність захищати об'єкти критичної інфраструктури та державні інформаційні ресурси, але й розширення можливостей держави протидіяти ворожим кібератакам. У цьому контексті Україна інтенсифікує взаємодію з НАТО та державами-членами з метою синхронізації зусиль у протидії кіберзагрозам та імплементації досвіду взаємодії у сфері кібербезпеки.

На минулорічному саміті у Мадриді була прийнята нова Стратегічна концепція НАТО, в якій окреслено гібридні загрози колективній безпеці євроатлантичного регіону, ключовими з яких визнано спроби авторитарних політичних режимів нівелювати значущість європейських цінностей, демократичних практик, підірвати стійкість політичних інститутів (НАТО, 2022). Одним із ключових інструментів гібридного впливу є здійснення масштабних кібератак, оскільки вони дестабілізують функціонування критичної інфраструктури, сприяють витоку

секретної інформації та персональних даних, створюють перешкоди у діяльності органів державної влади та військових структур. У цьому контексті політичний діалог і співпраця у сфері кібербезпеки розглядаються ключовими інструментами формування стійкості Альянсу до сучасних гібридних викликів.

Під егідою Альянсу функціонує Координаційний центр передового досвіду у сфері кіберзахисту, мета якого – дослідження актуальних проблем кіберзахисту, організація навчальних тренінгів у таких сферах як технології, стратегії, операції та законодавство. Його було створено за ініціативи Естонії та у взаємодії з Німеччиною, Італією, Латвією, Литвою, Словаччиною, Іспанією. У 2023 році Україна стала членом цієї організації, що сприятиме поглибленню співпраці та вивченню закордонного досвіду протидії кіберзагрозам. Водночас міністр оборони Естонії Х. Певкур на офіційній церемонії вступу зазначив, що Координаційний центр сприятиме перемозі України на полі кібербою за допомогою синхронізації зусиль держав-партнерів і спільного використання новітніх технологій у протидії кіберзагрозам (CCDCOE, 2023).

Україна приймала участь у міждисциплінарній конференції СуСоп 2023 «Зустріч з реальністю», організованій Координаційним Центром передового досвіду у сфері кіберзахисту. Представник України І. Вітюк зазначив, що поглиблення партнерського діалогу та співпраці у сфері кібербезпеки є запорукою стійкості нашої держави в умовах повномасштабного вторгнення (Vitiuk, 2023). Учасники заходу обговорили низку актуальних питань щодо кіберстійкості сучасних суб'єктів політики, врахування українського досвіду протидії кібератакам і наголосили на поглибленні двосторонньої співпраці.

Щорічно українські фахівці з кіберзахисту приймають участь у змаганнях NATO TIDE Hackathon. Дана ініціатива НАТО спрямована на обмін досвідом щодо розробки нових програмних рішень у сфері кіберзахисту, розширення можливостей використання новітніх інформаційних технологій у протидії дезінформації та кібератакам в умовах сучасної політичної дійсності (NATO, 2023).

Посиленню стійкості України у кіберпросторі сприяє співробітництво з державами-членами НАТО. США та Данія спільними зусиллями реалізують Проєкт USAID «Кібербезпека критично важливої інфраструктури України», спрямований на оптимізацію законодавчої та інституційної бази, навчання українських спеціалістів, посилення співпраці державного та приватного секторів у сфері кіберзахисту (U.S. Embassy in Ukraine, 2023). До реалізації цієї ініціативи приєдналася Нова Зеландія як один із ключових партнерів НАТО. Посилення кіберстійкості України розглядається цими державами як ключова складова комплексної допомоги у протидії державі-агресору.

Велика Британія фінансує українську кіберпрограму, мета якої – захист критичної інфраструктури та процесу надання адміністративних послуг. Йдеться про залучення світового передового досвіду приватних і державних стейкхолдерів у сфері кіберзахисту. На думку Прем'єр-міністра Р. Сунака, російські кібератаки на критичну інфраструктуру та сферу надання послуг, спрямовані на зниження морального духу українських громадян. Посилення кібербезпеки України сприятиме підвищенню рівня стійкості держави та нарощуванню потенціалу у боротьбі за відновлення територіальної цілісності та суверенітету (Gov. UK, 2023).

Отже, Україна завдяки активізації співпраці з НАТО у сфері кібербезпеки розширює можливості протидії державі-агресору. По-перше, залученість до діяльності спеціальних інституцій НАТО сприяє обміну досвідом та новітніми технологіями у сфері кіберзахисту, що посилює стійкість держави перед гібридними викликами сьогодення. По-друге, Україна активно приймає участь у тематичних заходах і посилює двосторонню співпрацю з державами-членами НАТО у сфері кібербезпеки, залучаючи їх ресурсний потенціал до протидії державі-агресору.

Література

The NATO CCDCOE welcomes new members Iceland, Ireland, Japan, and Ukraine (2023). CCDCOE. URL: <https://ccdcoe.org/news/2023/the-nato-ccdcoe-welcomes-new-members-iceland-ireland-japan-and-ukraine/>

UK to give major boost to cyber defences as Ukraine mounts

counteroffensive (2023). *Gov. UK*. URL: <https://www.gov.uk/government/news/uk-to-give-ukraine-major-boost-to-mount-counteroffensive>

NATO Strategic Concept (2022). URL: <https://www.nato.int/strategic-concept/index.html>

TIDE Hackathon Concludes in Poland (2023). *NATO*. URL: <https://www.act.nato.int/article/tide-hackathon-concludes-in-poland/>

Vitiuk, I. (2023). *Ukraine in Cyberspace: One Year After*. URL: https://www.youtube.com/watch?v=302u5HWn_bM&list=PLV8RTnZwQxclFT_77aeGoM1LkopXWE518&index=30

The United States and Denmark Partner to Strengthen Ukraine's Cybersecurity (2023). *U.S. Embassy in Ukraine*. URL: <https://ua.usembassy.gov/the-united-states-and-denmark-partner-to-strengthen-ukraines-cybersecurity/>

Калашлінська Марина Вікторівна
кандидат політичних наук,
Донецький Національний Університет ім. Василя Стуса,
м. Вінниця, Україна
ORCID: 0000-0001-5825-3631

РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ У ПІДТРИМЦІ МЕДІАЦІЇ ТА ПЕРЕГОВОРІВ В СУЧАСНИХ ПОЛІТИЧНИХ ПРОЦЕСАХ

Зростання актуальності дослідження ролі цифрових технологій у сфері медіації та переговорів в сучасних політичних процесах в останні роки стає дедалі очевиднішим. Це зумовлено, зокрема, стрімким розвитком інформаційного суспільства і, відповідно, глобальними змінами в комунікаційних каналах не лише серед громадян та бізнес-середовища, а й на міжнародній арені та в політичних відносинах. Цифровізація відкриває нові можливості для ефективного вирішення конфліктів, обміну інформацією та міжнародної співпраці, розширюючи перелік інструментів до розв'язання політичних конфліктів і пошуку шляхів досягнення глобальної безпеки. Цифрові технології надають можливість ефективніше обмінюватися інформацією на відстані та створюють основу для низки інноваційних рішень у веденні переговорів, зокрема, завдяки таким інструментам, як:

1. Сучасні комунікаційні платформи і сервіси, що побудовані на новітніх інформаційних технологіях, зокрема, такі як спеціалізовані платформи для відеоконференц-зв'язку (наприклад, Zoom, Teams, Webex), хмарні рішення та інші веб-сервіси, революціонізували процес переговорів та медіації. Вони дозволяють учасникам взаємодіяти ефективно, безпечно та в інтерактивно, незалежно від їх географічного розташування, що відкриває нові можливості для міжнародної співпраці та діалогу;

2. Мобільні додатки, ключовою відмінністю яких від стандартних веб-версій є підвищена інтуїтивність інтерфейсу, оптимізована для мобільних пристроїв; швидкість сповіщень,

максимально наближена до комунікації в реальному часі; геолокація та оптимізація споживання енергії тощо. Це робить мобільні додатки незамінними для оперативної взаємодії учасників переговорів, незалежно від їх місця розташування.

3. Сучасні цифрові аналітичні інструменти та засоби аналізу даних, об'єднують потужні алгоритми та моделі для обробки великих масивів даних, а також виявлення в них прихованих закономірностей та стратегічних тенденцій розвитку. Це дозволяє переговорним групам та посередникам оперативно визначати ключові зони ризику в переговорах, а також здійснювати планування в умовах мінливих обставин, максимально враховуючі об'єктивні дані та неочевидні тенденції. Це робить перемовини більш прагматичними, дозволяє знижувати вплив емоційної складової процесу перемовин, що може сприяти розробці виважених аналітичних прогнозів та прийняттю обґрунтованих рішень в ході переговорів.

4. Безпека та шифрування інформації у контексті переговорного процесу і медіації, без перебільшення, відіграють критичну роль. Використання передових методів шифрування, сучасних кіберзахисних технологій, а також технологій на основі блокчейну спрямовані на підвищення захисту конфіденційності, надійності та непорушності цілісності даних. Ці інструменти максимізують рівень довіри між сторонами для того, щоб дозволити їм вести переговори без страху порушення приватності переданої інформації, дозволяючи їм зосереджуватися на основних аспектах переговорів без страху порушення приватності.

Таким чином, в епоху цифрової трансформації, роль цифрових технологій у медіації та політичних переговорах невинно зростає. Сучасні цифрові інструменти не лише оптимізують комунікаційні процеси, а й надають можливість для детального аналізу інформації, гарантуючи швидкість, ефективність та безпеку даних. Хоча існують виклики у інтеграції традиційних методів медіації в цифровий контекст, сучасні практичні приклади підкреслюють велику ефективність та актуальність цифрових рішень в політиці. Отже, цифрові технології не просто розширюють можливості медіації та

переговорів, але ї сприяють ефективній взаємодії сторін, незалежно від географічних або епідеміологічних обмежень, підсилюючи співпрацю та досягнення консенсусу в глобальному контексті.

Література

Ebner, N. (2021). Integrative negotiation: Paying the price of popularity. *Discussions in Dispute Resolution: The Foundational Articles*, 84-88.

Koopmans, S. (2018). *Negotiating Peace: A Guide to the Practice, Politics, and Law of International Mediation*. OUP Oxford.

Latifah, E., Bajrektarevic, A., Imanullah, M. (2019). Digital Justice in Online Dispute Resolution: The Shifting from Traditional to the New Generation of Dispute Resolution. *Brawijaya Law Journal*. 6. 27-37. doi: <https://doi.org/10.21776/ub.blj.2019.006.01.02>.

Сокоринський Володимир Олегович
*Одеський національний університет ім. І. І. Мечникова,
м. Одеса, Україна*

ЦИФРОВИЙ ТОТАЛІТАРИЗМ ЯК ЗАГРОЗА СУЧАСНІЙ ЦИФРОВІЙ ДИПЛОМАТІЇ

Сьогоднішня цифрова життя та безпосередньо цифрової дипломатії дедалі стає більш технологічним та складним. Умови та супровід взаємовідносин між країнами та світом формується із використанням досягнень комп'ютеризації суспільства та використання інформаційних технологій. Використання таких технологій, як соціальних мереж, гаджетів дає можливість новим чином підходити державам до вирішення власних потреб та завдань. Маючи на меті вдосконалення таких процесів, перед країнами та світом стає питання захисту цих каналів зв'язку та упередження процесів, які може викликати тенденції цифрового тоталітаризму. З огляду на такі тенденції, автор задається питаннями актуалізації розгляду цифрового тоталітаризму, як загрозу сучасної цифрової дипломатії.

За для розуміння сутності терміну цифрової дипломатії було прийнято вважати дефініцію, яку використовують М. Г. Окладна, В. Ю. Стеценко у власній статті, а саме «...цифрова дипломатія в широкому розумінні – це використання можливостей мережі Інтернет і інформаційно-комунікаційних технологій для вирішення дипломатичних завдань» (Окладна & Стеценко, 2020, С.14).

Отже, “цифрова дипломатія” постає невід’ємною частиною сьогоденної системи міжнародних відносин, яка сприяє підтриманню відносин в режимі реального часу. Так наприклад, розуміючи сучасні процеси неконтрольованої цифровізації та технологізації взаємовідносин у суспільстві та країнах, держави дедалі більше стикаються з питанням регламентації та встановленням рамок цих контактів через присутність в мережі Інтернет різних політичних акторів та представників

громадського суспільства. Пригадуючи «залізний закон бюрократизації» Роберта Міхельса, уряди постійно намагаються перевести такі контакти у бік закритих та прихованих використовуючи додаткові можливості технологічного прогресу, такі дії, за сутністю вважаються загрозами цифрового тоталітаризму, як явище.

Першою проблемою з якою зіштовхуться «цифова дипломатія» – питання відкритості та доступності. Завдяки розвитку цифрових технологій та мережі-Інтернет, представники «громадянського суспільства», соціально-політично активні громадяни та ЗМІ тепер можуть постійно чатувати політиків та дипломатів заявами та повідомленнями, активно розповсюджуючи, як власні відгуки так і безпосередні заяви. Так, наприклад, загальновідомий сайт WikiLeaks ще в 2010 році пригломшив світову аудиторію опублікувавши 250 тисяч дипломатичних телеграм, які мали відверті оцінки американських дипломатів про світових лідерів, їхніх урядів та держав. Доктор Ілон Манор, вчений у галузі цифрової дипломатії та викладач Тель-Авівського університету та Університету Бен-Гуріона у Негеві у статті «WikiLeaks Revisited» стверджує «WikiLeaks, можливо, викликав справжній страх перед цифровими інструментами серед міністерств закордонних справ. Самі характеристики соціальних мереж, їх відкритість і схильність до обміну інформацією, мабуть, здавалися чужими дипломатам, добре навченим конфіденційності» (Manor, 2015).

Виходячи з таких тенденцій наступною проблемою для цифрової дипломатії постає проблема «цифрової дати». Так наприклад, Аннехріс Кебрюгге, у власній статті стверджує, що «Інтернет ніколи не забуває: повністю видалити онлайн-повідомлення неможливо, і легко припуститися помилок. Один твіт може мати отруйний ефект кілька місяців» (Koerbrugge, 2018). Таким чином, сьогоденна так звана Twitter-Diplomacy є дуже не однозначною та потребує повноцінного розуміння того, що публікується офіційними представниками чи органами держав та урядів. Окрім існування таких способів впливу на цифрову дипломатію, існують також і так звані «ботоферми»,

рухи «клітивістів» та «слактивістів», які не виходячи з власних гаджетів можуть впливати на порядок денний міжнародних організацій та держав. Проте такі приклади, швидко змінюються за рахунок появи та розвитку нейромереживих програм на кшталт ChatGpt, який на сьогодні викликає міжнародні дискусії в сфері кібербезпеки, дипломатії, цифрової демократії тощо. На думку І. Манора «Генеративний ІІ, здатний формулювати заяви для преси, писати твіти та повідомлення, відповідати на консульські питання та намічати стратегії успішних переговорів, може зробити багатьох дипломатів непотрібними. Інші прогнози зводять дипломатів до редакторів, яким доручено «налаштовувати» та «адаптувати» промови ChatGPT або перевіряти мову, яка використовується в резолюціях ООН, створених ChatGPT. Інші вважають, що ChatGPT просто зруйнує дипломатію, створивши нові проблеми та можливості» (Manor, 2023).

Через створення та існування такого додатку постає питання «підірваності» стану цифрової дипломатії. Довіра до цифрової дипломатії може бути під загрозою, особливо коли сьогодні існує загроза розповсюдження та поширення цифрових тоталітарних тенденцій. Уряди та держави можуть з легкістю вдаватися до обманних дій, яке ускладнить дипломатам встановлення/продовження відносин через онлайн-платформу. Дірк Хелбінг – німецький професор обчислювальної соціології факультету гуманітарних, соціальних і політичних наук, член факультету комп'ютерних наук ETH Zurich – виділяє наступні риси сучасних цифрових тоталітарних суспільств, а саме: 1) масове стеження; 2) неетичні експерименти з людьми в рамках існування соціальної інженерії; 4) примусове підпорядкування людей; 5) пропаганда та цензура; 6) існування «доброзичливої» диктатури; 7) поліцейська діяльність, тобто наявність «поліцейської держави»; 8) виборче застосування забезпечення прав людини) (Helbing, 2017).

Цифровий тоталітаризм постає системою тотального контролю за всіма сферами життя суспільства, використовуючи електронні технічні засоби, які в свою чергу дозволяють лімітувати чи корегувати діяльність людини в Інтернеті.

Алармізм в цьому питанні постає актуальним через можливість маніпулювання даними та спрощення систем спостереження. Таким чином, політичні режими можуть використовувати цифрові платформи для маніпулювання даними, переслідування за громадянами та контролю інформаційних потоків, підтримувати довіру, необхідне для ефективної дипломатії.

Цифрові тоталітарні держави широко застосовують цензуру, обмежуючи вільний потік інформації. Саме такі маніпуляції можуть призвести до змін норм сьогочасного глобалізованого світу та ускладнити міжнародне співробітництво з питань цифрової безпеки. Створення міжнародних коаліцій проти цифрового тоталітаризму буде діючим тільки тоді, коли держави почнуть жваво обговорення щодо скоординованих глобальних зусиль, надійних мір кібербезпеки та дотримання демократичних цінностей, гарантуючи, що цифрова дипломатія може працювати в безпечному та захищеному середовищі довіри.

Література

Окладна, М. Г., Стеценко, В. Ю. (2020). *Роль цифрової дипломатії в сучасній зовнішній політиці держави*. URL: https://apir.org.ua/wp-content/uploads/2020/12/Okladna_Stetsenko15.pdf

Helbing, D. (2017). Digital fascism rising? URL: <https://www.theglobalist.com/fascism-big-data-artificial-intelligence-surveillance-democracy/>

Koebrugge, A. (2018). Ctrl-Alt-Delete: is Digital Diplomacy Worth the Risk? URL: <https://www.leidensecurityandglobalaffairs.nl/articles/ctrl-alt-delete-is-digital-diplomacy-worth-the-risk>

Manor, A. (2015). WikiLeaks Revisited. URL: <https://digdipblog.com/2015/11/09/wikileaks-revisited/>

Manor, A. (2023). Towards the Strategic Use of AI in Diplomacy. URL: <https://digdipblog.com/2023/08/15/towards-the-strategic-use-of-ai-in-diplomacy/>

Рогозіна Анастасія Володимирівна
*Донецький національний університет імені Василя Стуса,
м. Вінниця, Україна*

ЦИФРОВА ДИПЛОМАТІЯ: ІНФОРМАЦІЙНИЙ ФРОНТ УКРАЇНИ В УМОВАХ ВІЙНИ З РОСІЄЮ

Перебіг подій останніх років змінив життя України та всього цивілізованого світу. Оголошення про початок повномасштабного вторгнення Росії 24 лютого 2022 року стало викликом для української влади і пересічних українців та потребувало прийняття швидких нетипових рішень. Цифрова дипломатія була покликана стати одним з ключових інструментів для активізації процесу взаємодії між країнами світу для ефективної боротьби з агресором. Питання територіальної цілісності та збереження суверенітету України стало ключовим національним інтересом держави. Такий стан речей вимагає залучення нових підходів у зовнішній політиці України та фактичну її переорієнтацію. У даному контексті ресурсний потенціал цифрової дипломатії є доволі високим та повинен стати новим інструментом боротьби в гібридній війні Росії проти України.

Цифрову дипломатію авторка пропонує розглядати за концепцією Дж.Найя «м'якої сили» (Най, 2004, С.4) як здатність держави досягати стратегічних завдань, шляхом використання сучасних інформаційних технологій. Ефективне використання інструментів цифрової дипломатії може забезпечити широкий плацдарм для дій України в політичному та інформаційному полі, для затвердження свого зовнішнього іміджу та залучення підтримки від країн-партнерів. Інструменти цифрової дипломатії здатні показати світу, ким є Україна, якими є її цінності, куди направлені її координати розвитку та представити світу реальне обличчя ворога.

Цифрова дипломатія є однією з структурних частин іміджу держави. На думку авторки, імідж держави – це складне дворівневе явище, яке формується цілеспрямовано, з метою підвищення конкурентоспроможності на політичній арені, результатом реалізації якого є дотримання національних інтересів і зовнішньополітичних цілей. Поняття «імідж держави» пропонується розуміти як сукупність реальних і штучно створених характеристик системи державних інститутів, політичних, правових, економічних систем, інформація про які направляється в інформаційно-комунікаційний простір з метою впливу на суспільну свідомість усередині держави й за її межами (Семченко, 2013, С.47).

Російсько-українську війну можна вважати першою в історії «Війною у смартфоні», адже окрім дій, які мають воєнний характер, Росія також використовувала та продовжує використовувати зброю сучасного часу – хакерські атаки, поширення фейків та ін. Враховуючи факт того, що роль Інтернету та інтернет ресурсів в соціально-політичному житті світу починає зростати, то війни все частіше стають інтегрованими у віртуальний простір.

Здобуття Україною незалежності в 1991 році та відокремлення від радянського союзу, вимагало рішучих кроків влади для формування ефективної зовнішньої політики держави. Головним завданням було сформуванню уявлення про Україну, її традиції, історію та культуру в очах світової спільноти, адже досить часто Україну ототожнювали з Росією. Отже, формування та реалізація національного бренду повинно було гарантувати підтримку закордонних партнерів. Вперше, необхідність реалізації процесів публічної дипломатії в Україні на офіційному рівні була визнана в 2006 році. Проте, особливо гостро дане питання активізувалось у 2014 році, коли Росія анексувала Кримський Півострів та окупувала частину території на сході України. Станом на зараз, Україною впроваджується Стратегія публічної дипломатії МЗС, ухвалена Наказом МЗС від 24.03.2021 року. Вперше в єдиному документі систематизовано що, кому, коли і як Україна говорить про себе у світі: ключові меседжі, аудиторії, формати та канали комунікацій. Стратегія встановлює чіткі та вимірювані цілі та

завдання на 2021-2025 роки та визначає сім ключових напрямів публічної дипломатії: культурна, експертна, економічна, кулінарна, цифрова, науково-освітня, спортивна (Кулеба, С.9). У контексті даної Стратегії, напрямок цифрової дипломатії є одним з найбільш прогресивних та передбачає використання інструментарію цифрових технологій. Це дозволить сформувати стійкий канал комунікації з світовою спільнотою в режимі реального часу з метою реалізації своїх національних інтересів, зокрема формування позитивного сприйняття України дасть змогу висвітлювати наслідки агресії Росії, їх масштаби та інформувати про можливі ризики в майбутньому. А також ділитись успіхами України на фронті, у вигляді результатів контрнаступальних дій та деокупаційних планів по звільненню українських територій.

Підводячи підсумок, варто зазначити, що формування позитивного іміджу України під час війни з Росією стало викликом для всієї нації, для управлінців всіх рівнів й для цифрової дипломатії. Ефективне використання її інструментів повинно було гарантувати підтримку партнерів у боротьбі з агресором. Розроблена ще до початку війни Стратегія публічної дипломатії Міністерства Закордонних Справ України, стала покроковою інструкцією для просування зовнішнього іміджу держави, підлаштувавшись під умови воєнного часу. Стратегія була частково переорієнтована, однією з основних задач було висвітлення воєнних злочинів Росії на території України, з метою одержання ресурсів для ведення оборонних та наступальних операцій. Використання широкого спектру інструментів цифрової дипломатії дозволило додати нових аспектів зовнішньому іміджу України, сепарувавши його від російських наративів, та спрямувавши його в бік таких сенсів як незламність, непереможність, європейськість та перспективність.

Література

Nye, J. S. (2004). *Soft Power: The Means to Success in World Politics*. Public Affairs Books.

Семченко, О. (2013). Формування іміджу держави в контексті політичної модернізації України. *Український науковий журнал «Освіта регіону»*, 3, 47-51.

Кулеба, Д. Стратегія публічної дипломатії МЗС України 2021-2025. *Офіційний портал Міністерства закордонних справ України.*
URL: [public-diplomacy-strategy.pdf](#)

ФЕЙКИ ТА ДІПФЕЙКИ ЯК ІНСТРУМЕНТИ НЕГАТИВНОГО ВПЛИВУ НА НАЦІОНАЛЬНУ БЕЗПЕКУ

Вовк Світлана Олександрівна

доктор політичних наук, доцент,

*ДЗ «Луганський національний університет імені Тараса Шевченка»,
м. Полтава, Україна*

ORCID: 0000-0002-6171-4782

ТЕХНОЛОГІЧНІ АСПЕКТИ СТВОРЕННЯ ДІПФЕЙКІВ ТА ЇХ НАСЛІДКИ ДЛЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ¹

У світі, який характеризується цифровими технологіями та інформаційною вразливістю, феномен дїпфейків (deepfake) став серйозним викликом для національної безпеки. Дїпфейки – це відео, аудіо або текстовий контент, створений штучним шляхом з використанням технологій, які дають можливість створювати контент зі сфальсифікованим змістом, що має реалістичний вигляд (Sauer, 2022).

Для створення дїпфейку матеріалу використовуються два основних способи. Перший спосіб використовує два основних алгоритми: кодер і декодер. Кодер починає процес, шукаючи спільні риси на двох різних зображеннях, які потрібно об'єднати в одне. Наприклад, якщо ми хочемо створити відео, де актор відтворює наші рухи, кодер аналізує рухи з нашого відео і виявляє спільні риси або параметри, що визначають ці рухи. Потім другий алгоритм, декодер, використовує ці знайдені спільні риси та параметри для перенесення їх на новостворене зображення

¹ Публікація містить результати досліджень, проведених при грантовій підтримці Національного фонду досліджень України за проектом 2021.01/002

актора. Це означає, що декодер замінює обличчя актора на обличчя, яке відповідає нашому, і змушує актора відтворювати наші рухи, жести та міміку. Основними ключовими елементами в цьому процесі є вибрані дії або рухи, які копіюються на нове зображення, щоб створити переконливий діпфейк матеріал. Такий підхід дозволяє створювати вражаюче реалістичний контент, який може бути використаний в різних сферах, але також вносить ризики для національної безпеки та впливу на громадське довіру та інші аспекти суспільства.

Другий спосіб створення діпфейку базується на використанні генеративних змагальних мережі (GAN), де два алгоритми працюють у взаємодії. Перший з алгоритмів називається генератором. Він використовує загальну інформацію та створює образи, такі як образ людини. Генератор об'єднує в собі різні ознаки цього образу, наприклад, тіло, обличчя, очі та інші характерні деталі. Другий алгоритм, що використовується у GAN, називається дискримінатором. Його основна функція полягає в оцінці того, чи є створене зображення, надане генератором, правдивим чи ні. Дискримінатор пробує виявити будь-які недоліки чи артефакти на зображенні, які свідчили б про його фальсифікацію. GAN використовують цю концепцію конкуренції між генератором і дискримінатором для досягнення високого рівня реалізму у створеному діпфейк-контенті. Процес навчання GAN полягає в тому, що генератор намагається підвищити якість своїх створених зображень, водночас дискримінатор намагається виявити їхні недоліки. Ця боротьба за перевагу між двома алгоритмами приводить до покращення якості створеного діпфейку-контенту.

Діпфейки, які представляють собою штучно створений контент з фальсифікованим вмістом, можуть бути використані для досягнення цілей, які становлять загрозу суверенітету, стабільності та безпеці країни.

По-перше, діпфейки використовуються для дискредитації політичних діячів та посадових осіб, зокрема і перших осіб держави. Крім того, у російсько-українській війні агресор таким чином розповсюджував фальшиву інформацію для досягнення своїх військових і політичних цілей. Так, на початку повномасштабного

вторгнення росія розповсюдила дідфейк звернення В. Зеленського із закликом до українців скласти зброю (Центр протидії дезінформації при РНБО України, 2022). В червні 2022 р. від імені мера Києва В. Кличка засобами платформи Zoom невідомий розмовляв із мерами Мадриду й Берліну (Мельник, 2002).

По-друге, дідфейки використовуються для маніпулювання громадською думкою шляхом «...спотворення фактів, що полягає у неповному, односторонньому чи упередженому їх поданні у публічну площину зі свідомим приховуванням суттєвих деталей чи перекручуванням достовірної фактологічної основи повідомлення...» (Лисенко & Манелюк, 2022, С. 45). В даному випадку, дідфейки можуть використовуватися і з метою підриву довіри до певних ЗМІ, як наслідок, громадяни стають більш схильними до сумнівів у правдивості новин, виникає ситуація загального відчуття невпевненості .

По-третє, використання дідфейків може впливати на діловий клімат, викликаючи зміни в ринкових умовах або репутаційних втрати компаній та бізнесу. Так, фейкові фінансові новини або аналітичні матеріали, які можуть вплинути на ціни акцій, курси валют та інші показники на фінансових ринках, що, в свою чергу, може призвести до паніки на фінансових ринках, вплинути на обмін валюти та інвестиційний клімат.

Отже, наведені приклади демонструють, що з моменту виникнення технологій для створення дідфейків виникає необхідність в розвитку заходів для їхнього виявлення, відслідковування та протидії. Національна безпека має бути здатною виявляти та протистояти цим загрозам для забезпечення стабільності держави.

Література

Березенко, І. (2023). *Нова зброя дезінформації під назвою ДІПФЕЙК*. URL: <https://mil.in.ua/uk/blogs/nova-zbroya-dezinformatsiyi-pid-nazvoyu-deepfake-dipfejk/>.

Лисенко, Ю, Манелюк, Ю. (2022). Технології політичного маніпулювання та їх вплив на громадську думку в сучасних політичних процесах. *Політикус*, 5, 42-47.

Мельник, В. (2022). Маємо не два Кличка, а ... три! Чи навіть більше? Дідфейк: що це таке, як розпізнати на кого уже «підміняли».

URL: <https://vikna.tv/styl-zhyttya/dipfejk-shho-cze-take-yak-praczyuyeta-rozpiznaty-obman/>

Sauer, N. (2022). Deepfakes are being used for good – here’s how. *The conversation*. URL: <https://theconversation.com/deepfakes-are-being-used-for-good-heres-how-193170>.

Остерігайтеся підроблених відео! Що таке дїпфейки та чого їх використовують (2022). *ICTV. Ранок*. URL: <https://ranok.ictv.ua/ua/2022/06/25/osterijgajtesya-pidroblenih-video-shho-take-dipfejki-ta-dlya-chogo-yih-vikoristovuyut/>.

Федорова Алла Іванівна
кандидат історичних наук, доцент,
Національний університет «Одеська політехніка»,
м. Одеса, Україна
ORCID: 0000-0002-0306-7804

ФЕЙКИ РОСІЙСЬКОЇ ПРОПАГАНДИ ЩОДО ІСТОРІЇ УКРАЇНИ ТА СПОСОБИ ПРОТИСТОЯННЯ ЇМ

Сучасне людство вступає в епоху інформаційного суспільства, що має свої «плюси та «мінуси»». Окрім позитивних моментів нові соціальні реалії «інформаційної епохи» з тотальним поширенням інформації можуть бути потенційними викликами та загрозами національній безпеці. Серед таких загроз виділяються фейки, дізфейки, маніпуляції, які противник використовує для досягнення своїх цілей невоєнними методами. У цій роботі ми розглянемо феномен російських інформаційних маніпуляцій, спрямованих на спотворення історії України, та визначимо способи, якими цьому можна протистояти.

Історія є невід'ємною частиною культурної спадщини кожної нації, і вона має важливе значення для формування національної ідентичності та розуміння минулого. Проте, в сучасному інформаційному світі, де фейки та дізфейки стають все поширенішими, ми зустрічаємось з тим, що історичні факти свідомо спотворюються. Україна, як незалежна держава, завжди була предметом інтересу для сусідньої Росії, особливо після отримання незалежності в 1991 р. РФ вживає різні засоби для впливу на громадську думку в Україні та за кордоном, в тому числі й фейки та маніпуляції щодо історії України. Ці неправдиві дані дуже швидко та занадто легко поширюються через різні соціальні мережі та мають на меті спотворити образ України та її історію в очах громадськості.

Наведемо основні фейки, які поширює російська пропаганда щодо історії України:

1. «Україна не має власної історії». В цьому ракурсі історія України подається виключно крізь призму російської історії, що України ніколи не було, а є логічне державне продовження «Русь-Росія».

2. «Україна була створена Росією». Намагання переконати, що Україна як незалежна держава є наслідком імперіалістичних зусиль Росії, а не результатом власної історії та боротьби за незалежність. Можемо з цього приводу згадати промову Путіна, що «Україну створив Ленін».

3. «Голодомор не був геноцидом». Спростовується факт геноциду українського народу в 1932-1933 р., відкидається відповідальність за цю трагедію, перекичуються історичні факти.

4. «Крим завжди був частиною Росії». Саме цим фейком РФ виправдовує анексію Криму у 2014 році.

5. «Україна співпрацювала з нацистами під час Другої світової війни». Ця теза спрямована на дискредитацію українського опору проти нацистської окупації під час Другої світової війни та створення негативного образу України.

Російські інформаційні маніпуляції у сфері історії України є складним і великим аспектом сучасної інформаційної війни й, безсумнівно, мають вплив на національну безпеку. Чимало з наведених фейків розвінчані в книзі «Ре-візія історії. Російська історична пропаганда та Україна» (Єрмоленко, 2019). Але можемо зазначити, що в умовах повномасштабної війни росії проти України більшість українців навчилися цьому протистояти. Чимало закордонних аналітиків зазначають, що Україна на сьогодні виграла інформаційну складову війни, залишилася тільки війна фізична (Свідерська, 2022). Але, тим не менше інформаційні вкиди не припиняються.

Сучасний світ вимагає від нас не тільки споживати інформацію, але й критично аналізувати її та розрізняти правду від брехні. Освіта грає ключову роль у цьому процесі, і саме її удосконалення допоможе нашому суспільству зберегти віру в правдивість інформації. Одним з ключових завдань вивчення

у ЗВО дисципліни «Історія України» під час війни росії проти України є виявлення та боротьба з дезінформацією що поширюється щодо історії нашої країни, вміння розпізнавати фейки, діпфейки та правдиві історичні факти, критично оцінювати джерела інформації тощо. Необхідно надавати здобувачам навички аналізу первинних джерел, вміння перевіряти факти, порівнювати інтерпретації історичних подій, а не сліпо довіряти будь-якій інформації.

Для боротьби з маніпуляціями та фейками важливо:

- підтримувати високі стандарти історичних досліджень;
- виробляти вміння працювати з оригінальними джерелами (архівні документи, історичні тексти, свідчення очевидців тощо);
- вміти підбирати та перевіряти джерела інформації (здобувачі мають навчитися розрізняти авторитетні джерела від сумнівних, довіряти лише перевіреним джерелам, наприклад, звернутися до онлайн-медіа, що відносяться до «білого списку» найкращих українських онлайн-медіа («Онлайн-медіа», 2023));
- розвивати критичне мислення (важливо навчити ставити питання, аналізувати джерела, порівнювати різні джерела та подавати обґрунтовані висновки);
- не поширювати неперевірені дані;
- розвивати цифрову грамотність (здобувачі повинні вміти розрізняти відредаговані фотографії та відео, розуміти алгоритми соціальних мереж і пошуку, знати та користуватися законами щодо інтернет-безпеки тощо) та ін.

Такими методами можна вдосконалити інформаційну безпеку та запобігти спотворенню історії України.

Отже, знання правдивої, об'єктивної історії України мають важливе значення не лише для розуміння минулого, а й для формування громадянської ідентичності та національної безпеки. В сучасному інформаційному суспільстві важливо віддавати належну увагу протидії фейкам, діпфейкам, маніпуляціям та розвивати свою інформаційну та медійну грамотність, в т.ч. і через проходження різноманітних онлайн курсів. Освіта та педагоги мають відігравати важливу роль у навчанні критичного мислення, аналізу джерел та розуміння важливості історичної правди. Потрібно збільшувати кількість

аудиторних годин на вивчення історії України у ЗВО, активно поширювати у суспільстві правдиву інформацію щодо вітчизняної історії, вчитися відрізняти правду від брехні, не поширювати якісь емоційні пости, які містять неперевірену Вами інформацію. Завдяки таким зусиллям ми можемо забезпечити стійке майбутнє для нашого суспільства, зберегти історичну ідентичність України та сприяти національній безпеці.

Література

Єрмоленко, В. (ред.) (2019). Ре-візія історії. *Російська історична пропаганда та Україна*. Київ: К.І.С.

Онлайн-медіа, що стали найякіснішими: білий список другого півріччя 2023. *Інститут масової інформації*. URL: <https://imi.org.ua/monitorings/onlajn-media-shho-staly-najyakisnishymy-bilyj-spysok-drugogo-pivrichchya-2023-i55817>

Свідерська, О. І. (2022). Цифрова пропаганда та ризики інформаційної безпеки у контексті російсько-української війни. *Політикус*. 2, 60-65. URL: <https://doi.org/10.24195/2414-9616.2022-2.10>

Шеломовська Оксана Миколаївна
*кандидат наук з державного управління, доцент,
Дніпровський державний технічний університет,
м. Кам'янське, Україна*
ORCID: 0000-0003-3409-9435

ФЕЙК-НЬЮЗ В СОЦІАЛЬНИХ МЕРЕЖАХ: СОЦІОЛОГІЧНИЙ АНАЛІЗ

Поширення інтернету і соціальних мереж значно полегшило поширення інформації та вільного доступу до неї. Це, в свою чергу, активізувало проблематику фейків і фейкових новин, які є однією з найголовніших загроз сучасності, особливо в умовах війни. Загалом, тема фейків у сучасному медіапросторі стала особливо популярною після президентських виборів у США 2016 року, коли інформаційні дуелі перемістились з телевізійного екрану до соціальних мереж. Проблема фейкових новин стосується всього світу, і вона поширюється все ширше, оскільки люди приділяють більше уваги новинам з соціальних мереж. Люди схильні довіряти інформації, що узгоджується з їхніми особистими переконаннями та відкидати будь-яку перевірку фактів, що дисонує з ними.

Фейкові новини – це явище, яке існує вже давно, хоча, безперечно, саме вираз «фейкові новини» став більш поширеним в останні роки. У 2017 році вираз “fake news” був визнаний словом року в словнику англійської мови Collins Dictionary. У ньому фейкові новини визначаються як неправдива, часто сенсаційна інформація, що поширюється під видом новинних повідомлень. Фактично, фейкньюс (фальшиві новини, інформаційні «качки») – це недостовірна, неправдива, спотворена або неповна інформація, що розповсюджується через медіа. Це інформаційна містифікація і навмисне поширення дезінформації у соціальних медіа і традиційних ЗМІ з метою введення в оману, щоб отримати фінансову чи політичну вигоду. У сучасному медіапросторі поняття "фейк" може включати не лише фальшиві новини, але й

підроблені фотографії, сторінки в соціальних мережах, створені від імені іншої особи – все, що не відповідає реальним фактам дійсності. Слово «фейк» щодо інформації у ЗМІ чи соціальних мережах завжди має негативне значення. Їхнє завдання – вводити в оману, спотворювати картину світу, тому вони є надзвичайно шкідливими для суспільства.

Сьогодні поширення фейкових новин набуває рис епідемії, оскільки, з одного боку, аудиторія втрачає довіру до більшості ЗМІ (вважаючи їх схильними до певної точки зору) і віддає перевагу отриманню інформації через соціальні медіа, а з іншого боку, саме завдяки соціальним мережам явище фейк-ньюз стає надзвичайно масовим. Фейкові новини пов'язані з емоційною стабільністю учасників комунікаційного процесу та народжуються в умовах кризи, відсутності рівноваги, що підтверджується експериментальним шляхом. Емоційна збудженість та відсутність почуття контролю стимулюють довіру до фейкових тверджень.

Поширення дезінформації виглядає так само, як поширення будь-якої іншої інфекції через соціальні контакти всередині соціальних груп («бульбашок»). Результати досліджень показують, що 38,9% учасників кожної «бульбашки» мають однакову схильність вірити дезінформації. Загалом, один контакт ділиться інформацією з 2,5% інших контактів в межах цієї бульбашки, але з урахуванням кількості контактів стає зрозуміло, що, незважаючи на такий низький відсоток, інформація в бульбашках все одно постійно циркулює. При цьому ця інформація може бути як хибною, так і правдивою однаковою мірою (Brainard, Hunter, Hall).

Дослідники MIT Management Sloan School виявили, що неправдиві чутки поширюються швидше та ширше, ніж правдива інформація. Було виявлено, що неправду на 70% частіше ретвітять у Twitter, ніж правду, і вона досягає перших 1500 людей у шість разів швидше. Цей ефект є більш вираженим у політичних новинах, ніж в інших категоріях. Боти поширюють правдиву та неправдиву інформацію з однаковою швидкістю, тому люди ретвітують неправдиву інформацію. За три дні достовірну інформацію передають у твіттері по ланцюгу від 10 до 11 осіб,

тоді як фейк репостять удвічі більше людей. Одна з можливих причин – гіпотеза новизни – людей приваблює нова та незвичайна інформація, яка часто буває саме у неправдивих новинах (MIT Sloan research).

За даними новітнього звіту Reuters Institute, побоювання суспільства щодо дезінформації та дезінформації залишається на високому рівні. У більшості випадків понад половина (56%) висловлює занепокоєння щодо розрізнення правдивої та фальшивої інформації в Інтернеті щодо новин, що є на 2 відсоткових пункти більше, ніж минулого року. Ті, хто в основному використовує соціальні медіа як джерело новин, виражають значно більше занепокоєння (64%), ніж ті, хто взагалі не використовує їх (50%). Багато країн з найвищим рівнем стурбованості також схильні використовувати соціальні медіа для отримання новин. Це не означає, що використання соціальних медіа спричинює розповсюдження дезінформації, але зафіксовані проблеми на цих платформах і більше взаємодії з різноманітними джерелами, схоже, впливають на впевненість людей у інформації, яку вони зустрічають (Report, 2023).

Найбільша частка осіб, які думаючи про онлайн-новини, висловлюють занепокоєння щодо того, що є справжнім, а що фейковим в інтернеті зафіксована в Африці (77%), а найменша в Європі (53%). За даними соціологічного дослідження Громадянської мережі ОПОРА «Медіаспоживання та громадсько-політична активність українців за кордоном», проведеного соціологічною групою «Рейтинг» у квітні – травні 2023 року (n=3043) у середньому 23% респондентів бачили неправдиву інформацію про Україну. Найбільше таких випадків зафіксовано в Ізраїлі (32%), трохи менше – в Чехії (26%), Німеччині (25%), Іспанії (23%), Угорщині (21%), а найменше – у Великій Британії (19%) та США (17%). Найчастіше респонденти бачили фейки про Україну в міжнародному сегменті соціальних мереж (62%). Серед українських джерел найбільше фейків траплялося в каналах та групах у месенджерах (50%) і соціальних мережах (47%). Більшість опитаних самостійно не перевіряє сумнівні повідомлення, а «просто знає, що це брехня чи маніпуляція» (56%), особливо коли йдеться про старших респондентів. Лише третина опитаних

перевіряє інформацію в інших джерелах – частіше це молодь (Медіаспоживання та громадсько-політична активність українців).

Опитування «Українські медіа, ставлення та довіра у 2022 р.», проведеного InMind на замовлення Internews, встановило, що про існування неправдивих новин знають 83% опитаних. Серед тих, кому відомо про такі матеріали, 3/4 декларують, що вміють відрізнити неправдиві новини від правдивих. Рівень впевненості спонукає людей думати, що проблема не є нагальною, адже тільки 37% обізнаних вважають проблему дезінформації актуальною. Більшості опитуваних – 78% – відомо про існування замовних матеріалів і 72% серед них вважають, що можуть відрізнити такі матеріали від справжніх новин. Основними критеріями, за якими можна відрізнити дезінформацію є: помітний заголовок, емоційно забарвлений текст, невідоме джерело / тільки одне джерело, неповна інформація, відсутність деталей, неточність цифр, неякісний аналіз подій, немає інформацій з місця події. Незважаючи на названі критерії, респонденти у повсякденному житті при визначенні дезінформації скоріше покладаються на свою інтуїцію, або оцінюють новину на логічність/алогічність. Майже кожний четвертий опитуваний (27%) зазначив, що знає про сервіси, за допомогою яких можна здійснити перевірку матеріалів на достовірність, але лише 26% з них мали досвід їх використання (Українські медіа, 2022).

Останні кілька десятиліть можна охарактеризувати як період пост-пост-правди, в якій важко відрізнити факти від сфабрикованої брехні. Небезпека фейк-ньюз, запущених через соціальні медіа полягає у тому, що вони можуть поширюватися вірусно та досягати величезного числа людей без особливого контролю за змістом інформації. Кількість фейкових новин збільшується пропорційно нестабільності в державі, а прямої залежності між схильністю вірити фейковим новинам та демографічними характеристиками населення не існує. При цьому, якщо виключити фактор стресу, люди з вищим рівнем освіти легше виявляють фейкові новини і менше схильні погоджуватись поширювати їх. Люди, що володіють аналітичним мисленням, швидше за все відрізнятимуть правду від брехні,

незалежно від їхніх політичних поглядів. Саме тому, існує необхідність підвищення медіаграмотності звичайного споживача інформаційних продуктів та розвитку навичок критичного мислення.

Література

Brainard J., Hunter P.R., Hall I.R. *An agent-based model about the effects of fake news on a norovirus outbreak.*
URL: <https://pubmed.ncbi.nlm.nih.gov/32037129/>.

MIT Sloan research about social media, misinformation, and elections.
URL: <https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections>.

Reuters Institute Digital News Report 2023.
URL: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf.

Медіаспоживання та громадсько-політична активність українців за кордоном. Велика Британія, Ізраїль, Іспанія, Німеччина, США, Угорщина, Чехія. URL: <https://www.opora.ua.org/viyna/doslidzhennia-mediaspozivannia-ta-gromadsko-politichna-aktivnist-ukrayintsiv-za-kordonom-24756>.

Українські медіа, ставлення та довіра у 2022 р.
URL: <https://internews.in.ua/wp-content/uploads/2022/11/Ukrainski-media-stavlennia-ta-dovira-2022-1.pdf>.

Медведська Вікторія Юрївна
доктор філософії з політології,
Луганський національний університет імені Тараса Шевченка,
м. Полтава, Україна
ORCID: 0000-0001-6817-155X

ДІПФЕЙКИ ЯК ЗАГРОЗА РОЗВИТКУ ТА ЕФЕКТИВНОГО ФУНКЦІОНУВАННЯ ДЕЛІБЕРАТИВНОЇ ДЕМОКРАТІЇ В УКРАЇНІ

Деліберативна демократія як модель взаємодії держави та громадянського суспільства дедалі більше набуває своєї актуальності. Зважаючи, що сьогодні Україна виборює свій шлях у найбільшому конфлікті на європейському континенті з часів Другої світової війни, питання щодо перспектив розбудови та розвитку деліберативної демократії в Україні у післявоєнні часи є надактуальним. Водночас, дідфейки, дезінформація та використання штучного інтелекту створюють ризики зловживання цими інструментами для успішної політичної та соціальної організації суспільства.

Фундаментальна демократична держава, яка ґрунтувалася б на довірі народу, який усвідомлює свою суспільну роль і відповідальність у державному управлінні, активній та постійній залученості громадян у процеси продукування, прийняття виважених політичних рішень та реалізації державної політики, необхідна сучасним демократичним суспільствам. Ключовим елементом функціонування ефективної деліберативної політики виступає довіра між державою і суспільством, дефіцит якої відчувається в сучасній політичній практиці і без подолання якого неможливий відкритий політичний дискурс з актуальних проблем.

З метою встановлення ризиків та загроз дідфейків на розвиток та функціонування деліберативної демократії в Україні, спершу необхідно визначити їх сутність та особливості проявів в суспільно-політичних процесах. Дідфейк виступає

інструментом генерації фальшивих відео та зображень. Дану технологію переважно застосовують до зображень, рухомого відеоконтенту, аудіо та тексту. Даний інструмент може становити неабияку загрозу, якщо його застосовувати для дезінформації та ведення брудних ігор в політичному середовищі.

Водночас, під деліберативною демократією розуміємо модель демократії, яка передбачає інституціоналізований діалог органів державної влади та громадянського суспільства, опосередкований аргументованим публічним дискурсом задля досягнення консенсусу, дотримання процедурно закріплених норм якого забезпечує раціональність політичних рішень (Медведська, 2021, С. 65). Зокрема, важливу роль за цієї моделі демократії варто присвятити обговоренню (деліберації). Це форма участі, за якої представники державної гілки влади можуть почути позиції та думки громадян, надати свій зворотній зв'язок, а також формалізувати рішення з питання, яке розглядалось під час деліберації.

Немає сумнівів, що небезпека використання дідфейків полягає у послабленні основ демократії як такої. Дослідження цієї проблематики дозволить зробити вагомий внесок у закріплення основ довіри між громадянами та органами державної влади в демократичних режимах.

Марія Павелець, наукова співробітниця Міжнародного центру етики в наукових і гуманітарних науках (IZEW) Тюбінгенського університету в Німеччині, у своїй роботі «Дідфейки та демократія» систематизує різні типи дідфейків, які можна розглядати як дезінформацію або мову ненависті, та окреслює яким чином вони послаблюють основні демократичні функції та норми. Зокрема, дослідниця визначає, що дідфейки перешкоджають уповноваженій участі громадян у дебатах та продукуванні деліберативних рішень, які їх стосуються (Pawelec, 2022)

Водночас, політичні технологи та аналітики побоюються дідфейків як інструменту «виклику правді в політиці», а громадські організації вважають, що цю технологію можуть використовувати авторитарні режими для досягнення диктаторських цілей та нав'язування власної волі (Pawelec, 2022).

Маніпулятивні відеозаписи мають на меті підірвати авторитет тієї чи іншої особи, переписати загальновідомі факти, спровокувати шквал хейту в сторону державних та політичних діячів, громадських активістів, знаменитостей, тощо. Діпфейки як продукт алгоритмів штучного інтелекту взаємодіють у генеративній змагальній мережі (GAN), за допомогою якої можна опрацювати щонайменше 250 фотографій будь-якої людини та створити фальшивий відеоконтент для прихованого впровадження в психіку громадськості власних мотивів (Вальорска, М. Агнешка, 2020). Зрозуміло, що політично зумовлена дезінформація, навмисне поширення маніпулятивного контенту вимагає розуміння основних необхідних кроків для виявлення потенційних діпфейків.

Згідно посібнику, розробленого командою Центру стратегічних комунікацій та інформаційної безпеки, створеного при Міністерстві культури та інформаційної політики України, спільно з Центром демократії та верховенства права за фінансової підтримки Швеції в межах проєкту «Школа протидії дезінформації», виокремлено наступні дії для аналізу та ідентифікації потенційних діпфейків (Аналітичний посібник, 2023):

1. Бути прискіпливим до відомостей про відео, які ви переглядаєте та враховувати якість зображення, дату публікації, його джерело, інформацію про автора, тощо.
2. Зосередити увагу на кадруванні та деталях зображених на відео, зокрема на назви міст, закладів, інфраструктуру, пору року і т.д.
3. Зробити скріншот екрану та перевірити на достовірність зображення за допомогою сервісу Google.
4. Проглянути інші достовірні ресурси на наявність того чи іншого зображення або відео і тим самим визначити його справжність (Аналітичний посібник, 2023).

Безперечно, діпфейки підривають колективний порядок денний і формування довіри та волі громадян. Результатом цього варто зазначити зниження легітимності прийнятих спільно з органами державної влади рішень, чому особливо загрожують поширені побоювання фальшивих маніпуляцій, зокрема під час

війни. Водночас, враховуючи контекст використання дипфейків, можемо припустити, що даний інструмент має не лише негативний вплив на розвиток деліберативної демократії, а також взаємодію держави та громадянського суспільства, що вимагає подальших прикладних наукових досліджень.

Отже, оскільки в основі деліберативної демократії лежить публічний дискурс, який розуміємо як процес обговорення, обміну думками, переконання, аргументацію, досягнення компромісу у ході продукування політичних рішень, дипфейки виступають як небезпечні технології на шляху формування ефективної політичної комунікації між органами державної влади та українського суспільства.

Позаяк розвиток деліберативної демократії в Україні потребує напрацювання механізмів для перевірки достовірності як зображувального, так і відеоконтенту, а також системи заходів для боротьби із фальшивими підробками, націленими на досягнення вигідного становища в тих чи інших політичних колах.

Література

Аналітичний посібник (2023). Гібридна війна Росії проти України. Як перемогти на інформаційному фронті. *Центр стратегічних комунікацій та інформаційної безпеки*. Україна. URL: <https://drive.google.com/file/d/1AEUYRLeYOx7kBbNPJL1XzwHXstCNJaJW/view>

Вальорска М. Агнешка (2020). *Дипфейк та дезінформація: практичний посібник*. Київ. URL: https://www.aup.com.ua/uploads/DEEPFAKES_FNF_AUP_2020.pdf

Медведська, В. Ю. (2021). *Деліберативна демократія як модель взаємодії держави та громадянського суспільства*: дисертація на здобуття наукового ступеня доктора філософії. Київ.

Pawelec, M. (2022). Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions. *DISO 1 (2): 19*. doi: <https://doi.org/10.1007/s44206-022-00010-6>

Ercan, S. A., Asenbaum, H., Curato, N., Mendonça, R. F. (2022). *Research Methods in Deliberative Democracy*. Oxford University Press. doi: [10.1093/oso/9780192848925.001.0001](https://doi.org/10.1093/oso/9780192848925.001.0001)

Лисичкіна Ірина Олексіївна
кандидат філологічних наук, доцент,
Національна академія Національної гвардії України,
м. Харків, Україна
ORCID: 0000-0002-2050-9379

Лисичкіна Ольга Олексіївна
кандидат філологічних наук, доцент,
Національна академія Національної гвардії України,
м. Харків, Україна
ORCID: 0000-0002-9511-9615

ФЕЙКОВІ НОВИНИ В СУЧАСНОМУ МЕДІЙНОМУ ПРОСТОРІ

Пересічна людина перенасичена інформацією, яка часто надходить у формі новин, причому факти перемишуються із вигадками з метою ввести в оману, обманути та нав'язати певні погляди та ідеї. Це стосується не лише новин, а й самих фактів, які втратили прямий зв'язок з реальністю з появою нового терміну "альтернативні факти" як неправди, фейків та брехні.

Мета нашого дослідження полягає в окресленні особливостей функціонування фейкових новин у сучасному медіа просторі.

Зауважимо, що факт – це щось, що дійсно існує – те, що ми називали б "реальністю" або "правдою". Альтернатива – це один із варіантів у наборі даних варіантів; зазвичай ці варіанти є протилежностями один одному. Отже, альтернативні факти – це протилежність реальності (тобто уява) або протилежність правді (неправда) (Dictionary.com, 2023).

Більше того, стає все складніше відрізнити правду від неправди, оскільки реальність і правда є досить суб'єктивними, і люди схильні приписувати додаткові значення, які вони здобувають зі свого особистого досвіду. Всеохоплююча сила віртуальної реальності, створена, серед іншого, завдяки іграм, таким як "Second life" і "Minecraft", сприяє змішуванню реальностей, у яких живе людина. У результаті неможливе стає

можливим, і межі між реальним світом та іншими реальностями зникають. Люди, зазвичай, сприймають реальність з одного або двох проекцій, ігноруючи решту. Ці проекції корелюють з новинами у тій формі, в якій люди отримують нову інформацію щодо реальності.

Згідно із словником Collins, новини (Collins Dictionary, 2023) означають 1) інформацію про нещодавно змінену ситуацію або нещодавню подію; 2) інформацію, яка публікується в газетах і передається по радіо та телебаченню про нещодавні події в країні або світі, або в певній галузі діяльності. Варто зауважити, що канали передачі інформації мають включати соціальні медіа та інші ресурси Інтернету, оскільки багато людей віддають перевагу новим медіа для отримання новин. Визначення вище підкреслює основні ознаки інформації, щоб вона класифікувалася як новина: новизна і поширення (через публікацію або передавання). Важливо зауважити, що новини не є синонімом правдивості, оскільки їхня надійність залежить від низки чинників: джерела, точки зору, перспективи тощо.

З 2017 року, коли термін "фейкові новини" було оголошено Словом року (Collins, 2017) за версією Collins, цей термін отримав нові відтінки значень порівняно з початковим з словника. Фейкові або неправдиві новини можна відносно вільно описати як процес і результат поширення недостовірної чи оманливої інформації, а також як дезінформацію, коли поширення неправдивої інформації спрямоване на обман людей. Для приховання обману і недостовірності новин використовуються різні комунікативні стратегії, такі як іронія, заголовки, оманливі висновки з наданих фактів, виклад однієї позиції, неправдиве посилення на авторитетний джерело, відконтекстуалізований вміст, фабрикований вміст із зміненими фотографіями, діпфейк тощо.

Серед іншого, термін "фейкові новини" використовується як ярлик для будь-якої інформації або джерела інформації для дискредитації опонентського нарративу. В результаті цей термін втратив будь-яку зв'язок з фактичною достовірністю представленої інформації, і дослідники вважають, що фейкові новини "були безповоротно поларизовані в нашому поточному

політичному та медійному кліматі"(Vosoughi, 2018). Отже, для підкреслення (не)достовірності, термін "неправда" є більш виправданим, ніж "фейк".

Новини, як достовірні, так і неправдиві, використовуються для побудови нарративу, як "оповідання, яке пояснює дії об'єкта, щоб виправдати їх перед аудиторією, як послідовність подій зі значущістю для оповідача/об'єкта та аудиторії" (Denzin, 1989, P.95). Отже, вони включають в себе історії про події, які оповідач визначає як важливі для аудиторії, при цьому нарратив є бажаним описом реальності. Наративи є основним джерелом інформації, оскільки "наративи відповідають основним цінностям цільової аудиторії та аргументують переконливий опис причинно-наслідкових зв'язків, який об'єднує події в пояснювальний фрейм"(Antoniades, 2010).

Існування неправдивих новин само по собі не викликає захоплення свідомості адресата. Схильність адресата споживати неправдиві новини та їхня кількість важливі для досягнення ефекту. Іншими словами, вірусність неправдивих новин обумовлена наступними факторами:

- перенасиченість інформацією, особливо в стрічках соціальних медіа;
- обмежена увага аудиторії;
- підтверджувальна упередженість як схильність до поширення інформації, яка підтримує наші переконання;
- пізнавальна упередженість як посилення на систему цінностей та концепції, такі як "БЕЗПЕКА", "ТЕРОРИЗМ", "КАТАСТРОФА", "ПОЛІТИКА" тощо;
- ефект третьої особи, або наша тенденція вважати, що інші більш вразливі до впливу мас-медіа в контексті політичної комунікації в соціальних медіа.

Дослідники з Массачусетського технологічного інституту досліджували розповсюдження перевірених істинних та неправдивих новинних повідомлень, які поширювалися у Twitter з 2006 по 2017 рік (Vosoughi, 2018). Аналіз показав, що неправдиві історії досягають значно більшої аудиторії, поширюються швидше і ширше порівняно з істинними історіями. Було виявлено, що неправда поширювалася значно швидше, глибше

і ширше, ніж правда в усіх категоріях інформації, і ефекти були більш виразними для неправдивих політичних новин, ніж для неправдивих новин про тероризм, природні катастрофи, науку, міські легенди або фінансову інформацію. Неправдиві історії викликали страх, огиду та здивування, істинні історії викликали сум, радість і довіру. Навпаки до загальноприйнятого уявлення, боти прискорювали поширення як істинних, так і неправдивих новин з однаковою швидкістю, що свідчить про те, що неправда поширюється більше, ніж правда через людей, а не через ботів (Vosoughi, 2018).

Неправдиві новини можуть відрізнятись за впливом в залежності від теми, на яку вони посилаються. Таким чином, неправильна інформація в контексті політики є складнішою для розкриття, порівняно з темами, такими як охорона здоров'я або злочин. Дезінформація набагато потужніша за неправду через її характер обману та введення в оману.

Отже, огляд основних особливостей сучасного медіапростору, зокрема новин, наративів, неправдивих та фейкових новин, дозволяє визначити їхні особливості наступним чином: реальність та правда не є обов'язковою основою сучасного медіапростору новин, хоча вони включені в новини та наративи; наративи, побудовані на дезінформації і реалізовані у формі неправдивих новин, мають найвищий потенціал у захопленні свідомості людей; схильність людей до певного наративу стає залежністю, яка спотворює сприйняття реальності та правди; термін "фейкові новини" може використовуватися як політизований ярлик; неправдиві новини можуть базуватися на неправді та/або дезінформації та мають значний впливовий потенціал на свідомість адресата.

Література

- Alternative facts (2023). *Dictionary.com*.
 URL: <https://www.dictionary.com/e/slang/alternative-facts/>
- News (2023). *Collins Dictionary*.
 URL: <https://www.collinsdictionary.com/dictionary/english/news>
- Word of the Year Shortlist (2017). *Collins Dictionary*.
 URL: <https://www.collinsdictionary.com/word-lovers-blog/new/collins-2017-word-of-the-year-shortlist,396,HCB.html>

Vosoughi, S., Roy, D., Aral, S. (2018). The spread of true and false news online. *Science*, 359, 1146-1151. DOI:10.1126/science.aap9559.

Denzin, N. K. (1989). *Interpretive Biography*. Sage.

Antoniades, A., Miskimmon, A., O'Loughlin, B. (2010). Great Power Politics and Strategic Narratives. *Working Paper, 7. Centre for Global Political Economy, University of Sussex*. URL: <https://www.sussex.ac.uk/webteam/gateway/file.php?name=cgpe-wp07-antoniades-miskimmon-oloughlin.pdf&site=359>

Орел Ольга Володимирівна
*кандидат педагогічних наук,
ВСП «Ніжинський фаховий коледж
Національного університету біоресурсів
та природокористування України»,
м. Ніжин, Україна
ORCID: 0000-0001-5187-7580*

ФЕЙК ЯК ІНСТРУМЕНТ ПОБУДОВИ НАРАТИВУ

Що таке фейкові новини? Терміну Fake News більше 125 років, як зазначено у словнику Мерріама-Вебстера. Як кажуть, це чітке поєднання двох відомих слів: фейк і новина. Це новини (тобто «звіти ЗМІ»), які є фейковими («неправдивими, підробленими»). Фейкові новини включають багато різних речей: сатиричні новини, чорний піар, вигаданий наклеп на конкурентів, тобто все різноманіття інформаційного забруднення. Крім того, після Дональда Трампа цей термін стали використовувати політики всього світу, називаючи так ЗМІ, чия робота їм не подобається.

Фейкові новини – це навмисно спотворені або повністю вигадані новини.

Ми не можемо точно знати, чи свідомо спотворюються деякі новини, але фейкові новини – є частиною навмисної дезінформаційної кампанії, очолюваної Росією. Наприклад, це повна вигадка, що стародавні «укри», які начебто є предками українців, розкопали Чорне море. Російський телеканал посилається на неіснуючу книгу, але насправді інформація взята з гумористичного шоу (Дезінформація, 2021).

Проте не всі фейкові новини настільки абсурдні. Часто брехня не впадає в очі, а повідомлення частково містить правду. Наприклад, закид інформації, що Україна є найбіднішою країною Європи, виходячи з середньої заробітної плати. Це неправда, хоча зарплата в Україні і насправді не найвища.

Такого роду фейкові новини поступово змінюють ставлення читача до певного явища, події, особи чи групи людей, особливо якщо вони є регулярними (Орел, Лисенко, 2022).

Наприклад, президент України майже завжди стає мішенню кремлівських фейкових новин. Мовляв, головну державну посаду займає непридатна для цього людина. При цьому навіть не важливо, хто наразі є президентом. За такої умови атакується сама ідея української державності. Якщо говорити про явища, то можна згадати волонтерський рух 2014 року в Україні. Росія створила багато фейкових новин про те, що добровольці – нацисти, або іноземні найманці, які вчиняють різні злочини. Коли понад мільйон українців стали внутрішньо переміщеними особами з окупованих територій, багато неправдивих новин мали на меті настроїти місцевих жителів проти них – і навпаки. Це налаштування груп людей один проти одного (Орел, Лисенко, 2022).

Такою групою може стати цілий народ, наприклад, кримські татари. Сама по собі кожна окрема фейкова новина не є сенсацією, деякі з них навіть виглядають смішно. Ефект досягається за рахунок масштабу та регулярності, крок за кроком. Досить раз побачити неправдиву інформацію, щоб зробити її вашими базовими знанням, навіть не завжди усвідомленими. Навіть, якщо згодом ця інформація буде спростованою, підсвідомо вона залишиться з вами, тому не читайте і не дивіться підозрілі новини. Цей акумулюючий ефект небезпечний! Фейкові новини також підривають довіру до ЗМІ загалом. Мовляв, всі брешуть, але так думати помилково (Дезінформація, 2021).

Відповідальні ЗМІ існують, і ми повинні вміти їх відрізнити. Від цього залежить якість нашої інформації та, як наслідок, наших правильних умовиводів. Очевидно, що це свідоме формування іміджу України. Але що таке імідж? Найбільше за кількістю дезінформації проти України полягає в дискредитації нашої влади, церкви, армії та інших інституцій. Все це для того, щоб показати Україну як слабку, занепалу, пограбовану попередніми владами державу, а Євромайдан – як державний переворот (Дезінформація, 2021).

Найбільше фейків про українську армію – кожен дев'ятий. Їй приписували різні злочини і диверсії. Наприклад, що українські військові просили у Росії притулку, чи гвалтували літніх жінок, чи грабували неіснуючі магазини, або офіцери випробували американську вакцину від коронавірусу на солдатах.

Усі ці історії відповідають двом протилежним сюжетам (Дезінформація, 2021):

про слабкість української армії;

про її жорстокість, аж до варварства.

Теза про слабку та неорганізовану українську армію з'явилася у 2014 році – на відміну від добре організованої та навченої низкою анексії територій незалежних країн (Грузія, Молдова) російської армії. Потім стало зрозуміло, що наша армія, завдяки добровольцям та волонтерам не така вже й слабка. Чому варті Наші Українські Кіборги – захисники Донецького аеропорту, які мужньо захищали доступи ворога до важливої авіаційної розв'язки окупованого Донецьку.

Потім була «сенсаційна» новина про звірства Українських військових – вигаданий хлопчик, розіп'ятий українськими воїнами у Слов'янську Донецької області. Цей дикий наратив сягає своїм корінням у Першу світову війну. У той час Британія поширювала брехливу історію про канадського солдата, розіп'ятого німцями. Це явище відоме як дегуманізація ворога – зобразити ворога не як людину, а як хижака, що жадає крові, а єдиний спосіб захистити себе – знищити цих «недолюдей». Такий захист своїх інтересів знімає внутрішню заборону на вбивство того самого сина, батька чи друга... Вони вже не люди, а звірі, які знушаються заради насолоди (Орел, Лисенко, 2022).

Дегуманізація – це психологічний процес зниження цінності життя конкретної людини або групи, шляхом позбавлення людських рис (Дезінформація, 2021).

Демонізація – це більш агресивна форма дегуманізації, суть якої полягає в приписуванні людині або групі осіб, ознак, що негативно впливають на їх сприйняття (Дезінформація, 2021).

Дегуманізація – це спеціальна методика пропаганди, спрямована на формування негативної думки у більшості

стосовно певної групи осіб. Групу, яку хочуть дискримінувати, можуть представляти, як менш повноцінних або розумних в інтелектуальному чи культурному плані людей, що в свою чергу, знижує їх цінність для суспільства. Отже, дегуманізація – це спроба забрати у людини, саме її людську індивідуальність та зробити її частиною, певної нібито «неповноцінної» групи (Дегуманізація).

Отже Росія намагається дегуманізувати Майдан, українську владу та український народ загалом. У цієї фейкової новини три аудиторії: росіяни, українці та світ, а точніше Захід. Мета – зробити росіян готовими нас убити, змусити частину українського суспільства змиритися з цим і виправдати агресію Росії в Україні в очах Заходу.

Друга за поширеністю розповідь про Україну як нацистську, фашистську, ультраправу державу має ту саму мету – показати українців монстрами. Ось серія матеріалів на цю тему (Дезінформація, 2021):

- свастика на українських танках, намальована у фотошопі;
- портрет Гітлера, який ВО «Свобода» нібито пропонувала розмістити перед банкнотою номіналом 1000 гривень;
- мітинг з портретом Гітлера;
- українські діти граються з плюшевим Гітлером.

Деякі з цих прикладів можуть розсмішити нас, але політичні наслідки цих наративів цілком реальні. Наприклад, наприкінці 2020 року авторитетне видання *The Economist* писало про 17 тисяч західних бойовиків, які їздили в Україну воювати (*Assessing the threat from America's far right, 2021*). У статті посилалися на книгу відомого американського соціолога Синтії Міллер-Ідріс "Hate in the Homeland". Після скандалу в Twitter авторка вибачилася. Вона додала, що книга пройшла три зовнішні рецензії та юридичну рецензію. Авторка отримала цифру з дослідження, в якому все було навпаки – більшість із 17 тисяч були росіянами і воювали проти України. Спадає на думку той факт, що ніхто з експертів не перевіряв цю вражаючу цифру, що наратив «крайньої правої України» вводить в оману весь західний світ. Це здається правдоподібним навіть для вчених, які зобов'язані все перевіряти.

Як ви вже знаєте, західний світ і західні цінності також є об'єктом російської дезінформації. У кожній країні пропагандисти шукають слабкі місця і створюють фейкові новини, щоб довести ці слабкості до абсурду. Підробки поширюються між країнами, підлаштовуючись під місцевий контекст. Один з головних наративів Кремля про західні країни «Армагедон» через велику кількість біженців і мігрантів, переважно мусульман (Орел, Лисенко, 2022).

Але справжній «Армагедом» почався в кінці 2021 року зі спроби Росії та Білорусі розпалити новий конфлікт з біженцями (Попович, 2021). Їх привезли літаками в Білорусь і автобусами доставили на кордон з Польшою. Кадри про скупчення людей на Польсько-Білоруському кордоні облетіли весь світ. Люди жили в лісі, де вже було холодно, крім того там було багато неповнолітніх дітей, які потребували їжі і теплих речей. Не дочекавшись пропуску через кордон мігранти влаштували не вдалі провокації. Потім в таборі біженців стався сплеск хвороби Covid 19 та почали помирати люди (була навіть новина про смерть дитини). Тоді влада Білорусі зробила резервовані приміщення, в які помістили мігрантів. Люди стали заручниками карткової гри двох маніпуляторів.

Отже, фейкові новини можуть спровокувати цілком реальні наслідки. Розпалити ненависть та спровокувати протестні настрої, серед яких обов'язково будуть заслані проплачені провокатори.

Підводячи підсумок, можна сказати, що фейкові новини – це навмисно спотворені, зманіпульовані новини або повні вигадки. Фейкові новини поширюються швидше, ніж правдиві. Для боротьби з фейковими новинами важливо розвивати медіаграмотність, перевіряти джерела інформації та використовувати критичне мислення. Також потрібні законодавчі заходи і механізми для виявлення та припинення поширення фейкових новин, при цьому не обмежуючи свободу слова. Боротьба з фейковими новинами є важливим завданням для забезпечення інформаційної безпеки і стабільності суспільства.

Література

Дезінформація: види, інструменти та способи захисту (2021). *Prometheus*. URL: https://courses.prometheus.org.ua/courses/course_v1:Prometheus+DISINFO101+2021_T2/about

Орел, О. В., Лисенко, І. М. (2022). *Інформаційне суспільство: навчальний посібник*. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея».

Дегуманізація (Демонізація) – що це таке і як працює простими словами. URL: <https://termin.in.ua/dehumanizatsiia-demonizatsiia/>

Assessing the threat from America's far right. URL: <https://www.economist.com/books-and-arts/2020/12/12/assessing-the-threat-from-americas-far-right>.

Попович, Д. (2021). «Тінь Кремля»: хто керує мігрантами на кордоні з Польщею. URL: <https://www.slovoidilo.ua/2021/11/10/kolonka/denys-porovich/svit/tin-kremlya-xto-keruye-mihrantamy-kordoni-polshheyu>

Новік Андрій Костянтинович
*Запорізький національний університет,
м. Запоріжжя, Україна*

РОСІЙСЬКІ ФЕЙКИ ЯК ФАКТОР РИЗИКУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Вплив російських фейків на національну безпеку України є актуальною проблемою в сучасному інформаційному полі. Фейкова інформація, генерована та поширювана російськими пропагандистами, ефективно використовується для досягнення політичних, економічних та соціокультурних цілей, що може призвести до серйозних наслідків для суверенітету та стабільності України.

У контексті повномасштабної війни та інформаційної боротьби, де надмірна інформаційна потужність може бути такою ж деструктивною, як і фізичний вплив, аналіз та розуміння фейкової інформації стає надзвичайно важливим завданням для українських владних структур та громадянського суспільства (Вовк, 2022).

Росія має потужну пропагандистську машину, яка працює як всередині країни, так і за її межами протягом багатьох років. Після вторгнення до Грузії у 2008 році державні ЗМІ перетворилися на ще одну зброю в арсеналі росії. Завдяки величезному фінансуванню RT і Sputnik змогли охопити мільйони людей в Африці та деяких інших країнах, поширюючи дезінформацію та проросійські наративи, що негативним чином впливає на стан національної безпеки нашої країни.

Сьогодні, в умовах повномасштабної війни, яку Росія розв'язала проти України, згубний вплив цього впливу стає дедалі очевиднішим. Країни посилили боротьбу з російською пропагандою. Проте багато хибних уявлень про Україну – від історії країни до цінностей, які поділяють українці – все ще існують.

Поняття єдиної нації широко включено в статті та промови Путіна під час підготовки до повномасштабного вторгнення. Цей наратив не новий: створений у Російській імперії, він століттями використовувався, щоб позбавити українців власної мови, культури, історії, права на незалежність і навіть існування.

У 2014 році, коли Росія вперше напала на Україну, пропагандистські зусилля були спрямовані на те, щоб усіляко це заперечувати. У російських ЗМІ не було «вторгнення» чи «окупації», лише «громадянська війна» чи «внутрішній конфлікт». Проте будь-які спроби перейменувати цю агресію мали на меті лише зняти з Росії відповідальність за свої злочини.

У 2022 році, коли Росія збрала до українських кордонів до 200 тисяч військових і почала неспровоковане повномасштабне вторгнення, заперечувати це було неможливо. І таким чином у гру вступили інші наративи: конфлікт нібито був спровокований розширенням НАТО, а тепер це проксі-війна між росією та Заходом (*Proxу war, racism, and not your business*).

Існує безліч методів, які рф використовує для дестабілізації національної безпеки України.

- просування в українському інформаційному просторі антиукраїнських наративів з метою зниження морального духу населення;
- запуск «інформаційних вірусів» для сіяння паніки, формування відчуття зневіри у власних силах;
- маніпуляції суспільною свідомістю завдяки поширенню неправдивої, неповної або упередженої інформації, поширення фейків.

Основними цілями інформаційного таргетування рф є:

- Спротив мобілізації та поширення антидержавних настроїв, особливо через анонімні канали в мережі Інтернет.
- Російська агентура в московському патріархаті може використовувати релігійну сферу для розпалювання ворожнечі.
- Поширення інформації про порушення прав та свобод людини і громадянина в Україні, особливо через історії окремих осіб, може викликати емоційну реакцію та деморалізацію в суспільстві.

- Розповсюдження інформації про економічний крах та залежність від донорських коштів може створити негативний наратив і занурити суспільство в песимістичні настрої.

- Підсилити ідею «тривалої війни» та формувати враження неможливості перемоги, може сприяти розчаруванню та безнадії.

- Поширення неправдивої інформації про ситуацію в зоні активних бойових дій та стан Збройних Сил України, може використовувати для спонукування до переговорів з агресором.

- Посилення деструктивних емоцій, таких як ненависть та зневажливе ставлення, може призвести до дестабілізації суспільства (Павленко, 2023, С. 13–14).

В умовах сьогодення проблема поширення фейків і дезінформації через Facebook та інші соціальні платформи стала ще гострішою. Соціальні мережі та їх контент можуть використовувати як засіб ведення інформаційної війни, поширюючи фейки, тим самим підриваючи національну безпеку країни, проти якої застосовується цей інструмент. Основне призначення фейків – через поширення інформації зі специфічним змістом (який стосується безпосередніх життєвих проблем та «чіпляє» емоційно) зробити керованим населення іншої країни, домогтися в ній (у країні) порушення національної згоди та єдності, спричинити внутрішньополітичну дестабілізацію тощо (Вовк, 2022, С. 82).

Російська пропагандистська машина регулярно розповсюджує дезінформацію, спрямовану на дискредитацію різних соціальних груп та спільнот. Деякі пропагандистські повідомлення використовуються для маніпулювання чутливими темами, зокрема правами дітей. Це включає в себе фейки про порятунок від «українських нацистів-карателів», які приховують примусову депортацію дітей з України. Ця ситуація вважається ознакою геноциду з боку росії, і невідомо, чи зможуть ці діти повернутися до своїх батьків. Крім того, російська пропаганда атакує базові права людини, розповсюджуючи фейки про евакуацію з міст, де тривають бойові дії, надаючи недостовірну інформацію про роботу лікарень під час війни (Дезінформація як порушення прав людини в контексті російського вторгнення в Україну).

Отже, російські фейкові інформаційні кампанії є значущим фактором ризику для національної безпеки України. Вони сприяють дестабілізації суспільства, маніпулюють громадською думкою та впливають на політичні процеси. Для забезпечення національної безпеки України необхідно активно протидіяти цим інформаційним загрозам і розвивати інструменти виявлення та відповіді на дезінформацію.

Література

Vovk, V. (2022). Fakes as a threat to national security in the conditions of a hybrid war. *Law and politics*, 2, 80–85. URL: <https://doi.org/10.33270/02222402.80>.

Павленко, І. та ін. (2023). Аналіз загроз національній безпеці у сфері внутрішньої політики. *Центр внутрішньополітичних досліджень*. URL: <https://doi.org/10.53679/NISS-analytrep.2023.06>.

Proxy war, racism, and not your business: 7 lies about Ukraine that Russian propaganda spreads in African countries. URL: <https://war.ukraine.ua/articles/fakes-russian-propaganda-spreads-in-african-countries/>

Дезінформація як порушення прав людини в контексті російського вторгнення в Україну: фаховий звіт (2023). *Реанімаційний пакет реформ*. URL: <https://rpr.org.ua/news/dezinformatsiia-iak-porushennia-prav-liudyny-v-konteksti-rosiyskoho-vtorhnnennia-v-ukrainu-fakhovy-zvit/>

ФАКТЧЕКІНГ ЯК ІНСТРУМЕНТ ПРОТИДІЇ В ГІБРИДНІЙ ВІЙНІ

Суська Ольга Олександрівна

доктор соціологічних наук, доцент,

Національний університет «Києво-Могиланська академія»,

м. Київ, Україна

ORCID: 0000-0001-9620-1859

«ОБРАЗ СУСПІЛЬСТВА» ТА ЙОГО ТРАНСФОРМАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

З розвитком цифрових комунікацій імітаційні технології все ширше використовуються вже не тільки мистецтвом, а впроваджуються в політичне і соціальне життя, формуючи «образ суспільства», структуру взаємодії соціальних спільнот та соціальних інститутів (імітуючи засади демократії), тематику соціальних та медіакомунікацій.

Підкреслимо, що суспільство, де демократичні права і свободи громадян не підкріплені організаційно і економічно (відсутні механізми реалізації правових гарантій, що робить аморфним законодавство); де виникає так зване «суспільство декларативного права» (правові норми не втілюються, а виконують роль цивілізаційного «кліше», «заставки», якою прикривається влада); де, демократично обрана і легітимна влада не виконує своїх передвиборних зобов'язань, – в такому суспільстві неодмінно починає відігравати важливу роль маніпуляція, інформація перетворюється на низку фейків, а медіакомунікація перетворюється на застосування засобів віртуального втручання у «свідомість мас».

Якщо, виходячи з ідеї П. Бурд'є, розуміти соціальне «поле політики» як простір взаємодії між агентами, що мають свої певні диспозиції, засвоєні протягом такої взаємодії у полі, то можна

увити, що агенти реагують на співвідношення сили та результативності впливу на структури, які конструюють соціальні відносини. (Bourdieu, 1991). У демократичних суспільствах навіть за наявності примусу з боку сил, вписаних в ці поля (зокрема, засобами медіа), і визначення конкретних диспозицій «силами поля», агенти здатні впливати на нього, діяти згідно обраній траєкторії, передбачуваним напрямом, зберігаючи певний запас свободи.

Після повномасштабного російського вторгнення на територію України суттєво змінились очікування та зникла пасивність та небажання осмислювати реальні події. В умовах війни «через певний час настає адаптація особистості до цих умов. Людина тут набуває позабуденний досвід, але вона практично ніколи не може повністю адаптуватися до цих умов. ...Однак тепер взаємодія особистості з екстремальними умовами життя ускладнюється, а не зводиться лише до емоційних реакцій. ...Вона намагається впоратись з собою, осмислити у більш широкому масштабі своє місце в системі соціальних відносин, дати оцінку тому, що відбувається навколо, переоцінити надбання свого минулого досвіду» (Шульга, 2022, С. 47-48).

Умови війни загострили розбіжності етичних і моральних цінностей, а неспроможність протидіяти епізодам агресивних дій реальних ворогів, або «ворожості» суспільства, перетворилися іноді у нездатність опанувати собою. В одному випадку – це породжує ескейпізм (утікання) від контактів із суспільством, яке потрапило у воєнну кризу (масова міграція), в іншому випадку – як наслідок проявляється втрата смислів і цінностей діяльності (в т.ч. професійної), а також падіння рівня «соціального оптимізму» (Held, 1992).

Серед результатів щорічного моніторингу, що проводить Інститут соціології НАН України привертають увагу «рейтинг» актуальності соціетальних цінностей.

Звертає увагу те (табл. 1), що група цінностей: різноманіття, розвиток і селективність, яка спрямована на розвиток країни в широкому значенні, а саме – соціальному, науковому, кадровому зайняла останні позиції. І не тільки тому, що ними «можна тимчасово знехтувати» під час війни. Скоріше тут справляє

Оцінка актуальності соціетальних цінностей

Соціетальна цінність	Може тимчасово знехтувати	Не може тимчасово знехтувати		Баланс
		У другу чергу	У пріоритеті	
Безпека	11,3	6,4	82,3	71,0
Сила	15,9	6,8	77,3	61,4
Порядок	17,2	11,9	71,0	53,8
Нормативність	19,7	9,7	70,6	50,9
Рівність	21,0	14,5	64,5	43,5
Свобода	35,7	17,0	47,3	11,6
Стабільність	40,3	11,8	38,0	7,7
Самостійність	39,8	16,1	44,2	4,4
Різноманіття	41,4	18,3	40,4	-1,0
Розвиток	44,7	16,1	39,1	-5,6
Селективність	43,6	19,7	36,7	-6,9

Джерело: *Українське суспільство в умовах війни (2022)*. Київ: Інститут соціології НАНУ України. 278.

певний тиск попередній повільний рух України до Європи, опанування загальносвітовими та європейськими цінностями. Тут актуально навести висловлювання Скота Леша і Майка Фезерстоуна, яке акцентує застереження, що «глобальна технологія потоків уже деконструювала як націю-державу, так і стару метафізику присутності. Проблема полягає в тому, що одночасно з цим вона створила цілковито новий апарат (не)безпеки» (Фезерстоун, Леш, 2008, С. 33-34). Коли йдеться про спроби зайняти в суспільстві позиції відповідні рівню володіння знаннями та готовності до виконання певних обов'язків (селективність), або ж пропонувати екстенсивний розвиток певної галузі (розвиток), то серед розростання титулів і статусних регалій, виникає ситуація, яку Френсіс Фукуяма (Fukuyama, 1999) визначав як приналежність до штучно створених еліт. Численні різноманітні інтерактивні івенти, конкурси, «ріеліти-шоу»,

лотереї, ін., в яких існує і повсякденно бере участь *homo profanum* (за висловом Фукуями), проголошуються основою буття і поступово формують відповідний «юзерським» цінностям взірець – *homo inercialis*.

Очевидно, «образ суспільства» тісно поєднаний з так званим «образом еліт», і там, де вони стигматизуються або маргіналізуються (наприклад, як відбулося після оприлюднення електронних декларацій депутатів з наддоходами), то реальний потенціал довіри до еліт, а відтак і позитивний міжнародний імідж країни різко знижуються.

Протягом російсько-української війни, яка є гібридною за своєю суттю, має місце широкомасштабний процес «промивання мізків» з боку агресивної російської пропаганди, що особливо дається взнаки на тимчасово окупованих територіях. Завдяки реанімуванню атомізованих ідеологічних структур, застосуванню «мови ворожнечі», за рахунок вироблення відповідних рефлексів, російська пропаганда здійснює процес відвертого тиску суспільства на свідомість особи, маючи на меті досягнути однодумства та конформності серед населення окупованих територій.

Кризові суспільні явища, яким, безумовно, і є війна спричиняють суттєву поляризацію думок, переконань, настановлень, що позначаються на житті людей, адже, згідно з думкою І. Валлерстайна, «логіка» системи перетворюється у набір інституціональних структур, які самостійно рухаються, самопідкріплюються, які детермінують рух траєкторією; проте, жодна конкретна ситуація не є більш складною, ніж довгі «моменти переходу», коли руйнуються більш прості зв'язки (Wallerstein, 2011). Протягом таких складних етапів завжди збільшується питома вага інформованості мас про події та явища соціальної дійсності. Між продукуванням інформації мас-медіа та освітніми (інтелектуальними) зусиллями суб'єктів процесу інформаційного обміну спільним є те, що ЗМІ, виробляючи інформацію, одночасно створюють так званий «горизонт новизни» (Luhmann, 2001). За висловом Н. Лумана, «на рівні всього суспільства спостереження подій саме є подією, причому такою, що відбувається майже одночасно із подіями,

які спостерігаються. ...Проблема тому полягає не в істині, а в неминучій, але разом з тим бажаній та керованій селективності» (Луман, 2010, С. 54-55). Ця селективність є набутком досвіду та інтелектуальних зусиль самих суб'єктів комунікації, вона дійсно «бажана» і «керована», адже спрямована на здійснення свідомого інформаційного вибору. Ілюстрацією такого усвідомленого вибору може слугувати думка респондентів соціологічного моніторингу Інституту соціології НАН України (відповіді на запитання «Яку ситуацію Ви особисто розглядатимете як перемогу у війні?»). Найбільшою виявилась питома вага відповідей щодо позиції: «вигнання російських військ з усієї території України та відновлення кордонів станом на січень 2014р.», причому по регіонах відповіді розподілились таким чином: Захід – 53,6%, Центр – 55,4%, Південь – 56,9%, Схід – 45,4%, Україна в цілому – 54,7% (Українське суспільство..., 2022, С. 272). Очевидним відкриттям в сенсі «усвідомленої селективності» став вибір, зроблений мешканцями півдня, які найбільш зосереджені на меті перемоги та звільненні усіх українських територій. Таким чином, російсько-українська війна продемонструвала, що ніякі зусилля агресора (воєнні дії, захоплення та руйнування об'єктів критичної інфраструктури тощо), відвертий і агресивний тиск на населення – особливо захоплених територій, не досягають їхньої «гібридної мети» – підпорядкування думок і переконань населення владі російських окупантів.

Ступінь наближення «образу суспільства» до реальності (через медіа, соціальні мережі, інші канали інформування) демонструє ілюзорність або реальність уявлень громадян, при цьому, може викликати в кожного індивіда певні інтелектуально-логічні реакції та почуття. Трансформування медіаповедінки (в сенсі користування різними видами медіа – і «новими», і традиційними), доводить, що для орієнтації у сучасному медіапросторі індивіду необхідні не тільки знання і компетенції щодо інформаційного вибору, але й серйозні «світоорієнтаційні орієнтири». Одним з таких орієнтирів могло б стати успішне суспільство, яке б надавало можливості розвитку і становлення кожному громадянину і так само піклувалось про його успішність. На жаль, в умовах повномасштабної російсько-

української війни, ситуація не дає можливості спрогнозувати, коли образ українського суспільства стане саме таким. Проте протидія проявам гідридної війни і свідоме ставлення до формування «образу суспільства» у медіапросторі є запобіжниками ворожим проявам та маніпуляціям.

Література

- Луман, Н. (2010). *Реальність мас-медіа*. Київ: ЦВП.
- Українське суспільство в умовах війни 2022 (2022). Київ: Інститут соціології НАН України.
- Фезерстоун, М., Леш, С. (2008). *Глобалізація, модерність і опросторовлення суспільної теорії: Вступ. Глобальні модерності*. Київ: Ніка-Центр.
- Шульга, М. О. (2022). Очікування в екстремальних умовах. *Українське суспільство в умовах війни. 2022*. Київ: Інститут соціології НАН України, 46-55.
- Bourdieu, P., Coleman, J. M. (1991). *Social theory for a changing society*. New York: Russell Sage foundation, cop.
- Fukuyama, F. (1999). *The Great Disruption: Human Nature and the Reconstitution of Social Order*. Free Press.
- Held, D. O. (1992). Democracy: from city-states to a cosmopolitan order? Held, D. (ed.). *Prospects for democracy*. Cambridge: Polity Press, 13-52.
- Luhmann, N. (2001). *Was ist Kommunikation? Aufsätze und Reden*. Stuttgart.
- Susska, O., Chernii, L., Sukharevska, H. (2022). Media as a tool of manipulative technology of russian infoaggression in the ukrainian media space. *AD ALTA, Journal of Interdisciplinary Research, vol. 12, Is. 1, Special Issue XXV*, 228-234.
- Wallerstein, I. (2011). Structural crisis in the world-system: where do we go from here? *Monthly review*, 62, 10, 31-39.

Олексунь Надія Олександрівна

Державний університет «Житомирська політехніка»,

м. Житомир, Україна

ORCID: 0000-0001-8799-8894

Седляківська Карина Геннадіївна

Державний університет «Житомирська політехніка»,

Житомир, Україна

ЗАГРОЗИ ТА МЕХАНІЗМИ ПРОТИДІЇ РОСІЙСЬКІЙ ПРОПАГАНДИ В УМОВАХ ВІЙНИ

Сьогодні ми живемо в реаліях гібридної війни, де боротьба йде в різних доменах – на суші, в повітрі, на воді, а також, в інформаційному просторі. Однією з головних проблем, з якими стикається Україна, є дезінформація та інформаційні операції, зокрема з боку держави-агресора. Так, російська пропаганда активно поширює різну дезінформацію для того, щоб розпалити національні, міжрегіональні, міжетнічні та релігійні ворожнечі.

Так, за даними Merriam-Webster (американська компанія, видавець довідників та лексичних словників) дезінформація – це неправдива інформація, яка навмисно і часто приховано поширюється (наприклад, шляхом поширення чуток), щоб вплинути на громадську думку або приховати правду (Merriam-Webster, 2023).

Починаючи з 2014 року росія активно поширювала дезінформацію, щоб підірвати незалежність держави, зменшити рівень довіри населення до влади, а також, виправдати свої неправомірні та відверто злочинні дії на території нашої країни. Російська пропаганда намагається протягом всього періоду війни спотворити уявлення про Україну і про те, що відбувається на території нашої держави. Крім того, поширення фейків торкнулися не тільки України, а й інших держав світу. Так, Corneliu Bjola у своїй статті пише про викриття ЗМІ

про ймовірне використання російським урядом соціальних медіа для впливу на президентські вибори в Сполучених Штатах у 2016 році або, ширше, для зриву виборчих процесів у Європі, що змістило громадський та академічний дискурс у бік обговорення та розслідування “темних сторін” цифрової дипломатії (Bjola C., 2017).

Після анексії Криму та ведення активних бойових дій в Донецькій та Луганській областях, ми можемо прослідкувати певну тенденцію фейкових новин та меседжів, що з’явилась у пропагандистів, про злочини української влади під егідою США та інших країн-союзників НАТО. Такими повідомлення країна-терорист постійно намагалася виправдати свої дії на території нашої держави.

Російська пропаганда подає Україну як країну, яка перебуває у хаосі, злочинності та безладі. Вона акцентує увагу на політичних розбіжностях, відродженні фашистських ідеологій та націоналістичних рухів. Також, серед найулюбленіших тем пропагандистів, часто звучить ідея про розміщення різних біологічних лабораторій США на території нашої держави, хоча жодних доказів не було виявлено. Варто додати, що часто російська пропаганда поширює ідею, що Україна активно знищує православні церкви, особливо після того, як в нашій державі було утворено Православну церкву України. Саме під таким камуфляжем були розповсюджені фейки щодо пограбування та руйнування церковних споруд. Серед популярних фейків часто лунають звинувачення української армії у злочинах проти мирного населення або використанні заборонених видів зброї.

За даними ГО «Детектор медіа», яка з початку повномасштабного вторгнення запустила спецпроект «DisinfoChronicle», станом на кінець жовтня 2023 року зафіксовано понад 1700 фейків та близько 600 маніпуляцій щодо різних подій та всіх сфер суспільного життя в інформаційному просторі (Детектор медіа, 2023). Загалом, кількість російських фейків з кожним днем зростає, оскільки послаблюються позиції країни-терориста на міжнародній арені і разом з тим міцніють позиції нашої держави.

Українські структури і урядові органи активно займаються впровадженням різних заходів для боротьби з російською пропагандою. Зокрема, використовуються методи фактчекінгу, розкриття фейків, впровадження нових освітніх програм та поширення критичного мислення серед населення. Однак, співпраця з міжнародними партнерами та організаціями є також важливим елементом в цьому процесі. Ця співпраця передбачає обмін інформацією та координацію зусиль з метою ефективної боротьби з російською пропагандою.

Одним з основних державних інститутів, що працює в даному напрямку є Центр протидії дезінформації при РНБО, який відіграє провідну роль у виявленні і представленні фейкової інформації. Основним завданням Центру протидії дезінформації при Раді національної безпеки і оборони (РНБО) є боротьба з дезінформацією та захист національної безпеки України. Для досягнення цієї мети, Центр проводить аналіз і моніторинг інформаційних потоків, ідентифікує та розкриває випадки дезінформації та фейкової інформації, а також розробляє та розповсюджує факти та докази, щоб протидіяти ними. Крім того, Центр проводить інформаційні кампанії та освітні заходи для населення з метою підвищення обізнаності про дезінформацію та розуміння її наслідків. Також, Служба безпеки України веде активну діяльність по протидії пропагандистським впливам російської федерації.

Варто додати, що відповідно до Стратегії національної безпеки України, також, був розроблений окремий документ – план заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року. Серед заходів, запланованих в межах окресленого Плану, на нашу думку особливої уваги заслуговує проект «Spravdi», що спрямований на протидію дезінформаційним кампаніям та деструктивній пропаганді, фахова підготовка спеціалістів з раннього виявлення, прогнозування та запобігання гібридним загрозам, забезпечення реалізації Національного проекту з медіаграмотності «Фільтр» (Жуган В., 2017).

Для ефективного захисту від дезінформації та протидії російській пропаганді необхідно забезпечити широку освіченість

населення з цього питання. Важливим є вміння перевіряти отриману інформацію, переконатися в її достовірності шляхом звернення до інших джерел та маючи належні знання про методи пропагандистського впливу, що дозволяє виявляти маніпулятивні прийоми та технології.

Україна продовжує невпинно працювати над запобіганням та протидією російській пропаганді. Захист від дезінформації вимагає постійного вдосконалення механізмів, усвідомлення загроз та підтримки населення. Тільки завдяки цьому Україна зможе зберегти свою інформаційну незалежність, національну безпеку та єдність у важкі часи війни.

Література

Bjola, C. (2017). Propaganda in the digital age. *Global Affairs*, 3(3), 189–191. URL: <https://doi.org/10.1080/23340460.2017.1427694>

DisinfoChronicle. Кремлівська дезінформація щодо військового наступу на Україну. *Детектор медіа*. URL: <https://disinfo.detector.media/>

Merriam-Webster (nd). Дезінформація. У *словнику Merriam-Webster.com*. URL: <https://www.merriam-webster.com/dictionary/disinformation>

Жуган, В. (2017, 27 лютого). Доктрина інформаційної безпеки України – це лише декларація – експерти. *Радіо Свобода*. <https://www.radiosvoboda.org/a/28336852.html>

Сушко Валентина Анатоліївна
*кандидат історичних наук, доцент,
Інститут мистецтвознавства, фольклористики та етнології
імені М.Т.Рильського НАН України,
ORCID: 0000-0003-0480-1473*

НАЦІОНАЛЬНА ТА ЕТНІЧНА ІДЕНТИЧНІСТЬ УКРАЇНЦІВ В УМОВАХ ВІЙНИ (НА ПРИКЛАДІ ХАРКІВЩИНИ)

Відсіч, яку дає український народ повномасштабному вторгненню в Україну, вимагає осмислення цих подій і чіткішого усвідомлення головного діяча Спротиву. Особливе значення в цьому має той факт, що відсіч ворог отримав саме в східних, «російськомовних» та таких, де агресор нараховував найбільший відсоток «співвітчизників» (Доній, Фесенко, С. 249 – 250).

Конституція України паралельно уживає термін «Український народ» в значенні всіх громадян України («Верховна Рада України від імені Українського народу – громадян України всіх національностей» – Преамбула) та «українська нація» у значенні етнічної нації («Стаття 11. Держава сприяє консолідації та розвитку української нації, її історичної свідомості, традицій і культури, а також розвитку етнічної, культурної, мовної та релігійної самобутності всіх корінних народів і національних меншин України».)

Харківщина належить до історико-етнографічного регіону «Слобідська Україна», який виникає у період розвою української етнічної нації, у XVII ст.; видатний історик та архівіст Д.І.Багалій вважав, що Слобідську Україну заснували українці, які до кінця XVIII ст. були найчисельнішим етносом регіону, вкраплення служилих людей та ромів були незначні. Від початку XIX ст. у Харкові великою стає німецька та єврейська діаспори, які відіграють значну роль у розвитку економіки та культури Слобожанщини. Впродовж наступних століть кількість неукраїнців у регіоні збільшується, що було цілоспрямованою

політикою російської імперії та її нащадка – радянської держави. Неукраїнське населення ставало рушієм колонізації та зросійщення українців.

Радянські часи, особливо після II світової війни, стали часом, коли українськість, хоча й не заборонялася офіційно, проте народна культура поділялася на буржуазно-націоналістичну та радянську. З першою, безумовно, боролися, а друга поступово перетворювалася на вихолощену, непривабливу та нижчевартісну, від якої культурна людина мала відмовитися задля прогресивнішої та культурнішої – як тут не згадати дошкульні слова Володимира (Зеева) Жаботинського про такі ж процеси ще 1904 р. (Жаботинський, 1991, С. 34 – 38). Яскравим прикладом був університетський та промисловий Харків: вдома молодь говорила українською, приїжджаючи до міста на роботу чи навчання – російською. У місті Харків у 1980-ті роки українською була тільки ОДНА школа – № 6, в решті навчання велося російською, а українська мова з'являлася з 2-го класу як предмет, від вивчення якого дитину можна було звільнити.

Період Незалежності став часом, коли Україна намагалася подолати хворобу імперськості, і війна стала перевіркою результатів цих процесів. Уже перший етап війни (2014 р.) показав, що Харків – українське місто. Однак масове згуртування та запеклість у відстоюванні свого, себе, своєї української ідентичності, відбулися саме у лютому 2022 р.

Належність до політичної нації визначається виключно самосвідомістю, а ті ознаки, що були характерними для носія етнічної нації втрачають своє значення. За нашими спостереженнями та результатами інтерв'ю, ми можемо твердити: більшість харків'ян до 24.02.2022 р. були мешканцями цього міста у другому поколінні або й у першому поколінні. У значній мірі зв'язок з родом та місцем походження був втрачений або свідомо та повністю, або частково через віддаленість. Припускаємо, що саме через це в Харкові такий стійкий був стереотип «ми тут – невідомо, чи й українці, а от там (на Західній) – насправді українці». Адже діти, приїжджаючи до бабусь у село на Харківщині чи Сумщині, Волині чи Карпатах на канікули, бачили святкову та привабливу сторону життя. Можливо, саме тому

виявився таким стійким ще один давній, народницький, стереотип про «село як колиску й джерело нашої культури».

Серед маркерів традиційної культури (архітектура, костюм, кухня, традиційна обрядовість) до 1990-х, основна маса містян мала певні уподобання у кулінарії та обрядовості, пов'язаній з традиційною релігією родини, однак переважним було відмова від етнічного та наслідування уніфікованим, встановленим у пізньо-радянський час, стандартам. Повсякденне та святкове вбрання уже від кінця XIX ст. було цілком європейського зразка. Нав'язана радянська обрядовість наприкінці XX ст. стала такою загальноживаною практикою, при чому з цього переліку досить швидко випали «жовтневі свята». Офіційне затвердження православних свят як державних з вихідними днями закріпило їх статус. Набагато краще збереглися традиції народної кулінарії.

З 1991 року питання етнічної та національної самоідентифікації вкрай актуалізувалося: на нашу думку, особливо болочим воно було для етнічних росіян. Так, керівники гуртків історико-краєзнавчого напрямку з Чугуївщини скаржилися, що не знають, за яким сценарієм проводити народні свята у дитячих колективах – за українським чи за місцевими традиціями та як пояснювати дітям особливості місцевої локальної традиції. Симптоматичним був виступ на фестивалі «Вертеп-фест 2019» рою пластунок в російських сарафанах, які їхня виховниця подавала як традиційне українське вбрання на підставі того, що колекція була зібрана на території держави Україна – тому є українською й колекція, і культура її носіїв (зібрана ця колекція була в селі, навіть самоназва жителів якого – «кацяпи»).

Від 2014 р. актуалізувалися офіційні маркери держави: уже не лише на мітингах на підтримку України використовуються прапори, а й на вікнах та балконах приватних помешкань, як кольори вбрання, так, як і використання вишиванок та віночків, патріотичних патчів та принтів на вбранні та аксесуарах (від просто блакитно-жовтих та червоно-чорних стрічок до відомих мемів: «Рускій военний корабль...», «Харків – залізобетон», бойові гуси, котики-патріотики тощо). Харків'яни набагато більше стали знати про українські офіційні свята (День Соборності, День

Українського Війська та Козацтва, а також – окремих видів Збройних Сил України та Національної гвардії та тих бригад, які базуються на Харківщині та від 24 лютого воювали тут) та вітати з ними одне одного.

Українська політична нація вперше заявила про своє існування 1 грудня 1991 року, коли більшість мешканців України заявила про підтримку Незалежності України як держави. Війна безпосередньо стала каталізатором націєтворчих процесів, але тільки прискорювачем, бо процеси йшли й до того. Так, чимало людей, які до 24.02.2022 не позиціонували себе як українців, тим більше свідомих українців, кардинально змінили свою думку про державу, її цінність для них, про що свідчать дані опитувань та репортажі з Маршів Єдності та інших патріотичних заходів.

Література

Конституція України 1996 (Верховна Рада України). *Офіційний сайт Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>

Багалій, Д. І. (1991). *Історія Слобідської України*. Харків : Основа.

Жаботинський, В. (1991). Вибрані статті з національного питання. Київ, Республіканська асоціація українознавців.

Фесенко, В. (2019). Пошук національної ідеї чи розробка й реалізація стратегії інтеграції українського суспільства. *Трансформація української національної ідеї*, 248 – 256.

Всеукраїнський референдум (1991). *Вікіпедія*. URL: [https://uk.wikipedia.org/wiki/Всеукраїнський_референдум_\(1991\)](https://uk.wikipedia.org/wiki/Всеукраїнський_референдум_(1991))

Тисячі харків'ян вийшли на Марш єдності (2022). *DW*. URL: <https://www.dw.com/uk/тисячі-харків'ян-вийшли-на-марш-єдності/a-6067485>

Марш Єдності 05.02.2022. URL: <https://www.youtube.com/watch?v=jjTY0xKckx8>

94% українців пишаються своїм громадянством – опитування. Інтерфакс. URL: <https://interfax.com.ua/news/general/919771.html>

ПУБЛІЧНЕ УПРАВЛІННЯ ТА НАЦІОНАЛЬНА БЕЗПЕКА

Примуш Микола Васильович

*доктор політичних наук, професор,
Донецький національний університет імені Василя Стуса,
м. Вінниця, Україна*

ORCID: 0000-0001-5769-7345

РЕФОРМИ В ОБМІН НА ЗБРОЮ

Реформи, які повинна провести Україна для продовження надання їй допомоги, стосуються не лише роботи Міноборони України і усіх силових відомств, а й функціонування наглядових рад Державних підприємств, антикорупційних органів (САП, НАБУ, НАЗК), Вищої ради правосуддя і загалом судової гілки влади.

Наскільки виправдані такі вимоги США і чи здатна Україна їх втілювати, поки обороняється від агресора?

За своєю структурою документ більшою мірою пов'язаний з питаннями протидії, запобігання та боротьби з корупцією. Американці рекомендують унормувати на рівні закону те, як корелюються посадові обов'язки керівника Спеціалізованої антикорупційної прокуратури і очільника Офісу генерального прокурора. Коли до Конституції вносили зміни через створення САП, була допущена колізія, за якою керівника органу, що мав би бути незалежним, за підсумками конкурсу призначає генеральний прокурор. Це неправильно, адже робить таке призначення політично залежним: генпрокурор може не погодити призначення або затягувати його.

У судовій реформі також чимало подібних правових прогалин, як-от остаточне призначення судді указом президента чи відбір кандидатів на посади Радою доброчесності, яку призначають «свої» ж – ВККС.

Є чимало питань і до прозорості роботи митниці. Держава щороку втрачає мільярди доларів через контрабанду, тому закономірно, що в США питають: «Чому нічого не робите з тим, що вас грабують на митниці, поки ви шукаєте гроші на війну?».

Пункти, які зазначені в листі, – це передусім вимоги українського громадянського суспільства. І, направляючи такого листа, американські партнери радше підтримують українців, ніж ставлять їм ультиматум. Потреба в цих реформах нагальна, бо проблема корупції з війною не зникла, а лише загострилася. А ці кроки реальні до виконання. Те, що стосується запобігання корупції, прозорості конкурсів до органів антикорупційної інфраструктури, можна реалізувати, ухваливши законопроекти або прийнявши інші політичні рішення. А деякі з них уже частково реалізовані. Наприклад, у переліку є відновлення декларування.

Казати, що Захід примушує нас здійснювати реформи у період війни, – це маніпулювати, бо йдеться не про кардинальні реформи, а про точкові зміни до законодавства, що усунуть лазівки, якими користується влада для тотального контролю за судовою та правоохоронною системами.

Справді, деякі реформи під час війни проводити складно, зважаючи на військові обмеження. Наприклад, як можна говорити про боротьбу з корупцією без повноцінної свободи слова чи можливості вільного доступу до інформації? Викриття корупції тепер стало надзавданням. Також чи можна стратегічно робити реформи, якщо немає політичної конкуренції, обумовленої зрозумілими обмеженнями воєнного часу? У таких умовах перелік, надісланий США, виглядає жорстким, але вибору в нас немає.

Звісно ж, американські партнери, висуваючи ці вимоги, були дипломатичними, а ультимативності цьому листу радше додав наш соціум. Однак важко заперечити, що нереалізація цих вимог зменшуватиме підтримку України. Я переконаний: після завершення цього етапу російсько-української війни вимоги від американців будуть ще більш жорсткими.

Однак жорсткість вимог нівелюється тим, як їхнє виконання зрештою вплине на безпекову ситуацію в Україні. Пункти, яких

вимагають американці, прямо пов'язані з теперішніми і майбутніми інвестиціями в Україну. Розташування іноземних приватних компаній на території України у випадку нових загроз спонукатиме світову спільноту більш активно реагувати. Пенні Пріцкер, спецпредставниця США з питань економічного відновлення України, заявляла, що спілкувалася з американськими бізнесменами і вони готові інвестувати в Україну, але для цього вони мають отримати гарантії, що їхні кошти будуть у безпеці. І йдеться не про російські ракети.

Вони хочуть контролювати свою допомогу Україні. Тому ще на початку 2023 року затвердили спеціальну програму контролю за фінансовою допомогою. У нас вже працювало троє аудиторів зі США, щоправда, вони здійснювали короткі місії. Крім того, Білий дім відправив наглядачку за проведенням реформ (нею стала ексміністерка торгівлі США Пенні Пріцкер), а Пентагон – провідного інспектора для контролю використання американської військової допомоги (Роберта Сторча).

Допомога США українцям стала в Америці предметом політики. Кожен цент, який надходить Україні, скурпульозно обговорюють опозиціонери, вимагаючи в Байдена звітності. Тому, для Білого дому важливо бачити, що їх витрачають за призначенням. Звідси – жорсткі вимоги до реформ.

Та логіка США полягає не лише у внутрішній політиці, а і у стратегічній перспективі. Будь-який успіх України в світі, зокрема в реформах, стане успіхом США. Як і будь-яка невдача. Білий дім не хоче, щоб Україною йому дорікали так, як Афганістаном. Тому такі вимоги виправдані.

Перелік кроків, які має реалізувати українська влада, заступник радника Білого дому з національної безпеки з питань міжнародної економіки Майк Пайл відправив на адресу Координаційної платформи донорів, прем'єр-міністру України Денису Шмигалю та в Офіс президента України.

Сарибаєва Ганна Миколаївна
доктор юридичних наук, доцент,
Національний університет «Одеська юридична академія»,
м. Одеса, Україна
ORCID: 0000-0003-4492-956X

МИТНА БЕЗПЕКА В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ: ТЕРМІНОЛОГІЧНИЙ ДИСКУРС

Питання національної безпеки для Української держави стоять на сьогоднішній день як ніколи гостро. Екзистенціальні загрози, з якими стикається Україна, змушують дивитися на національну безпеку більш пильно, враховуючи всі складові та напрямки.

Закон України «Про національну безпеку України» визначає наступні напрямки національної безпеки, на які спрямовується державна політика у сферах національної безпеки і оборони: воєнна, зовнішньополітична, державна, економічна, інформаційна, екологічна, безпека критичної інфраструктури, кібербезпека України та на інші (ЗУ «Про національну безпеку України»). Очевидно, що у військовий час основні зусилля зосереджені на воєнній та зовнішньополітичній складових. Разом із тим, інші напрямки, можливо і виглядають як другорядні, однак заслуговують на увагу як такі, що створюють передумови та забезпечують життєдіяльність держави в такі непрості часи.

Митним кодексом (далі – МК) України, який є чинним з 2012 року, запроваджено поняття митної безпеки. Під ним розуміється стан захищеності митних інтересів України. У свою чергу митними інтересами є національні інтереси України, забезпечення та реалізація яких досягається шляхом здійснення митної справи. Митна справа у всьому розмаїтті проявів спрямована на реалізацію державної митної політики. А митна політика, серед іншого, є діяльністю держави у сфері захисту митних інтересів та забезпечення митної безпеки України (МК України).

Схематично співвідношення перелічених понять можна зобразити наступним чином (див. Рис. 1):

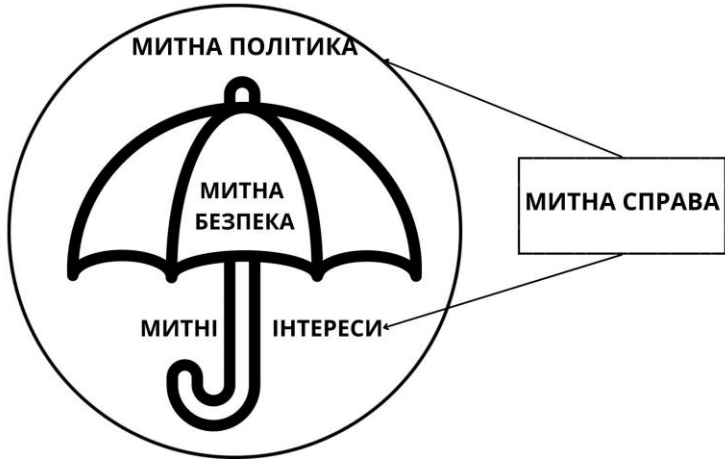


Рис. 1. Співвідношення понять «митна безпека», «митні інтереси», «митна справа» та «митна політика»

Джерело: створено автором.

Судячи зі співвідношення цих понять, забезпечення митної безпеки досягається в кінцевому рахунку через здійснення митної справи. А вона, як відомо зі статті 543 МК України, безпосередньо реалізується митними органами – Державною митною службою України та митницями. Відповідно до статті 5 МК України державна митна політика є складовою частиною державної економічної політики. Очевидно, що і митна безпека та митні інтереси поглинаються поняттями «економічна безпека» та «економічні інтереси» відповідно.

В літературі існує думка про те, що, серед митних інтересів найважливішими є: створення умов сприяння міжнародній торгівлі; недопущення контрабанди та порушення митних правил; удосконалення митного законодавства України відповідно до світових та європейських стандартів; прискорення та спрощення митних процедур; недопущення ввезення

небезпечних для здоров'я людей товарів (Брачук, 2017, С. 159). Крім того, митні правовідносини охоплюють не тільки економічну сферу, а й зовнішньополітичну, внутрішньополітичну, науково-технологічну, екологічну, інформаційну, соціальну, гуманітарну, а також сфери державної безпеки та безпеки державного кордону (Калініченко, 2015, С. 15). З контексту не зрозуміло, що саме автор вкладає в поняття «митні правовідносини», адже на цю тему є чимало точок зору, однак у будь-якому разі очевидно, що сфера виникнення митних правовідносин тією чи іншою мірою перебільшена. Разом із тим перебільшено і сферу митних інтересів та митної безпеки.

Митні інтереси забезпечуються митними органами, про що йдеться у частині 1 статті 544 МК України. Зокрема, призначенням митних органів є створення сприятливих умов для розвитку зовнішньоекономічної діяльності, забезпечення безпеки суспільства, захист митних інтересів України (МК України, 2012). Тобто, виходячи з процитованої статті, і створення сприятливих умов для розвитку зовнішньоекономічної діяльності, і забезпечення безпеки суспільства відокремлені законодавцем від митних інтересів.

Що ж тоді є митними інтересами? Очевидно, за логікою законодавця, все те, що охоплюється поняттям «митна справа» – митний контроль, митне оформлення, справляння митних платежів, протидія митним правопорушенням тощо. Кожен з названих різновидів діяльності митних органів не є самоціллю, вони спрямовані на досягнення більш глобальних цілей, які в сутності зводяться до забезпечення наповнення Державного бюджету, недопущення переміщення через митний кордон України заборонених до такого переміщення товарів, або товарів, які можуть нашкодити людям, тваринам, рослинам, екології та суспільству в цілому. Ці більш глобальні цілі цілком відповідають загальноновизнаним сферам національних інтересів – економічним, екологічним, соціальним тощо. А митні органи є складовою інституційного механізму захисту цих інтересів. Наприклад, у випадку вчинення адміністративного правопорушення у митній сфері, навряд чи хтось стверджуватиме, що правопорушник посягнув на порядок здійснення митного

контролю чи митного оформлення, зазначивши завідомо неправдиві відомості у митній декларації. Очевидно, що його мета уникнути сплати або мінімізувати суму податків, тим самим завдавши шкоди економічним інтересам країни.

На підставі зазначеного дозволимо собі висновок про штучність понять «митна безпека» та «митні інтереси», які повністю охоплюються іншими загальновизнаними сферами національної безпеки та інтересів. Мета виокремлення цих понять на рівні кодифікованого акту не дуже зрозуміла. Навряд чи узагальнене визначення без деталізації його в конкретних повноваженнях, функціях чи задачах державних органів, відповідальних за їх забезпечення, допоможе захисту цих інтересів та забезпеченню безпеки. Поки ж бачимо фрагментацію поняття національна безпека, яка на сьогоднішній день, навпаки, вимагає консолідації зусиль всіх залучених інституцій, уніфікації підходів до реалізації безпекових заходів для подолання сучасних викликів та загроз.

В Європейському Союзі митна безпека – термін, який вживається в контексті реальних та потенційних терористичних загроз, зокрема безпеки транскордонного переміщення товарів (European Commission). Аспекти безпеки були вперше включені в митне законодавство ЄС після терористичних атак у вересні 2001 року в Сполучених Штатах (Regulation (EU), 2013). Її актуальність була підкреслена глобальними проблемами безпеки, спричиненими численними терористичними інцидентами. «Резолюція Пунта-Кани», прийнята Комісією з питань політики Всесвітньої Митної Організації в грудні 2015 року, закликає митні органи посилювати заходи безпеки і виступає за тіснішу співпрацю на національному та міжнародному рівнях, а також з іншими органами влади (WCO, 2015).

Іноземний досвід лише підкреслює хибність підходу українського законодавця до розуміння концепту «митна безпека», а так само пов'язаного з ним поняття «митні інтереси».

Література

Брачук, А. О. (2017). Особливості забезпечення митної безпеки та митних інтересів в умовах спрощення митних процедур. *Lexportus*, 1(3), 156-167.

Митний кодекс України 2012 (Верховна Рада України). *Офіційний сайт Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/4495-17#n416>

European Commission. Customs security. URL: https://taxation-customs.ec.europa.eu/customs-4/customs-security/customs-security_en

Калініченко, А. І. (2015) Митна безпека як складова національної безпеки України. *Право та інновації*, 2 (10), 14-18.

Закон про національну безпеку України 2018 (Верховна Рада України). *Офіційний сайт Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#n106>

Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code. *OJ L 269 10.10.2013, 1*.

Resolution of the Policy Commission of the World Customs Organization on The Role of Customs in the Security Context (2017). *World Customs Organisation*. URL: <https://www.wcoomd.org/-/media/wco/public/global/pdf/about-us/legal-instruments/resolutions/resolution-of-the-wco-policy-commission-on-the-role-of-customs-in-the-security-context.pdf?la=en>

Абакіна-Пілявська Людмила Миколаївна
кандидат юридичних наук,
Національний університет «Одеська юридична академія»,
м. Одеса, Україна

ДО ПИТАННЯ ДИНАМІКИ КРИМІНАЛЬНОГО ЗАКОНУ В УМОВАХ ВОЄННОГО СТАНУ

Повномасштабна агресія проти нашої держави викликала зміни в усіх сферах суспільного життя без виключень. Така активна трансформація вимагала відповідної реакції в частині правової охорони держави, національних інтересів, прав та свобод громадян, в тому числі за допомогою заходів кримінально-правового впливу. Перед кримінальним правом постала задача забезпечення належного правового реагування на ті суспільні відносини та кримінально-протиправні практики, які виникли внаслідок війни.

В першу чергу, мова йде про новелізацію кримінального закону. Так, КК України 2001 року було доповнено десятки разів з початку повномасштабного вторгнення.

15 березня 2022 року кримінальний закон був доповнений нормою щодо встановлення нової обставини для звільнення від кримінальної відповідальності – виконання обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України (ст. 43-1 КК України), чим було виключено кримінальну відповідальність цивільних осіб за застосування вогнепальної зброї проти осіб, які здійснюють збройну агресію проти України, в основі чого закладено необхідність кримінально-правового стимулювання соціальної активності громадян щодо заподіяння шкоди ворогові.

28 липня 2022 року було запроваджено новий вид звільнення від відбування покарання у зв'язку з прийняттям уповноваженим органом рішення про передачу засудженого для обміну як військовополоненого (ст. 84-1 КК України).

Особливо важливо, що Кримінальний кодекс України за час дії воєнного стану отримав закріплення нових кримінально-караних діянь, таких як:

- колабораційна діяльність (ст. 111-1 КК України);
- пособництво державі-агресору (ст. 111-2 КК України);
- несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану (ст. 114-2 КК України);

- незаконне використання з метою отримання прибутку гуманітарної допомоги, благодійних пожертв або безоплатної допомоги (ст. 201-1 КК України);

- образа честі і гідності військовослужбовця, погроза військовослужбовцю (ст. 435-1 КК України);

- виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників (ст. 436-2 КК України). Та при цьому варто відмітити, що окремі із закріплених норм викликали дуже багато питань на практиці при їх застосуванні та призвели до ряду типових ситуацій в частині складнощів розмежування і їх колізійності, що вимагає відповідного унормування та подальшої розробки.

Окремо варто відмітити кроки законодавця в частині посилення відповідальності за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК).

Окрім того, чинний КК України за час дії воєнного стану зазнав чималих змін в частині кваліфікації «загальнокримінальних» правопорушень, які мають місце під час дії воєнного стану та в силу цього вимагають більш суворої реакції держави на їх вчинення в такій обстановці. В контексті чого потрібно виділити визнання воєнного та надзвичайного стану обставинами, що впливають на кваліфікацію (ч. 2 ст. 111, ч. 2 ст. 113, ст. 114-2, частини четверті статей 185–187, 189, 191, ч. 3 ст. 201-2, ч. 5 КК України).

В першу чергу, в фокусі знаходилися кримінальні правопорушення проти власності, що, серед іншого, було обґрунтовано збільшенням кількості випадків посягання на чуже майно, в тому числі непоодинокими були випадки резонансних викрадень, що вимагало відповідних рішень з боку держави. Тому вже 3 березня 2022 року частини четверті статей 185 КК України (крадіжка), 186 КК України (грабіж), 187 КК України (розбій), 189 КК України (вимагання), 191 КК України (привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем) були доповнені кваліфікуючою ознакою вчинення цих кримінальних правопорушень «в умовах воєнного або надзвичайного стану». Оскільки відтоді було встановлено формулювання саме як вчинення «в умовах воєнного стану», то всі кримінально карані посягання із зазначених, вчиненні в період дії воєнного стану, автоматично відносяться до особливо кваліфікованих складів з відповідним рівнем покарання незалежно від розміру завданої шкоди. Більше того, таке посилення караності зазначених посягань потягло за собою обтяження й інших кримінально-правових наслідків, таких як неможливість звільнення від кримінальної відповідальності на підставі ст. ст. 45–48 КК України, подовження передбачених ст. 49 КК України строків давності притягнення до кримінальної відповідальності, подовження строків погашення судимості, а також змінило окремі кримінально-процесуальні аспекти (збільшення розміру застави, полегшення підстав для тримання під вартою тощо).

Отже, кримінальний закон від 24 лютого 2022 року зазнав чимало змін в частині кримінально-правової охорони суспільних відносин внаслідок повномасштабного нападу та дії воєнного стану, що було викликано трансформацією низки правовідносин як у сфері національної безпеки, так і захисту інших сфер суспільних відносин, прав та інтересів громадян. Звісно, окремі новели викликають багато питань, як в частині юридично-змістовного характеру, так і практичного застосування, що вимагає відповідних подальших розробок та внесення необхідних змін з метою уникнення виниклих колізій та різночитання кримінально-правових норм, встановлення уніфікованого підходу реалізації кримінально-правових приписів та уникнення помилок правозастосування.

Гученко Катерина Володимирівна

Київський університет інтелектуальної власності та права

Національного університету «Одеська юридична академія»

ORCID: 0009-0000-4395-1277

ЗНАЧЕННЯ ОСОБЛИВОСТІ СТРУКТУРИ ОСОБИСТОСТІ СУБ'ЄКТА ЗЛОЧИНУ ДЕЗЕРТИРСТВО ДЛЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

У першу чергу, коли ми говоримо про національну безпеку як захист суверенітету країни, її громадян, території та інтересів від зовнішніх загроз і внутрішніх викликів, які можуть поставити під загрозу її добробут і виживання, ми мусимо зазначити, що вона охоплює широке коло проблем і включає в себе різні виміри безпеки (Про національну безпеку). До них ми можемо віднести: по-перше, військова безпека; по-друге, економічна безпека; по-третє, політична безпека; по-четверте, кібербезпека; по-п'яте, екологічна безпека; по-шосте, енергетична безпека; по-сьоме соціальна безпека.

Звичайно, що із врахуванням умов транзиції, особливо на сучасному етапі соціально-економічному розвитку України, цей перелік може бути ще більш охоплююче доповненим. Слід також зазначити нормативно-правові акти, такі як: Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»; Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»; Закон України «Про національну безпеку України».

Нами планується зупинитися на деяких аспектних моментах, що стосуються саме військової безпеки. Варто зазначити, що це – традиційний аспект національної безпеки, що зосереджується на захисті нації від зовнішніх військових загроз. Вона передбачає наявність сильних збройних сил, ефективних оборонних стратегій та спроможності стримувати агресію або реагувати на збройні конфлікти.

Відповідно до ст. 408 КК України дезертирство – це самовільне залишення військової частини або місця служби з метою ухилитися від військової служби, а також нез'явлення з тією самою метою на службу у разі призначення, переведення, з відрядження, відпустки або з лікувального закладу (Кримінальний кодекс України). Відповідно до ст. 401 КК України військовими кримінальними правопорушеннями визнаються передбачені цим розділом кримінальні правопорушення проти встановленого законодавством порядку несення або проходження військової служби, вчинені військовослужбовцями, а також військовозобов'язаними та резервістами під час проходження зборів (Кримінальний кодекс України). Тобто, зважаючи на це та на легальне визначення поняття злочину дезертирство, можемо вважати, що дезертир – це військовослужбовець, який самовільно залишив військову частину або місце служби з метою ухилитися від військової служби, а також нез'явлення з тією самою метою на службу у разі призначення, переведення, з відрядження, відпустки або з лікувального закладу, тобто без належного дозволу командира (начальника) та/або без виконання покладених на нього обов'язків.

Військовослужбовці-дезертири можуть мати різні характеристики, а причини їхнього дезертирства можуть бути найрізноманітнішими. Ось деякі загальні характеристики суб'єкта злочину дезертирство:

По-перше, військовослужбовець-дезертир, як правило, перебуває у самоволці і не з'являється на службу у визначений час і в визначеному місці; по-друге, вони відмовляються виконувати накази або поставлені завдання, що може порушити субординацію і згуртованість підрозділу; по-третє, вони залишають свою військову частину або базу без офіційного дозволу, що є порушенням військових статутів; по-четверте, такі військовослужбовці часто демонструють втрату мотивації до військової служби. Це може бути пов'язано з особистими проблемами, незадоволеністю своєю роллю або підрозділом чи іншими факторами.

Також не слід забувати, що особисті проблеми, такі як сімейні проблеми, фінансові труднощі, проблеми у стосунках або

емоційний дистрес, можуть вплинути на рішення солдата дезертирувати. Деякі дезертири можуть мати проблеми з психічним здоров'ям, такі як тривога, депресія або посттравматичний стресовий розлад (ПТСР), що може вплинути на їхнє рішення дезертирувати. Солдати-дезертири можуть не мати відданості своїй військовій службі або, можливо, пішли на військову службу без справжнього бажання служити.

У деяких випадках до дезертирства може призвести тиск з боку товаришів по службі або інший вплив у військовому середовищі. Вони можуть відчувати себе відірваними від свого підрозділу або через брак товариських стосунків, або через відчуття ізоляції. Страх перед відправкою в зону бойових дій або перед небезпечними ситуаціями може спонукати деяких солдатів до дезертирства. Дезертирів може спокусити привабливість цивільного життя, вільного від військової дисципліни та обмежень. Деяким солдатам може бути важко адаптуватися до суворой військової культури і способу життя, що призводить до дезертирства.

Важливо розуміти, що не всі солдати, які йдуть у самоволку або дезертирують, мають однакові характеристики або мотиви. Деякі з них можуть мати законні особисті проблеми або занепокоєння, які заслуговують на розуміння і підтримку, в той час як інші можуть навмисно ухилятися від виконання своїх обов'язків. Наслідки дезертирства можуть бути значними, включаючи дисциплінарні стягнення і правові наслідки (кримінально-караними). Військове керівництво в особі ДБР, як правило, працює над пошуком і затриманням дезертирів, щоб забезпечити підтримання дисципліни в лавах.

Структура особистості суб'єкта, який вчиняє злочин дезертирство, може мати значні наслідки для національної безпеки (Кавунська, Корнієнко, Шкута, С. 57). Розуміння характеристик і мотивацій осіб, які дезертирують з військової служби, є важливим з кількох причин, і це може вплинути на національну безпеку наступним чином. Перша позиція – оперативний вплив. Коли солдат дезертирує, це може зірвати військові операції, оскільки підрозділи можуть бути недоукомплектовані або невідготовлені до виконання своїх

завдань. Це може послабити боєготовність та ефективність військових. Дезертирство може створювати вразливі місця у військових частинах, особливо під час активних конфліктів або розгортання. Зниклий солдат може наразити своїх товаришів на більший ризик.

Друга позиція – ерозія дисципліни. Дезертирство одного або кількох солдатів може підірвати дисципліну і моральний дух у підрозділі (Гученко, 2023). Сприйняття того, що солдати можуть дезертирувати за власним бажанням, може підірвати військову згуртованість. Дії дезертирів можуть поставити під сумнів авторитет військового керівництва, впливаючи на його здатність підтримувати порядок і боєготовність у лавах.

Третя позиція – ризики для безпеки. Дезертир може володіти секретною інформацією про військові операції, обладнання або тактику. Якщо вони потраплять в чужі руки, ця інформація може бути використана противником (Chandler, 2017, С 367). У деяких випадках дезертири можуть становити внутрішню загрозу, співпрацюючи з противником або займаючись шпигунством.

Четверта позиція – розподіл ресурсів. Зусилля з пошуку і затримання дезертирів можуть відволікати ресурси і особовий склад від інших пріоритетів національної безпеки. Дезертирство може призвести до додаткових фінансових витрат, пов'язаних з розслідуваннями, судовими процесами і можливим ув'язненням.

П'ята позиція – психологічні фактори. Розуміння структури особистості дезертирів може допомогти військовим і правоохоронним органам виявити вразливі місця в їхніх лавах і вирішити такі проблеми, як психічне здоров'я, емоційні розлади або моральні проблеми. Визнаючи загальні фактори, що сприяють дезертирству, влада може впроваджувати превентивні заходи і надавати підтримку солдатам, які стикаються з особистими проблемами.

Шоста позиція – правові та політичні рамки. На правову систему і політику щодо дезертирства впливають обставини і мотивація дезертирів. Розмежування між тими, хто дезертирує з законних причин, і тими, хто робить це навмисно, має важливе значення для судового розгляду. Розуміння структури

особистості дезертирів може допомогти в розробці програм реінтеграції, які допоможуть їм повернутися до військової служби або цивільного життя після повернення.

І остання позиція – психологічна війна. Супротивник може спробувати використати дезертирів, використовуючи їх для пропаганди, поширення дезінформації або психологічної війни.

Таким чином, концепція національної безпеки є динамічною і розвивається у відповідь на мінливі глобальні та внутрішні фактори. Стратегії національної безпеки розробляються з урахуванням конкретних обставин країни і можуть включати в себе комбінацію вищезазначених компонентів. Ефективна політика національної безпеки спрямована на захист інтересів нації, відстоюючи її цінності та принципи, і часто вимагає тонкого балансу між військовими та невійськовими заходами.

Розуміння структури особистості осіб, які вчиняють дезертирство, має вирішальне значення для розробки політики, втручань і заходів безпеки, спрямованих на зменшення ризиків, пов'язаних з дезертирством. Це дозволяє владі усунути першопричини дезертирства, надати підтримку солдатам, які відчують труднощі, а також підтримувати цілісність і боєготовність збройних сил, що має важливе значення для національної безпеки.

Література:

Chandler, J. (2017). To become again our brethren': desertion and community during the American Revolutionary War, 1775–83. *Historical Research*, 90(248), 363–380. Doi: <https://doi.org/10.1111/1468-2281.12183>. DOI: <https://doi.org/10.1111/1468-2281.12183>

Гученко, К. В. (2023). Компаративістський аналіз кримінальної відповідальності за вчинення дезертирства в Україні та в світі. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*, 10. URL: <https://doi.org/10.54929/2786-5746-2023-10-01-02>

Кавунська, А., Корнієнко, М., Шкута, О. (2023). *Дезертирство в Україні: кримінально-правовий та кримінологічний аспект*. Одеса: Юридика. URL: <https://dspace.oduvs.edu.ua/server/api/core/bitstreams/709dee25-1201-4e68-ab35-9a1a07514d1e/content>

*Кримінальний кодекс України 2001 (Верховна Рада України).
Офіційний сайт Верховної Ради України.*

URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>

*Закон про національну безпеку України 2018 (Верховна Рада
України). Офіційний сайт Верховної Ради України.*

URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>

Бобось Олександр Леонідович
кандидат ветеринарних наук
ORCID: 0009-0004-1827-5640

ВПЛИВ ГЛОБАЛЬНИХ КРИЗ НА ЗАХИСТ ПРАВ СПОЖИВАЧІВ ТА МОЖЛИВОСТІ ПУБЛІЧНОГО УПРАВЛІННЯ В УКРАЇНІ

Глобальні кризи, такі як військовий стан, економічні труднощі чи екологічні проблеми, не лише порушують сталість суспільного розвитку, але й викликають суттєві зміни у сфері публічного управління щодо захисту прав споживачів. В Україні це набуває особливої актуальності, оскільки країна стикається з рядом викликів, які вимагають дієвих стратегій управління у сфері захисту прав громадян (Щерба, 2020).

Варто розглянути думку вченого О. Бурлака, що важливі аспекти впливу глобальних криз на можливості публічного управління у сфері захисту прав споживачів є:

– *ефективність захисту*: можуть порушити ринкові відносини та підвищити ризики для споживачів, такі як обмеження доступу до товарів та послуг, підвищення цін, чи навіть неналежна якість продукції. Публічне управління повинно вживати заходів для посилення контролю за ринками, впровадження ефективних стандартів безпеки та якості, а також забезпечення доступності інформації для споживачів;

– *адаптація правового середовища*: вимагати швидких змін у законодавстві для захисту прав споживачів. Публічне управління повинно активно реагувати на зміну обставин, шляхом внесення або модифікації нормативно-правових актів, які гарантують адекватний захист прав громадян;

– *зміцнення механізмів контролю та відповідальності*: важливо забезпечити ефективний контроль за виконанням законів та стандартів. Публічне управління повинно підсилити механізми нагляду, вживати заходів щодо виявлення та покарання порушень, а також забезпечувати високий рівень відповідальності для бізнес-структур;

– залучення громадськості та стейкхолдерів: варто залучати громадськість та представників бізнесу до процесів прийняття рішень. Публічне управління має стимулювати взаємодію між всіма сторонами для спільного вирішення проблем та розробки стратегій виходу з кризи;

– забезпечення інформаційної прозорості: доцільно забезпечувати громадськість та споживачів актуальною та достовірною інформацією. Публічне управління повинно активно бути з громадськістю, надавати чітку інформацію про ситуацію та заходи, які приймаються для захисту прав споживачів (Бурлак, 2022).

Отже, всі ці аспекти вимагають від системи державного управління гнучкості, інноваційної та активної співпраці з усіма зацікавленими сторонами для забезпечення ефективного захисту прав споживачів та їх адаптивності до змін.

Таким чином, уряд має вживати комплексні заходи для забезпечення ефективного захисту прав споживачів в умовах невизначеності та змін. Це включає в себе посилення контролю за ринками та впровадження стандартів безпеки, адаптацію правового середовища для швидкого реагування на кризові ситуації, зміцнення механізмів контролю та відповідальності, а також активне залучення громадськості та стейкхолдерів до прийняття рішень. Складовою також є забезпечення інформаційної прозорості для зміцнення довіри громадськості до управлінських рішень та заходів, спрямованих на захист прав споживачів.

Література

Бурлак, О. С. (2022). Захист прав споживачів в умовах воєнного стану в Україні. *Актуальні проблеми вітчизняної юриспруденції*, 3. URL: http://apnl.dnu.in.ua/3_2022/5.pdf

Чальцева, О. М., Швець, К. А. (2022). Сучасні фактори впливу на глобальну публічну політику. *Політичні інститути та процеси*, 3. URL: <https://jpl.donnu.edu.ua/article/view/12633>

Щерба, О. І. (2020). Споживча поведінка за умов глобалізації. *Теорія та історія соціології*, 3. URL: http://habitus.od.ua/journals/2020/13_2020/part_1/4.pdf

Ніколаєв Кирило Дмитрович
кандидат сільськогосподарських наук, доцент,
Міжрегіональна Академія управління персоналом,
м. Київ, Україна
ORCID: 0000-0003-0404-6113

ЕКОЛОГІЧНІ ВИМІРИ ГІБРИДНОЇ ВІЙНИ: ВПЛИВ СУЧАСНИХ ЗАГРОЗ НА НАЦІОНАЛЬНУ ТА РЕГІОНАЛЬНУ БЕЗПЕКУ

Сьогодні сучасні конфлікти визначаються не лише військовими діями, але й широким спектром інструментів впливу, включаючи: інформаційну війну, економічний тиск та екологічні загрози. Так, багатоаспектне поняття “гібридна війна” вимагає комплексного розуміння.

Екологічні аспекти визнаються не лише як компонент природо збереження, але і як стратегічний інструмент у формуванні впливу та забезпеченні національної безпеки.

Варто підтримати думку вченого О. Мотайла, який розглядає більш детально екологічні виміри гібридної війни: вплив сучасних загроз на національну та регіональну безпеку:

– *екологічні загрози як інструмент впливу*: використання екологічних аспектів може стати ефективним знаряддям впливу в сфері публічного управління. Наприклад, створення екологічних криз, таких як забруднення водних ресурсів чи руйнування природних екосистем, може ставити тиск на уряд та вимагати реагування;

– *екологічна безпека як складова національної безпеки*: розгляд екологічних питань в контексті гібридної війни вказує на необхідність визнання екологічної безпеки як важливого елементу національної безпеки. Заходи з охорони довкілля стають важливою складовою стратегій управління кризовими ситуаціями;

– *інформаційна війна навколо екологічних питань*: інформаційні кампанії щодо екології можуть впливати

на громадську думку та ставлення до урядових заходів. Зміцнення інформаційної свідомості може бути ключовим для підтримки громадянами екологічних ініціатив;

– *сталість екологічного управління*: урядам слід розвивати сталий підхід до управління навколишнім середовищем, забезпечуючи не лише економічну, а й екологічну стабільність. Це може включати в себе прийняття чітких екологічних стандартів та сприяння ініціативам з відновлення екосистем (Мотайло, 2020).

Варто зазначити, що екологічні аспекти у гібридній війні виступають як потужний знаряддя впливу в сфері публічного управління. Створення екологічних криз, визнання екологічної безпеки як складової національної безпеки, інформаційна війна та сталий підхід до екологічного управління визначають стратегічні напрямки. Ці аспекти свідчать про необхідність інтеграції екологічних аспектів у стратегії управління кризовими ситуаціями та важливість забезпечення сталого розвитку для економічної та екологічної стійкості країни (Альван, 2019).

Таким чином, використання екологічних загроз стає стратегічним знаряддям тиску на уряд та мобілізації громадської підтримки. Підвищення рівня екологічної безпеки визначає необхідність інтеграції екологічних аспектів у стратегії управління кризовими ситуаціями, враховуючи їх важливість для національної безпеки. Інформаційна війна в екологічній сфері впливає на громадську думку та урядові рішення, підкреслюючи ключову роль інформаційної свідомості. Забезпечення сталого екологічного управління стає стратегічним кроком для стійкості екосистем та забезпечення економічної та екологічної стабільності країни. Все це вказує на необхідність комплексного підходу до екологічних питань у рамках гібридної війни для забезпечення безпеки та сталого розвитку.

Література

Альван, А. (2019). Проблеми розвитку системи національної безпеки України. *Державне управління*, 3. URL: <https://periodica.nadpsu.edu.ua/index.php/governance/article/view/288/289>

Мотайло, О. В. (2020). Ризики та загрози національній безпеці. *Державне управління*, 31. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2020/5_2020/23.pdf

Оцінки загроз глобального характеру розвідувальних органів іноземних держав, можливість їхнього використання для планування в сфері національної безпеки України (2023). URL: <https://censs.org/otsinky-zahroz-hlobalnoho-kharakteru-rozviduvalnykh-orhaniv-inozemnykh-derzhav/>

Мерзлюк Людмила Володимирівна
*Національний авіаційний університет,
м. Київ, Україна*

ПУБЛІЧНО-ГРОМАДСЬКЕ ПАРТНЕРСТВО ТА МІЖНАРОДНА СПІВПРАЦЯ В УПРАВЛІННІ РЕГІОНАЛЬНОЮ БЕЗПЕКОЮ В УМОВАХ СУЧАСНИХ ЗАГРОЗ

Публічно-громадське партнерство та міжнародна співпраця стали ключовими факторами в управлінні регіональною безпекою в умовах сучасних загроз. Країна стикається з різноманітними викликами, починаючи від тероризму та кіберзагрози до глобальних пандемій. Стає очевидним, що ефективне управління безпекою тепер виходить за межі внутрішніх меж країн.

Варто відмітити думку вченої А. Крутової (Крутова, 2019, С. 158-171), що публічно-громадське партнерство відіграє важливу роль у взаємодії між урядовими та неприбутковими секторами, громадськістю та бізнесом. Відкрите обговорення, обмін інформацією та спільні ініціативи стають основою для створення реалізованих стратегій безпеки.

Слід зазначити, що міжнародна співпраця є необхідністю, адже багатонаціональні виклики вимагають глобальних відповідей. Спільні зусилля країн, об'єднаних в різних форматах, від регіональних союзів до міжнародних організацій, стають ефективним механізмом протистояння загрозам.

Крім цього, управління регіональною безпекою в умовах сучасних загроз вимагає від нас інноваційних стратегій, гнучкості та взаємодії. Публічно-громадське партнерство та міжнародна співпраця стають країною досягнення спільної мети – забезпечення безпеки та стабільності в регіоні та за його межами.

Слід відмітити думку М. Шавлака, що цілеспрямована співпраця між урядами, громадським сектором та міжнародними

партнерами є важливою для розробки та впровадження стратегій, спрямованих на запобігання та вирішення сучасних загроз. Забезпечення відкритості та прозорості у взаємодії стає гарантією успішного управління безпекою, а також відновленням довіри громадськості до інститутів (Шавлак, 2022).

Крім цього, спільне розуміння загроз, обмін аналітичною інформацією та координація дій на різних рівнях – це основа ефективного управління ризиками. Партнерство розширює можливості виявлення та вирішення проблем, що виникають в різних сферах, від економічної безпеки до кіберзахисту та вирішення конфліктів.

Доречно зауважити, що міжнародна співпраця не тільки сприяє обміну кращими практиками, але й забезпечує об'єднання зусиль у вирішенні глобальних проблем. Це особливо актуально в умовах взаємозалежності та швидкого поширення загроз, де ізольовані підходи вже неефективні (Захаріна, Симоненко, Сайкевич).

Отже, публічно-громадське партнерство та міжнародна співпраця стають каталізаторами для створення стійких та адаптивних систем управління регіональною безпекою, спроможних ефективно протидіяти викликам сучасності.

Таким чином, управління регіональною безпекою в умовах сучасних загроз вимагає глибокої взаємодії та співпраці між різними секторами суспільства та міжнародними партнерами. Публічно-громадське партнерство стає кількісно та якісно новим підходом, сприяючи обміну ідеями, ресурсами та експертними знаннями. Міжнародна співпраця є ключовою у формуванні відповідального та гнучкого підходу до регіональної безпеки. Об'єднані зусилля країн та організацій на міжнародному рівні стають необхідною передумовою для вирішення глобальних викликів, що стоять перед сучасним світом. Отримані через партнерство та співпрацю результати стають важливою основою для створення ефективних стратегій, які не лише адаптуються до сучасних реалій, але й передбачають майбутні виклики. Такий підхід створює стійкі та динамічні системи управління безпекою, спроможні реагувати на невизначеність та забезпечувати стабільність в регіоні та світі.

Література

Захаріна, О. В., Симоненко, Л. І., Сайкевич, М. І. Публічно-приватне партнерство, як механізм розвитку інфраструктури регіону. *Державне управління: удосконалення та розвиток*. URL: <http://www.dy.nauka.com.ua/?op=1&z=1193>

Крутова, А. С. (2019). Проекти державно-приватного партнерства: реалізація та аналіз ефективності. *Економічний простір*, 141, 158-171.

Шавлак, М. А. (2022). Вектори удосконалення процедури прийняття рішення про здійснення державно-приватного партнерства в умовах війни. *Публічне управління та митне адміністрування*, 3. URL: <http://customs-admin.umsf.in.ua/archive/2022/3/9.pdf>

Шевченко Роман Петрович
*Національний авіаційний університет,
м. Київ, Україна*

ЗАГРОЗИ ГЛОБАЛЬНОЇ ТА РЕГІОНАЛЬНОЇ БЕЗПЕКИ ТА ЇХ ВПЛИВ НА ВЕТЕРАНІВ ВІЙНИ І ЧЛЕНІВ ЇХ РОДИНИ

В світі, де геополітична ситуація постійно змінюється, загрози глобальної та регіональної безпеки стають суттєвим фактором, який впливає на різні соціальні групи, зокрема на ветеранів війни та члени їх родин. Ці загрози можуть приймати різні форми, включаючи військові конфлікти, терористичні акти, економічні нестабільності та політичні напруження.

Варто зазначити думку вченої К. Спицької, що загрози глобальної та регіональної безпеки становлять серйозне викликання для ветеранів війни та їх родин. Серед ключових загроз варто відзначити такі аспекти:

- *воєнні конфлікти*: постійні або нові війни можуть створювати нестабільність та загострювати умови для ветеранів, які вже пройшли через військові дії;
- *тероризм*: терористичні атаки можуть викликати психологічний стрес та безпекові загрози, особливо для тих, хто вже мав досвід воєнних дій;
- *економічна нестабільність*: глобальні або регіональні економічні кризи можуть призводити до втрати робочих місць та фінансових труднощів для ветеранів та їхніх родин;
- *політична напруженість*: напружені відносини між країнами можуть погіршити безпекові умови, впливаючи на життя тих, хто пройшов через військовий конфлікт;
- *екологічні кризи*: природні катастрофи та зміни клімату можуть призвести до гуманітарних криз та додаткових труднощів для ветеранів та їхніх родин (Спицька, 2022).

Отже, урахування всіх цих аспектів вимагає ретельної уваги та розробки ефективних стратегій для забезпечення безпеки

та підтримки ветеранів в умовах непередбачуваного та швидко змінюю чого світу.

Крім цього, необхідно розробляти програми безпеки, спрямовані на запобігання можливим конфліктам та забезпечення захисту ветеранів від нових загроз. Це може включати в себе участь у міжнародних миротворчих місіях та підтримку дипломатичних ініціатив.

Варто наголосити, що розвиток програм психологічної та соціальної підтримки для ветеранів і членів їх родин. Це включає в себе надання доступних сервісів психотерапії, консультування та інших ресурсів для подолання емоційного стресу (Аналіз системи соціального захисту, 2022).

Отож, реінтеграція ветеранів у суспільство вимагає розвитку програм навчання та професійної реабілітації. Забезпечення їм нових навичок та можливостей для власного розвитку допоможе їм успішно інтегруватися в цивільне життя.

Отже, важливо залучати громадянське суспільство, включаючи неприбуткові організації та волонтерів, у підтримку ветеранів. Широкий соціальний і психологічний фонд може стати опорою для тих, хто повертається з військової служби, допомагаючи їм відновити своє місце у суспільстві (Аналіз системи соціального захисту, 2022).

Таким чином, загрози глобальної та регіональної безпеки ставлять перед ветеранами війни та їх родинами серйозні виклики. Вирішення цих проблем вимагає комплексних стратегій, орієнтованих на безпеку, психологічну підтримку та успішну реінтеграцію ветеранів у суспільство. Розробка програм безпеки, психосоціальної допомоги, професійної реабілітації та активна участь громадянського суспільства є важливими кроками для створення стійкого та підтримуючого середовища для тих, хто віддав своє служіння на благо миру та стабільності.

Література

Аналіз системи соціального захисту ветеранів та військовослужбовців (2022). URL : <https://legal100.org.ua/wp-content/uploads/2022/08/2022-Bila-kniga.pdf>

Спицька, К. (2022). Правові засади соціального захисту учасників бойових дій в Україні. *Юридичний вісник*, 2. URL: http://yurvisnyk.in.ua/v2_2022/22.pdf

Конопля Арсен Ігорович
ORCID: 0000-0002-6823-3471

Лисиця Віталіна Вячеславівна
кандидат педагогічних наук,
Глухівський національний педагогічний університет імені О. Довженка,
м. Глухів, Україна
ORCID: 0000-0003-2228-2013

ЦИФРОВА ГІГІЕНА ЯК ЗАСІБ ФОРМУВАННЯ НАВИЧОК БЕЗПЕЧНОЇ РОБОТИ В МЕРЕЖІ ІНТЕРНЕТ У ДІТЕЙ ДОШКІЛЬНОГО ВІКУ

Заклади дошкільної освіти повинні забезпечити право дітей дошкільного віку на здобуття освіти, але пріоритетним є те, що освітній процес має організовуватися в безпечному інформаційному середовищі. В зонах бойових дій навчання дітей дошкільного віку здійснюється за допомогою дистанційних платформ навчання, а тому проблема цифрової гігієни є надзвичайно актуальною та нагальною.

Передусім, звернемося до законодавчої бази: на початку квітня 2022 року МОН надало ряд методичних рекомендацій для працівників закладів дошкільної освіти на період дії воєнного стану в Україні щодо організації дистанційного навчання у ЗДО. Так, у Методичних рекомендаціях щодо здійснення освітньої діяльності з питань дошкільної освіти на період дії правового режиму воєнного стану зазначається: «Базовий компонент дошкільної освіти, як стандарт дошкільної освіти, є актуальним у будь-який час. Він утворює політику держави у галузі дошкільної освіти. Заклади дошкільної освіти мають відповідати його вимогам і під час дії воєнного стану. Задля забезпечення ефективності комунікації з батьками, вихователями й усіма, хто задіяний в освітньому процесі, рекомендовано обрати оптимальні для здійснення кожного конкретного завдання канали комунікації. Основними формами онлайн-комунікацій є: відеоконференція, форум, чат, блог, електронна пошта,

анкетування, соціальні мережі. У складних умовах корисними можуть бути сервіси та інструменти комунікації в онлайн-режимі. Ефективними можуть бути розміщені на сайті ЗДО завдання і рекомендації для батьків щодо роботи з дітьми, відповідно до їхнього віку; створення груп із батьками, вихователями, психологами в соціальних мережах Viber, Telegram, WhatsApp тощо для отримання інформаційно-освітніх та психолого-педагогічних послуг; використання електронних платформ Zoom, GoogleMeet, Google Classroom, Microsoft Teams та ін.» (Лист, 2022).

У статті 9 Закону України «Про освіту» зазначено, що однією з форм здобуття освіти є дистанційна. Вона визначається, як «індивідуалізований процес здобуття освіти, який відбувається в основному за опосередкованої взаємодії віддалених один від одного учасників освітнього процесу у спеціалізованому середовищі, що функціонує на базі сучасних психолого-педагогічних та інформаційно-комунікаційних технологій» (Закон про освіту, 2017).

З метою розуміння проблеми цифрової гігієни дітей старшого дошкільного віку звернемося до ключової дефініції поняття: «цифрова гігієна».

Цифрова гігієна – це грамотне споживання інформації, а також дотримання базових правил кібербезпеки: не використовувати один і той самий пароль на всіх акаунтах, застосовувати двофакторну ідентифікацію, регулярно здійснювати резервне копіювання та оновлення застосунків (Цифрова гігієна, 2020). Визначення, яке б стосувалося конкретно дітей дошкільного віку: «цифрова гігієна безпечної роботи в мережі Інтернет дітей старшого дошкільного віку», на жаль, не знаходимо.

Натомість в мережі Інтернет існує безліч практичних рекомендацій, порад для дитячої безпеки в Інтернеті; важливими є Рекомендації для педагогічних працівників та батьків щодо безпеки дітей у цифровому просторі, які надані МОН України. Зокрема, у змісті зазначається, що «інформаційно-комунікаційні технології є важливим інструментом у житті дітей під час здобуття освіти, соціалізації, самореалізації. Водночас, безконтрольне та

безвідповідальне їх використання містить ризики для здоров'я, розвитку та благополуччя дітей. До основних ризиків відносять: контактні ризики (сексуальні експлуатації та зловживання, домагання для сексуальних цілей («грумінг», розбещення), онлайн-вербування дітей для вчинення злочинів, участь у екстремістських політичних чи релігійних рухах або для цілей торгівлі людьми); ризики контенту (принизливе та стереотипне зображення та надмірна сексуалізація жінок та дітей; зображення та популяризація насильства та нанесення собі ушкоджень, зокрема, самогубств; принизливі, дискримінаційні або расистські вирази або заклик до такої поведінки; реклама, контент для дорослих); ризики поведінки (залякування, переслідування та інші форми утисків, розповсюдження без отримання згоди сексуальних зображень, шантаж, висловлювання ненависті, хакерство, азартні ігри, незаконне завантаження або інші порушення прав інтелектуальної власності, комерційна експлуатація); ризики для здоров'я (надмірне використання призводить до позбавлення сну та фізичної шкода). Всі перераховані вище ризики не є вичерпними, постійно оновлюються та здатні негативно вплинути на фізичне, емоційне та психологічне благополуччя дитини» (Безпека дітей, 2021). Отже, з огляду на ризики, роль цифрової гігієни в формуванні безпечних та етичних звичок в мережі Інтернет у дітей старшого дошкільного віку є надважливою.

Оскільки мова йде про дітей дошкільного віку, то під час дистанційного навчання має обов'язково забезпечуватися регулярна взаємодія педагога з батьками дітей.

Батькам під час комунікації з дитиною варто, зокрема: говорити з дитиною про безпеку в Інтернеті та сприяти розвитку в неї критичного мислення, вчити робити аргументований вибір та нести відповідальність за його результати; будувати відкриті та довірливі стосунки з дитиною; формувати корисні звички використання гаджетів та цифрового середовища та підвищувати самооцінку дитини, дозволяти дитині самостійно робити вибір і бути відповідальною за це; заохочувати користуватися гаджетами в зонах видимості дорослих; встановлювати часові межі користування гаджетами

та контролювати додатки, ігри, веб-ресурси та соціальні мережі, якими користується дитина, та їх відповідність віку дитини; бути уважними до проявів страху чи тривоги, зміни поведінки, режиму сну та апетиту (Безпека дітей, 2021).

Отже, роль педагогів з метою формування цифрової гігієни як засобу формування навичок безпечної роботи в мережі Інтернет у дітей дошкільного віку полягає у систематичній тісній взаємодії педагога з батьками дітей: наданні рекомендацій, здійсненні фахової підтримки та організації спільно з батьками безпечного діджиталізованого освітнього простору для дітей дошкільного віку в умовах війни.

Література

Безпека дітей у цифровому просторі – МОН надає рекомендації для педагогічних працівників та батьків (2021). URL: <https://www.vin.gov.ua/news/ostanni-novyny/34665-bezpeka-ditei-u-tsyfrovomu-prostori-mon-nadaie-rekomendatsii-dlia-pedahohichnykh-pratsivnykiv-ta-batkiv>

Лист про рекомендації для працівників закладів дошкільної освіти на період дії воєнного стану в Україні 2022 (Міністерство освіти і науки України). URL: <http://surl.li/bsdns>

Закон про освіту ст. 9, 2017 (Верховна Рада України). URL: https://kodeksy.com.ua/pro_osvitu/statja-9.htm

Цифрова гігієна: яких правил варто дотримуватися в інтернеті? (2020). URL: <http://surl.li/mnbwd>

Гуральський Назар Романович
*Поліський національний університет,
м. Житомир, Україна
Житомирська державна нотаріальна контора
Житомирської області*

ПРОПОЗИЦІЇ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ

Однією з найбільших мовних проблем українського ЗМІ є використання російської мови в засобах масової інформації. Це стало особливо актуальним під час конфлікту на сході України та анексії Криму, коли російська пропаганда зміцнила свою позицію в українському інформаційному просторі.

Крім того, існує проблема недостатньої розвиненості української мови в ЗМІ. Багато журналістів використовують невірну граматику, використовують російські слова та вислови, що негативно впливає на якість та рівень інформації, яку отримують глядачі та читачі.

Для вирішення цих проблем запроваджуються різноманітні заходи, такі як підвищення мовної культури журналістів, створення нових україномовних медіа, фінансування мовних проєктів тощо. Важливо також забезпечити розвиток української мови в школах та університетах, щоб молодь могла вільно володіти мовою та зрозуміти її значення.

Також є наступні пропозиції державного регулювання ресурсами засобів масової інформації:

1. Розробка та впровадження законодавства щодо захисту інтелектуальної власності та авторських прав в медіа-сфері. Це дозволить забезпечити високий рівень якості та достовірності інформації, що розповсюджується, та зменшити кількість фейків та дезінформації.

2. Розвиток та підтримка незалежних медіа-організацій, які не залежать від влади та виконують свої функції на професійному рівні. Для цього можуть бути розроблені різні програми та

ініціативи, які допоможуть фінансово та організаційно підтримати незалежні ЗМІ.

3. Забезпечення безпеки та захисту інформації в інтернеті. Можна впроваджувати програми з кібербезпеки та підвищення кібермедіа-грамотності, що допоможуть зменшити кількість дезінформації та фейків, які поширюються в мережі.

4. Розвиток та підтримка медіа-освіти та медіа-грамотності в школах та вищих навчальних закладах. Це допоможе підвищити рівень свідомості населення про проблеми пропаганди та дезінформації, та допоможе людям зрозуміти, як розпізнати та уникати поширення фейків (Компанець, Григорович, С. 11).

Загалом у нас уже функціонують стратегії інформаційної безпеки та кібербезпеки. Однак в нинішніх реаліях досить важко дотримуватися цієї стратегії. Потрібно укладати міжнародні угоди стосовно сприяння інформаційної безпеки та кібербезпеці. Необхідна допомога країн-партнерів, обмін досвідом тощо (Про Стратегію кібербезпеки України).

Для того, щоб позбутися російської пропаганди на території України потрібен довготривалий та складний процес, який вимагає комплексного підходу та координації зусиль влади, громадських організацій та ЗМІ. Можна навести кілька можливих шляхів розв'язання цієї проблеми:

Розвиток україномовних ЗМІ та медіа-простору. Держава може надавати підтримку україномовним ЗМІ та медіа-проектам, які зосереджені на поширенні об'єктивної та правдивої інформації. Також можна стимулювати розвиток нових цифрових медіа-платформ та онлайн-ресурсів, що дозволяє відстежувати та боротися з пропагандою в режимі реального часу.

Зміцнення законодавства про засоби масової інформації. Держава може змінити законодавство, щоб заборонити поширення пропагандистських та дезінформаційних матеріалів на території України. Такі заходи повинні забезпечувати право громадян на інформацію, але водночас захищати від пропагандистських впливів.

Створення системи моніторингу та аналізу пропагандистських матеріалів. Для ефективного боротьби з пропагандою потрібна система моніторингу та аналізу

інформації, що поширюється в ЗМІ. Це дозволить вчасно виявляти та припиняти поширення пропагандистських матеріалів та інформаційних атак на Україну.

Вбереження ЗМІ від стороннього впливу в Україні є важливою складовою демократичного суспільства. Для цього необхідно встановлювати та розвивати ефективну систему державного регулювання в галузі ЗМІ, яка забезпечуватиме захист прав журналістів, свободу слова та незалежність ЗМІ від стороннього впливу. Державне регулювання повинно забезпечувати збалансований розвиток ЗМІ, в тому числі і в електронному вигляді, розвиток інфраструктури, підтримку професійного розвитку журналістів та сприяння розвитку інноваційних технологій в цій галузі.

Крім того, необхідно створювати умови для розвитку інформаційної грамотності в суспільстві, щоб громадяни могли самостійно оцінювати інформацію, що надходить з різних джерел. Для цього потрібно забезпечувати доступність якісної та об'єктивної інформації, зокрема, за допомогою державних ЗМІ, які повинні працювати в інтересах громадян, а не політичних чи бізнесових структур. Також важливо розвивати медіаграмотність, яка дозволить громадянам не тільки правильно розуміти інформацію, а й діяти відповідно до отриманих знань, наприклад, приймати обґрунтовані рішення під час виборів або при взаємодії з державними органами влади (Бондаренко, Бугрова, Герасименко, 2016, С. 3).

Також необхідно дотримуватися Стратегій, які ще були прийняті 14 травня 2021 року, а саме: Стратегію національної безпеки України, Стратегію кібербезпеки України, Стратегію інформаційної безпеки тощо, вони досить змістовні, чіткі і якщо дотримуватися їх, а також залучати міжнародні організації, країни-партнерів до збагачення інформаційного простору України, тільки тоді ми вийдемо на новий етап розвитку та захисту інформації в цілому, ЗМІ та кібербезпеки.

Проаналізувавши досвід інших країн, для України є доцільним позбутися корупції в медіасфері, зробити незалежними ЗМІ та максимально забезпечити захист від російської пропаганди, але для цього необхідне терпіння, бажання та час.

Література

Компанець, О., Григорович, А. *Державне регулювання ЗМІ в Україні: проблеми та шляхи вирішення*. URL: https://www.academia.edu/48851812/ДЕРЖАВНЕ_РЕГУЛЮВАННЯ_ЗАСОБІВ_МАСОВОЇ_ІНФОРМАЦІЇ_В_УКРАЇНІ_ПРОБЛЕМИ_ТА_ШЛЯХИ_ВИРІШЕННЯ

Бондаренко, В., Бугрова, О., Герасименко, О. *Державне регулювання ЗМІ: проблеми та перспективи*. URL: http://nbuv.gov.ua/UJRN/nptu_2016_3_12

Указ про Стратегію кібербезпеки України 2021 (Президент України). *Офіційний сайт Президента України*. URL: <https://www.president.gov.ua/documents/4472021-40013>

Ліщук Аліна Олександрівна
*Донецький національний університет імені Василя Стуса,
м. Вінниця, Україна*

ПУБЛІЧНЕ УПРАВЛІННЯ НАВЧАЛЬНИМИ ЗАКЛАДАМИ НА РЕГІОНАЛЬНОМУ РІВНІ

Однією з найважливіших сфер публічного управління в країні є освіта. Якість освіти є ключовим фактором, що визначає розвиток суспільства, конкурентоспроможність нації та якість життя громадян. Освіта є важливою складовою суспільства, і якість освіти визначає економічний, соціокультурний та інтелектуальний розвиток країни. Публічне управління в освіті впливає на якість навчання, доступність освіти та готовність суспільства до викликів сучасного світу.

Україна проводить політику децентралізації, передаючи більше повноважень регіонам. Оскільки освіта в Україні є виключно важливим сектором, дослідження публічного управління на регіональному рівні стає актуальним для розуміння наслідків децентралізації в освіті.

Публічне управління навчальними закладами на регіональному рівні є важливою складовою системи освіти і відіграє ключову роль у забезпеченні доступу до якісної освіти та підвищенні її якості. Воно передбачає координацію, планування, фінансове управління, моніторинг і оцінку результатів роботи навчальних закладів. Освітні системи різних регіонів можуть відрізнятися за структурою, ресурсами, демографічними характеристиками та іншими факторами. Тому важливо розробляти та реалізувати стратегії управління, які враховують конкретний контекст кожного регіону.

Публічне управління в освітній сфері повинно бути орієнтоване на результат та спрямоване на задоволення потреб суспільства, громадян та розвиток освітньої системи. Це вимагає ефективного використання ресурсів, вдосконалення

управлінських процесів та підтримку інновацій у навчальних закладах.

Управління навчальними закладами на регіональному рівні в Україні може стикатися з різними викликами і труднощами, такими як фінансові обмеження, потреби різних груп населення, нестабільність законодавчого середовища. Для ефективного управління необхідно розробляти стратегії, які враховують ці виклики та забезпечують стале покращення якості освіти.

Міністерство освіти і науки України відіграє ключову роль у формуванні освітньої політики та контролі за її виконанням. Однак, ефективність його діяльності може покращити шляхом більшої прозорості, співпраці з громадськістю і міжнародними партнерами, а також активного застосування сучасних методів моніторингу та оцінки якості освіти.

Важливим елементом управління якістю освіти є розробка та впровадження освітніх стандартів та критеріїв оцінки якості. Освітні програми повинні бути актуалізовані, враховуючи потреби сучасного суспільства та ринку праці.

Залучення громадськості, батьків, студентів та вчителів у прийняття рішень у галузі освіти сприяє більшій відкритості та відповідальності в системі освіти.

Державне управління якістю освіти в Україні є складною та актуальною проблемою, що знаходиться у центрі уваги влади, науковців, освітян та громадськості. Загальна думка про стан управління якістю освіти може бути схильною до критики, однак, в той же час, відзначається певний прогрес та зусилля, спрямовані на вдосконалення системи.

Низький рівень фінансування освіти, бюрократичність, недостатній контроль та координація між різними органами влади – це одні з основних проблем, які впливають на публічне управління якістю освіти в Україні. Це може призводити до незрозумілих та неефективних рішень, розбалансованості програм, недостатньої уваги до потреб учасників освітнього процесу.

Однак в Україні існують позитивні зміни в сфері державного управління якістю освіти. Зокрема, останні роки характеризуються активізацією реформ та впровадженням

нових підходів до управління освітніми процесами. Заходи, спрямовані на покращення якості освіти, включають розробку та впровадження стандартів, оцінку результатів навчання, залучення громадськості до процесів планування та моніторингу.

Дослідження також підтвердило важливість ролі учасників освітнього процесу, таких як вчителі, студенти, батьки, які активно впливають на якість освіти та виконання стратегічних завдань в цій сфері. Реформи в державному управлінні освітою повинні бути орієнтовані на розвиток людського потенціалу, забезпечення рівних можливостей для всіх громадян та забезпечення сталого соціально-економічного розвитку країни.

Україна визначила амбіційні стратегічні цілі, такі як інтеграція до європейського освітнього простору, підвищення якості освіти та підготовки конкурентоспроможної робочої сили. Для досягнення цих цілей необхідне ефективне управління якістю.

Отже, у світлі отриманих результатів можна висловити припущення, що подальший розвиток публічного управління якістю освіти в Україні є важливим завданням для досягнення сучасних стандартів якості освіти та підвищення конкурентоспроможності країни на міжнародному рівні. Відповідальність за успіх цих зусиль лежить на державних органах, науковцях, освітянах, громадських організаціях та інших зацікавлених сторонах, які повинні спільно працювати над розвитком ефективної системи державного управління освітою в Україні.

Публічне управління навчальними закладами на регіональному рівні є складним і важливим завданням, яке вимагає уважної уваги та постійного вдосконалення.

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ДЕТЕРМІНАНТИ ФОРМУВАННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Милосердна Ірина Михайлівна
кандидат політичних наук, доцент,
Одеський національний університет імені І.І. Мечникова
ORCID: 0000-0003-2083-9500

ОСНОВНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ЯК ЕЛЕМЕНТУ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Національна безпека є багатоплановим явищем, пов'язана з регіональною та міжнародною (глобальною) безпекою і розглядається як одна з глобальних проблем людства. Національна безпека являє собою стан захищеності життєво важливих інтересів особистості, суспільства і держави від внутрішніх і зовнішніх загроз шляхом утримання збройних сил та охорони державних секретів.

Можна говорити, що національна безпека являє собою геополітичний аспект безпеки загалом, який охоплює питання фізичного виживання держави, захисту та збереження її суверенітету і територіальної цілісності. Національна безпека охоплює політичну безпеку, економічну безпеку, військову безпеку, енергетичну та природну безпеку, екологічну безпеку, гуманітарну безпеку, інформаційну та кібербезпеку.

І якщо впродовж більшої частини ХХ століття національна безпека була зосереджена на военній безпеці, то за сучасних умов ми є свідками зростаючої ролі інформаційної сфери, швидких темпів розвитку інформаційно-комунікаційних технологій та впливу Інтернету, соціальних мереж, тож національна безпека держави постає перед новими викликами та загрозами.

Термін «інформаційна безпека» означає захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення з метою забезпечення: цілісності, що означає захист від неправомірної зміни або знищення інформації та включає забезпечення безвідмовності й достовірності інформації; конфіденційності, що означає збереження дозволених обмежень на доступ та розкриття, включно із засобами захисту особистого життя і службової інформації; і доступності, що означає забезпечення доступності та доступності. Також інформаційну безпеку можна визначити, як «захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення з метою забезпечення конфіденційності, цілісності та доступності» (Nieves Michael, Dempsey Kelley, Pillitteri Victoria Yan, 2017).

У рамках Резолюції Генеральної Асамблеї ООН А/RES/53/70 «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки» ідея інформаційної безпеки набуває визнання та «відзначається значний прогрес у розробці й упровадженні новітніх інформаційних технологій та засобів телекомунікації, однак, висловлюючи заклопотаність тим, що ці технології та засоби потенційно можуть бути використані з метою, несумісною із завданнями забезпечення міжнародної стабільності, та можуть негативно впливати на безпеку держав, а також на безпеку суспільства. Таким чином, у Резолюції А/RES/53/70 підкреслюється ідея «запобігання неправомірному використанню або використанню інформаційних ресурсів або технологій у злочинних або терористичних цілях» (Developments in the field of information and telecommunications in the context of international security, 1999).

Нині проблема інформаційної безпеки постала ще гостріше, оскільки значно зросла роль накопичення, оброблення та поширення інформації, зокрема, в ухваленні стратегічних рішень, збільшилася кількість суб'єктів інформаційних відносин і споживачів інформації. Зміни, що відбуваються в інформаційній сфері, з одного боку, зумовлюють перехід до єдиних стандартів,

з іншого – характеризуються зведенням нових бар'єрів, пов'язаних із забезпеченням безпеки особи, суспільства і держави в цілому.

Важливим результатом поширення інформаційних і комунікаційних технологій та проникнення їх в усі сфери суспільного життя є створення правових, організаційних і технологічних умов для розвитку демократії за рахунок реального забезпечення прав громадян на вільний пошук, одержання, передачу, виробництво і поширення інформації.

Виокремимо найбільш суттєві групи інформаційно-технічних небезпек, зумовлених досягненнями науково-технічного прогресу в умовах глобалізації.

Перша група пов'язана з розвитком нової зброї – інформаційної, яка здатна ефективно впливати і на психіку, свідомість людей, і на інформаційно-технічну інфраструктуру суспільства. У даному випадку ми говоримо про зростання пропаганди / дезінформації, які можуть проявлятися у зміні або підтасовуванні даних чи введенні недостовірних даних з метою здійснення впливу на результати політичних процесів, дестабілізації правлячих режимів та ін.

Друга група інформаційно-технічних небезпек для особистості, суспільства і держави – це новий клас соціальних злочинів, що ґрунтуються на використанні сучасних інформаційних технологій (махінації з електронними грошима, комп'ютерне хуліганство та ін.). Питання забезпечення інформаційної безпеки як однієї з важливих складових національної безпеки держави особливо гостро постає в контексті появи транснаціональної транскордонної комп'ютерної злочинності та кібертероризму.

Тут під загрозою опиняється конфіденційність, оскільки кібератаки можуть бути націлені на різні джерела конфіденційної інформації та здебільшого здійснюються зі злочинною метою: шпигунство, розкрадання персональних даних, «крадіжка особистості», шахрайство.

Зміцнення інформаційної безпеки визначається Законом України «Про національну безпеку України» від 21.06.2018 р., та Указом Президента України Про рішення Ради національної

безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Так в Законі України «Про національну безпеку України» зазначається, що «державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями» (Закон України «Про національну безпеку України», 2018).

Можна погодитися із О. В. Олійником, що «головна мета державної політики інформаційної безпеки має полягати у захисті: конституційних прав і свобод людини і громадянина, забезпеченні єдності їх прав і обов'язків; духовних, морально-етичних, культурних, історичних, інтелектуальних та матеріальних цінностей суспільства, його інформаційного і природного середовища; конституційного ладу, суверенітету, територіальної цілісності, інформаційної безпеки в політичній, економічній, соціокультурній, науковотехнологічній, оборонній і державної безпеки, екологічній, власне інформаційній тощо складових національної безпеки» (Олійник, 2016, С.75).

Таким чином, формування, впровадження інформаційної безпеки виступає важливою складовою національної безпеки держави, яка забезпечує стійкий розвиток стану захищеності інформаційної інфраструктури, прав і свобод людини і громадянина, демократичних процедур в державі.

Література

Закон про національну безпеку України 2018 (Верховна Рада України). *Офіційний сайт Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>

Олійник, О. В. (2016). Принципи забезпечення інформаційної безпеки України. *Юридичний вісник*, 4(41), 72-78.

Указ про Стратегію кібербезпеки України 2021 (Президент України). *Офіційний сайт Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#n12>

Developments in the field of information and telecommunications in the context of international security: Resolution by the General Assembly A/RES/53/70 4 December 1998.

URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement>

Nieles M., Dempsey, K., Pillitteri, Victoria Yan An Introduction to Information Security. NIST Special Publication 800-12 Revision 1. doi: <https://doi.org/10.6028/NIST.SP.800-12r1>

Варнавська Інна В'ячеславівна
кандидат педагогічних наук, доцент,
Херсонський державний аграрно-економічний університет
ORCID: 0000-0002-3061-0665

ЕМОЦІЙНЕ ВИГОРЯННЯ ЯК ПСИХОЛОГІЧНИЙ ФЕНОМЕН

Згідно з сучасними даними, під психічним вигорянням розуміється стан фізичного, емоційного і розумового виснаження, виявляється у професіях соціальної, інформаційної сферах, що є більш об'єктивними. Під емоційним виснаженням більшість фахівців уявляють почуття емоційної спустошеності і втоми, викликане роботою. Особливо, виникаючі негативні установки можуть спочатку мати потайливий характер і з'являтися у внутрішньо стримуваному роздратуванні, яке згодом «виривається» назовні і призводить до конфліктів. Редукція професійних досягнень виникає в результаті почуття некомпетентності в професійній сфері, усвідомлення власної неспіху в ній. На зараз не існує єдиної точки зору щодо сутності психічного вигоряння і його структури, адже вони вважаються наслідком недостатньої поінформованості фахівців.

Емоційне вигоряння – один із нових механізмів захисту, тому його визначення є дещо розмитим. Синдром «емоційного вигоряння» можна розглядати як полісистемний детермінований симптомокомплекс, пов'язаний з низкою змін у поведінці, певними стратегіями і захисними механізмами, спотворенням процесу самоактуалізації і розвитку особистості. Психологічна природа емоційного вигоряння почала вивчатися порівняно нещодавно. Термінологічно і змістовно, виявлено багато значень цього поняття. Емоційне вигоряння розглядається як складне багатоаспектне явище, саме це і викликає аспектність наповнення його категоріального визначення.

У зв'язку з цим синдром емоційного вигоряння позначається поняттям «професійне вигоряння», що дозволяє розглядати цей

феномен в аспекті професійної деформації під впливом робочих стресів. Професійне вигоряння – це окремий випадок емоційного вигоряння, синдром, який розвивається внаслідок виснаження особистісних ресурсів людини на фоні постійного стресу і втоми.

Професійне вигоряння – це нормальна реакція психіки на постійний рівень емоційного «зашумлення». Деякі дослідники дотримуються точки зору, що професійне вигоряння є психологічною реакцією адаптації до умов роботи. Насамперед цьому явищу віддані представники тих професій, чия діяльність пов'язана зі спілкуванням з людьми, емпатією і високою відповідальністю. Так, доречно виділити три основні складові професійного вигоряння:

- емоційне виснаження (внаслідок високої навантаження і конфліктів на роботі);
- відсторонене, цинічне ставлення до людей (виникає як захисна реакція психіки на емоційне виснаження), іноді переходить в дегуманізацію;
- зниження своїх професійних досягнень, синдром самозванця.

Причиною емоційного вигоряння є невдоволення напрямом діяльності. Отже, підсвідомо людина не спрямована на те, щоб не відповідально ставитися до виконувannya обов'язків. Можна зробити дуже простий висновок: емоційне вигоряння є причиною, а професійне вигоряння – наслідком.

Професійне вигоряння кожний переживає по-своєму. Але при будь-якому розладі організм завжди посиляє сигнали, які повинні підказати людині: «щось пішло не так». У випадку із професійним вигорянням такі ознаки також існують. Все починається з відчуття перевантаження і розчарування результатами своєї роботи. Щоб людина не робила, їй здається, що цього недостатньо. У результаті чого – розчарування посилюється, з'являється гнів, почуття виснаження і безпорадності. Якщо цей стан вчасно не зупинити, емоційні розлади можуть переважати в цілком реальні хвороби. На ці розлади також можуть вказувати симптоми, які спочатку буває навіть складно пов'язати з роботою. Але при такому порушенні у багатьох виникають проблеми зі сном, головний біль, розлад,

хронічна втома, апатія, підвищується артеріальний тиск, знижується імунітет. Схожі симптоми можуть з'являтися і на тлі звичайного перевтоми. Але якщо це так, то співробітникам вистачить тижневої відпустки, щоб повернутися в норму. А в деяких випадках буває досить просто достатньо відіспатися або відпочити на вихідних.

Емоційне вигорання є формою професійної деформації особистості. Цей стереотип емоційного сприйняття дійсності складається під впливом низки факторів: зовнішніх і внутрішніх. До зовнішніх відносять: хронічну напруженість психоемоційної діяльності, дестабілізуючу організацію діяльності, підвищену відповідальність за виконуючі функції та операції, несприятливу атмосферу професійної діяльності, психологічно «важкий» контингент, з яким має справу професіонал у сфері. До внутрішніх факторів відносять: схильність до емоційної ригідності, інтенсивну інтеріоризацію – сприйняття і переживання обставин професійної діяльності, слабку мотивацію віддачі в професійній діяльності.

Щодо причин виникнення й основних симптомів емоційного вигорання в існує багато різних думок, але всі вчені погоджуються з тим, що основним джерелом вигорання є взаємодія з людьми, не напружені відносини в системі «людина – людина». Емоційне вигорання може перерости в професійне вигорання – глобальний деструктивний феномен, який поширюється на всю професійну діяльність особистості, що є неприпустимим для роботи фахівця. Тому збереження психологічного здоров'я кваліфікований працівників є надзвичайно актуальним завданням на сучасному етапі розвитку суспільства.

Основною причиною виникнення вигорання вважають психологічну і душевну перевтому, а також при синдромі емоційного вигорання спостерігається розлад особистості, її професійної ролі. Або вигорання як професійна криза, яка пов'язана не тільки з професійною діяльністю в цілому. Тому варто розглядати емоційне вигорання як складний багатовимірний конструкт, що виникає в результаті негативних психічних переживань, виснаження від тривалого впливу напруги у представників професій, діяльність яких пов'язана

з міжособистісним спілкуванням, який супроводжується емоційною складовою.

Отже, емоційне вигоряння – це синдром, який розвивається під впливом хронічного стресу і постійних навантажень і призводить до виснаження емоційно енергетичних та особистісних ресурсів людини.

Література

Шаумян, О. Г. (2019). Дослідження особистості сучасного менеджера у сфері інформаційної безпеки. *European Humanities Studies: State and Society*, 2, 84-199.

Бондаренко Степан Юрійович
Національна академія Служби Безпеки України,
м. Київ, Україна
ORCID: 0000-0001-8328-5117

Вітомський Юрій Леонідович
Київський університет інтелектуальної власності та права
Національного університету «Одеська юридична академія»,
м. Київ, Україна

ПСИХОЛОГІЧНІ ЧИННИКИ ФОРМУВАННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

Психологічні чинники відіграють значну роль у формуванні національної безпеки держави. Національна безпека виходить за рамки військового потенціалу і поширюється на психологічне благополуччя та стійкість населення країни. Нами виділяються деякі ключові психологічні фактори, які сприяють формуванню національної безпеки.

У першу чергу – національна ідентичність та єдність. Сильне почуття національної ідентичності та єдності може посилити безпеку держави. Коли громадяни ідентифікують себе зі своєю нацією, вони більш схильні підтримувати національні інститути, цінності та інтереси. Ця єдність сприяє солідарності під час кризи (LaMothe, 2012, P. 39).

Не варто забувати і про психологічну стійкість населення, яка дозволяє йому адаптуватися до різних загроз і викликів та відновлюватися після них. Стійкі люди та громади краще підготовлені до подолання катастроф, економічних потрясінь та інших кризових ситуацій. Впевненість і довіра до уряду, сил безпеки та громадських інституцій мають вирішальне значення для національної безпеки. Населення, яке вірить в ефективність і чесність своїх інститутів, більш схильне до співпраці під час кризи.

Психологічна готовність має важливе значення для реагування на кризи, будь то стихійні лиха, пандемії чи загрози безпеці. Добре поінформоване і психологічно підготовлене населення може вжити відповідних заходів під час надзвичайних ситуацій. Ефективне інформування про ризики має вирішальне значення для інформування громадськості про потенційні загрози та заходи, що вживаються для їх пом'якшення. Розуміння того, як люди сприймають ризики і реагують на них, має важливе значення для стратегій національної безпеки.

Держави і супротивники можуть вдаватися до психологічної війни і пропаганди, щоб впливати на громадську думку, поширювати дезінформацію і створювати страх або невпевненість. Розпізнавання цих тактик і протидія їм є важливими для національної безпеки (Wolfers, 1952, P. 501).

Усунення психологічних чинників, що призводять до екстремізму та радикалізації, є критично важливим аспектом національної безпеки. Програми запобігання, втручання та дерадикалізації спрямовані на протидію привабливості екстремістських ідеологій (Goldgeier, 1997, С. 139). Підвищення обізнаності населення з питань кібербезпеки допомагає захиститися від кіберзагроз. Люди, поінформовані про ризики в Інтернеті, з меншою ймовірністю стануть жертвами кібератак або піддадуться маніпуляціям дезінформації в мережі.

Психічне здоров'я відіграє важливу роль у національній безпеці, оскільки особи, які мають проблеми з психічним здоров'ям, можуть становити загрозу для себе та інших. Доступ до послуг і підтримки у сфері психічного здоров'я може посилити загальну безпеку.

Психологічні фактори впливають на те, як нація реагує на кризи і на швидкість відновлення. Ефективне реагування на кризу включає психологічну підтримку постраждалих осіб і громад. Участь громадськості у заходах безпеки, таких як повідомлення про підозрілу діяльність або участь у реагуванні на надзвичайні ситуації, сприяє національній безпеці.

Дотримання прав людини та верховенства права має важливе значення для національної безпеки. Порушення прав людини може викликати невдоволення, незадоволення і нестабільність,

що негативно впливає на безпеку. Освітні та інформаційні кампанії можуть інформувати громадськість про потенційні загрози, заходи безпеки та важливість національної безпеки.

Варто також зазначити, що психологія, у тому числі й юридична, та формування національної безпеки держави нерозривно пов'язані між собою. Сфера психології, яка вивчає людську поведінку, пізнання та емоції, відіграє вирішальну роль у формуванні політики та практики національної безпеки. Психологія допомагає зрозуміти, як окремі особи і суспільства сприймають і реагують на загрози. Когнітивні упередження, емоції та сприйняття ризиків можуть суттєво впливати на оцінку ризиків для безпеки. Планувальники національної безпеки повинні враховувати ці психологічні фактори при оцінці загроз.

Психологічні принципи мають важливе значення у формуванні стратегій реагування на кризові ситуації та стійкості. Психологія визначає, як люди та громади реагують на катастрофи, кризи та надзвичайні ситуації. Ефективна комунікація, сприйняття ризиків і психологічна підтримка мають вирішальне значення для забезпечення стійкості суспільства.

Психологія має фундаментальне значення для розуміння процесів радикалізації та екстремізму (Yu, 2018, P. 112). Вивчаючи психологічні чинники, які спонукають людей до екстремістських ідеологій, уряди можуть розробляти програми протидії радикалізації, спрямовані на ці вразливі місця.

Противники часто використовують психологічні тактики, такі як пропаганда і дезінформація, щоб маніпулювати громадською думкою і створювати страх або розкол. Розуміння психологічного впливу цих тактик має вирішальне значення для розробки стратегій протидії пропаганді та дезінформації.

Психологічне благополуччя населення є життєво важливим для національної безпеки. Психологічні стресори, зокрема економічні труднощі, конфлікти та невизначеність, можуть впливати на психічне здоров'я. Вирішення проблем психічного здоров'я та надання підтримки є необхідними для підтримки стабільності суспільства.

Людська поведінка відіграє центральну роль у кібербезпеці. Психологічні фактори, такі як обізнаність користувачів,

сприйнятливості до соціальної інженерії та дотримання протоколів безпеки, впливають на вразливість нації до кіберзагроз. Психологія може допомогти визначити фактори, які заохочують або перешкоджають участі громадськості в заходах безпеки. Ефективне залучення громадськості та співпраця з органами безпеки мають важливе значення для забезпечення національної безпеки.

На дотримання прав людини та верховенства права впливають психологічні та моральні принципи. Порушення цих принципів може призвести до суспільного невдоволення і нестабільності, що може загрожувати національній безпеці. Психологія відіграє важливу роль у тому, як люди сприймають свій уряд та державні інституції. Довіра, впевненість і легітимність є важливими для забезпечення громадської підтримки заходів національної безпеки.

Розуміння психологічних факторів, які сприяють виникненню різних загроз, таких як тероризм або насильство, є основою для розробки програм профілактики та втручання. Ці програми можуть бути спрямовані на усунення першопричин безпекових ризиків.

Таким чином, психологія відіграє центральну роль у формуванні національної безпеки держави. Розуміння людської поведінки, пізнання, емоцій та соціальної динаміки є життєво важливим для оцінки загроз, формулювання політики, розробки ефективних стратегій, а також забезпечення стійкості та добробуту населення. Взаємозв'язок між психологією та національною безпекою підкреслює важливість міждисциплінарного підходу до безпекових викликів.

Зважаючи на це, національна безпека – це не лише військовий чи оборонний потенціал; вона також включає психологічне благополуччя і стійкість нації. Уряди і служби безпеки повинні враховувати ці психологічні фактори при розробці політики, стратегій і програм, спрямованих на захист безпеки і добробуту свого населення.

Література

Goldgeier, J. M. (1997). Psychology and security. *Security Studies*, 6(4), 137-166.

LaMothe, R. (2012). Obsession for National Security and the Rise of the National Security State-Industry: A Pastoral-Psychological Analysis. *Pastoral Psychology*, 61(1), 31-46.

Wolfers, A. (1952). " National security" as an ambiguous symbol. *Political science quarterly*, 67(4), 481-502.

Yu, Z. O. (2018). Psychological security as the foundation of personal psychological wellbeing (analytical review). *Psychology in Russia: State of the Art*, 11(2), 100-113.

Лихотоп Ілля Володимирович
Національна академія внутрішніх справ,
м. Київ, Україна

СХИЛЬНІСТЬ КУРСАНТІВ ДО НАВІЮВАННЯ

У сучасному світі більшість людей досить легко можуть повірити в те, що їм нав'язують. У фаховій літературі це називають «навіювання» або «сугестія» (від лат. *suggestio* – натяк, навіювання). Навіювання, переконання, наслідування є способами взаємодії людей у процесі спілкування. Навіювання відрізняється від маніпуляції за метою впливу (Захаренко, 2020).

Поняття «навіювання» та «схильність до навіювання» (тобто, навіюваність) слід розрізняти (Саннікова & Кривдик, 2022). Навіювання є процесом, що включає індивідуально-психологічні характеристики суггеренда (того, хто сприймає психологічний вплив) та особливості того, хто здійснює вплив (суггестора – людини, яка впливає на емоції, почуття, а через них і на розум суггеренда; джерела впливу; обставин, за яких здійснюється вплив; зміст і форму подачі інформації). Схильність до навіювання є свідомою або несвідомою формою сприйняття особистістю психічного впливу (або впливів), тобто, навіюваність або «піддатливість» навіюванню.

Сугестивність визначається як властивість особистості, що проявляється в ситуативній піддатливості навіюванню.

Важливим аспектом є суггестабільність адресата впливу, тобто його сприйнятливості до сугестії. Із зростання рівня суб'єктивного контролю особистості знижується рівень її схильності до сугестивності, тобто зростає суггестабільність (Корнієнко & Колодка, 2020).

Тобто, навіювання (процес), схильність до сугестивності (це піддатливість навіюванню), сугестивність – особистісна властивість.

Емпіричне дослідження було проведено серед майбутніх поліцейських, які є курсантами 1 курсу Національної академії

внутрішніх справ (n=30), віком від 18 до 21 року. Опитування проводилось у червні 2023 року. Метою дослідження було вивчення схильності курсантів до навіювання.

Одним із пріоритетів у виборі досліджуваних стала саме обрана ними професія, адже поліцейським треба вміти відстоювати власну позицію, не піддаватись навіюванню сторонніх осіб під час виконання своїх службових обов'язків.

У дослідженні використовувався опитувальник, який передбачав швидкі відповіді респондентів на п'ять завдань-запитань. Разом із запитанням респондентам озвучувався приклад можливої відповіді, для того щоб перевірити чи відтворюють вони запропонований варіант відповіді, чи напишуть свій варіант. Сигналом, що означав початок виконання завдання, було слово «Почали!». Слідом за цим відразу озвучувалось запитання. Респондентам потрібно було зосередитись на сприйнятті голосу дослідника, який зачитував запитання опитувальника.

У першому завданні пропонувалось написати прізвище будь-якого письменника (наприклад: «Шевченко»). Відповідно до отриманих відповідей більшість респондентів вказали прізвища інших письменників, однак декілька написали запропонований варіант.

У наступному завданні звучала вказівка написати будь-яку коротку фразу і наводився приклад («Літо настало»). Згідно з отриманими результатами більшість відповідей респондентів були досить близькими до запропонованого варіанту. Однак частина респондентів написали зовсім інші короткі фрази.

У третьому завданні респондентам потрібно було написати назву будь-якого предмета (наприклад: «Стіл»). При аналізі відповідей респондентів на дане завдання було визначено, що жоден із респондентів не відтворив запропонований варіант, більшість відповідей були абсолютно іншими.

У четвертому завданні респондентам потрібно було зобразити будь-який предмет (наприклад: «трикутник»). Як свідчать отримані результати виконання даного завдання респондентами, менше половини з них зобразили предмети, близькі до запропонованого варіанту (геометричні фігури: коло,

квадрат). Половина респондентів зобразила інші предмети. Декілька респондентів не встигли виконати це завдання.

У останньому завданні респондентам потрібно було написати будь-яке число (наводився приклад: «9»). Згідно з отриманими результатами жоден із респондентів не написав запропоноване число.

Після проведення опитування проводився підрахунок балів, набраних респондентами за кожне завдання: 4 бали – відтворений запропонований варіант відповіді; 3 бали – відповідь, близька за змістом до наведеного прикладу; 2 бали – швидше далека, ніж близька за змістом відповідь; 1 бал – відповідь абсолютно не пов'язана із наведеним прикладом.

Підрахунок загальної суми балів кожного респондента проводився шляхом додавання балів, отриманих ним за кожне завдання.

Статистична обробка даних проводилася за допомогою функцій та формул версії Excel, яка входить у програмний пакет Microsoft Office 2007.

Відповідно до отриманих результатів загальна сума балів, набраних респондентами, сягала від 9 до 15 балів. Обраховано, що середньогруповий бал становить 8,5; стандартне відхилення 2,6.

Встановлено, що середні показники знаходяться у межах від 5,9 балів до 11,1 балів. Показники, що вищі за 11,1 балів, відповідають підвищеному рівню навіюваності, а нижчі за 5,9 балів показники – зниженому рівню навіюваності. Розподіл респондентів у групи відповідно до рівня навіюваності подано у таблиці 1.

Таблиця 1

Рівні навіюваності респондентів

	<i>Підвищений рівень</i>	<i>Помірний рівень</i>	<i>Занижений рівень</i>
К-сть осіб	3	23	4
%	10%	76,7%	13,3%

Відповідно до табличних даних курсантам характерні різні рівні навіюваності.

Більшості респондентів (76,7%) притаманний помірний рівень навіюваності. Вони помірно піддатливі навіюванню. Не схильні до сліпого підкорення, мають свою думку та здатні до критичного аналізу інформації, проявляють активність. Помірна схильність до навіюваності респондентів вказує на їх здатність до співпереживання та емпатії, яка є однією із передумов розуміння емоцій інших людей, у тому числі і тих осіб, хто є об'єктом професійної уваги поліцейського.

Знижений рівень навіюваності характерний незначній кількості респондентів (13,3%). Вони проявляють критичне мислення стосовно людей та інформації, схильні до самоконтролю, характеризуються незалежністю від групи, вимогливі до інформації та до оточуючих. Знижений рівень навіюваності є хорошим показником, адже для майбутнього працівника правоохоронних органів важливо не піддаватись оманливим навіюванням та спробам переконання їх у тому, що вони діють неправильно під час виконання службових обов'язків.

Підвищений рівень навіюваності має кожен десятий респондент (10%). Вони не настільки критично сприймають та аналізують інформацію, приймають рішення, порівняно з іншими респондентами. Можуть проявити більшу сприйнятливність щодо інформації, ніж їх одногрупники, а також емоційність, вразливість, конформізм.

Таким чином, за результатами проведеного дослідження визначено, що курсантам притаманна різна піддатливість навіюванню. Визначення їх суттєвості як особистісної риси потребує проведення подальших досліджень.

Література

Захаренко, Л. М. (2020). Механізм дії маніпулятивного впливу. *Сучасні проблеми забезпечення національної безпеки держави: III Міжнар. наук.-практ. конф.* Київ, 306-308. URL: https://www.researchgate.net/profile/Olena-Gulac/publication/349086017_AKTUALNI_PITANNA_FORMUVANNA_TA_REALIZACII_POLITIKI_U_SFERI_BEZPEKI_ORGANAMI_MISCEVOGO_SAMOVRADEVANNA/links/601ecec54585158939891902/AKTUALNI-PITANNA-FORMUVANNA-TA-

REALIZACII-POLITIKI-U-SFERI-BEZPEKI-ORGANAMI-MISCEVOGO-SAMOVRADEVANNA.pdf#page=306

Корнієнко, В., Колодка, К. (2020). Індивідуально-психологічні особливості навіюваності в умовах інформаційної пропаганди. *Молодий вчений*, 2(78), 80-83. doi : 10.32839/2304-5809/2020-2-78-18

Саннікова, О., Кривдик, В. Г. (2022). Особливості самоставлення суггерендів. *Диференціальний підхід у дослідженні професійного самоздійснення особистості* : Всеукр. наук.-практ. конф. Одеса, 5-14. URL: <http://dspace.pdpu.edu.ua/bitstream/123456789/15937/1/Sannikova%20Olha%20Pavlovna%202022.pdf>

Бутко Олена Миколаївна

*Комунальний заклад «Харківський ліцей №54 Харківської міської ради»,
м. Харків, Україна*

Загоровська Марія Вікторівна

*Комунальний заклад «Харківський ліцей №54 Харківської міської ради»,
м. Харків, Україна*

Савченко Людмила Леонідівна

*кандидат педагогічних наук, доцент,
Комунальний заклад «Харківська гуманітарно-педагогічна академія»
Харківської обласної ради, м. Харків, Україна
ORCID: 0000-0002-6750-2676*

ІНФОРМАЦІЙНА БЕЗПЕКА ПІД ЧАС ВІЙНИ

Інформаційний простір дозволяє бути на зв'язку з рідними, дізнаватись останні новини з фронту, хоч якось контролювати те, що відбувається навколо. Для дітей та підлітків інтернет залишається світом розваг та спілкування з друзями. Але важливо пам'ятати, що за позначкою геолокації на пості чи фотографії, веселим відео в соціальній мережі чи одним повідомленням може ховатися справжня небезпека. Особливо під час війни, коли інфопростір використовують окупанти для військових нападів на українські міста.

Інформація відіграє головну роль у сучасному світі, саме тому американський дослідник М. Маклуен вивів таку тезу: «Істинно тотальна війна – це війна за допомогою інформації» (Горбулін&Качинський, 2004, С.16). Маклуен найпершим ввів поняття «інформаційна війна» у науковий обіг та заявив, що в наш час економічні зв'язки і відносини все більше і більше приймають вигляд обміну знаннями, а не обміну товарами. На сьогодні інформація є не тільки можливістю передачі знань, подій, описати емоції або почуття, це потужна зброя, яка може не лише маніпулювати свідомістю, а й вбивати, адже за допомогою інформації можна зробити певні нації, думки,

ментальність – ворожою, сформувати негативне та вороже ставлення до подій, особистостей, особистих думок тощо. Саме в період військової агресії Російської Федерації у 2022 році та війни з Україною, інформація набуває важливого та смертельного значення. Інформація – це надсильний інструмент та механізм маніпулювання будь-якими подіями, наслідками подій, суспільною думкою, формувати та впливати на певну оцінку подій тощо.

Практичні й теоретичні аспекти вдосконалення кібербезпеки України й, зокрема, питання захисту прав людини в інформаційному просторі були предметом дослідження таких українських науковців, як С. Онищенко, А. Глушко, О. Мережко, Ю. Яковенко, Ю. Заскока, Ю. Деркаченко, С. Кухтик, Д. Березовський, А. Бежевець. Перелічені вчені аналізують поняття «інформаційна безпека», основні загрози інформаційній безпеці, етапи забезпечення інформаційної безпеки, нормативно-правове забезпечення інформаційної безпеки України, визначення механізмів запобігання та протидії інформаційній безпеці та ін.

Інтернет і гаджети – це можливість бути на зв'язку зі своїми рідними та друзями. Діти та підлітки зараз проводять багато часу в інтернеті, зокрема у соцмережах, дивляться улюблених блогерів, спілкуються з однолітками.

Проте, тут на них може чатувати небезпека. Українці думають, що досконало знають методи російської пропаганди. Але «розп'яті хлопчики» залишились у минулому. Нині використовується витонченіша інформаційна зброя. Відшукати болісну тему, сформувати у суспільстві протилежні позиції, знайти людей, які їх поділяють, та підбурювати їх один проти одного.

Для цього у країни-терориста є безліч інструментів: соціальні мережі, іноземні медіа, «хороші рускі», блогери-інсайдери, ПСГО та багато інших. Такі терміни, як «інформаційна війна», «спеціальні психологічні операції», «пропаганда» чули всі. Але далеко не всі розуміють, як самих українців використовують для цих процесів та як наша поведінка ненавмисно стає допоміжним інструментом для ворога.

Діти потребують зараз особливої турботи та уваги. Через невеликий життєвий досвід і особливості дитячої психіки їм загрожує більше небезпек – фізичних та психоемоційних – ніж дорослим. Водночас існують інструменти, які дозволяють мінімізувати ризики та вберегти фізичне та психічне здоров'я дитини.

Інформаційна безпека відіграє ключову роль саме в періоди ведення військових дій та конфліктів. Адже неправильно, неправдиво подана інформація може спричинити панічні настрої у населення, впливати на хід подій, сприяти внутрішньому переміщенню населення, погіршенню іміджу політичного керівництва, породжувати недовіру до політиків, їх заяв, звернень, що може негативно впливати на ведення бойових дій, сприяє порушенню психічного та фізичного здоров'я населення, а також може нанести непоправної шкоди для всього результату військових дій. Тому запобігання розповсюдженню такої викривленої інформації в період військових конфліктів має важливе значення для всього перебігу військового конфлікту.

Можна виділити такі актуальні правила поведінки в інформаційному просторі:

- Профіль дитини в соціальних мережах варто зробити закритим: щоб писати дитині, переглядати вміст її сторінки могли лише ті, кого дитина додасть у друзі.
- Якщо хтось із користувачів у мережі просить приватну інформацію (особистий номер телефону чи номер батьків, де батьки працюють, де родина зараз перебуває, яка ситуація в місті, де розміщується військова техніка в місті чи військові об'єкти) – таку інформацію в жодному разі не можна передавати. Навіть якщо це онлайн-друг, якого дитина знає в реальному житті. Адже зараз дуже часто особисті профілі зламують для отримання інформації або створюють фейкові профілі.
- Не можна знімати розміщення та пересування військової техніки та військових у місті, де перебуває дитина. Оскільки окупанти можуть переглядати відкриті профілі українців для визначення місця розташування військових для подальшого нападу. А також злочинці можуть намагатися вести листування

з дитиною для шантажу чи примушування до отримання інформації про розміщення техніки в місті.

- Не знімати місця вибухів та потрапляння снарядів, оскільки окупанти можуть використовувати фото- та відеодані, які потрапили в мережу, для коригування подальшого нанесення вогню по місту.

- Не переходити за невідомими посиланнями, які були надіслані в приватні повідомлення в будь-якій соціальній мережі чи месенджері. Адже за ними можуть ховатися хакерські атаки.

- Якщо ви переглядаєте та обговорюєте новини з дитиною, варто переконатися в їхній правдивості. Усі новини, заяви високопосадовців та обмеження в містах краще повторно перевірити в офіційних каналах комунікації, на офіційних сайтах державних установ, в офіційних Telegram-каналах посадовців.

- Якщо дитину автоматично додали до невідомих груп, важливо відписатися від них та заблокувати їх. А також розповісти про це дорослим.

- Якщо до дитини хтось пише з проханням допомоги або виконати спеціальне завдання, важливо, щоб дитина повідомила про це дорослим. Варто разом зробити скріншот групи, повідомлень та через онлайн-форму звернутися до кіберполіції – <https://ticket.cyberpolice.gov.ua/>.

Основними механізмами протидії неправдивої, викривленої, неперевіреної інформації в умовах військових конфліктів та бойових дій є: формування медіаграмотності населення; постійне висвітлення об'єктивної інформації через урядові інтернет-видання, ЗМІ, спілкування з громадянами; встановлення відповідальності за фейки та розповсюдження їх серед населення; контроль фейкових акаунтів, які пересилають свідомо неправдиву, викривлену інформацію; формування спеціальних підрозділів у кіберполіції, які займатимуть виявленням фейків, дипфейків та їх нейтралізацією.

Кіберфахівці СБУ системно відслідковують інформаційне поле, фіксують фейки і вживають заходи, аби оперативно нейтралізувати шкідливу діяльність проросійських пропагандистів, ботоферм та притягнути зловмисників до відповідальності.

Отже, з першого дня повномасштабного вторгнення агресора в Україну ми відчули на собі вплив ІІСО та інших інструментів інформаційної війни. На сьогодні потік інформації настільки потужний, що дорослим людям часом буває дуже складно орієнтуватися в новинах, а про дітей – годі й казати. На жаль, пересічний українець не має навички відрізнити правду від фейку. Особливо це відчувається в східних регіонах, де левову частку інформаційних каналів займають російські медіаресурси. Як наслідок, багато людей втратило орієнтири та розуміння, що буде далі, оскільки пропаганда все глибше вкорінилась у свідомості багатьох. Саме тому надзвичайно важливо всім навчитися відповідально і свідомо споживати інформацію так, щоб не наразити себе та інших на небезпеку, не стати жертвою обману, відділити корисну інформацію від непотрібної чи шкідливої. Завдання агресора – посіяти паніку, наше – зберігати спокій та не піддаватися на будь-які провокації.

Література

Горбулін, В. П., Качинський, А. Б. (2004). Методологічні засади розробки стратегії національної безпеки. *Стратегічна панорама*, 3, 15-24.

Перспективні технології. URL: https://uk.wikipedia.org/wiki/Перспективні_технології.

Закон про національну безпеку України 2018 (Верховна Рада України). Офіційний сайт Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.

Закон про основні засади забезпечення кібербезпеки України 2017 (Верховна Рада України). Офіційний сайт Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

Куля Ірина Федорівна

Придунайська філія МАУП, м. Ізмаїл, Україна

ORCID: 0000-0002-8363-1478

Беженар Карина Дмитрівна

Придунайська філія МАУП, м. Ізмаїл, Україна

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА

В сучасному світі все частіше постає проблема збільшення інформаційної безпеки підприємств, яка залежить саме від ступеня захищеності інформаційної сфери. Збереження стабільності функціонування та економічного росту, розвиток науково-технічних інновацій залежать від правильної організації інформаційної захищеності підприємств.

Глобальний розвиток інформаційних технологій, модернізована обробка інформації спостерігаються зі зростанням науково-технічного прогресу. Разом з цим і підвищується роль інформаційної безпеки підприємств.

При веденні діяльності кожен підприємець в обов'язковому порядку зіштовхується з необхідністю отримання, зберігання, обробки, перетворення, поширення, передачі та видалення непотрібної або зайвої інформації. Інформація, яка несе користь для підприємства має бути захищеною від зловмисників. При захисті інформації слід перекрити всі канали можливого витоку та забезпечити безпеку зберігання інформації на усіх носіях, що мають на підприємстві.

Згідно законодавства України інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації (Про основні засади розвитку інформаційного суспільства).

Потреба в володінні інформацією призводить до оволодіння інформацією про навколишнє середовище та процеси, що протікають в ньому, тобто інформованості індивіда, соціуму та держави.

Стан та ступінь інформованості впливає на майбутні дії, а також на обґрунтування рішень, які прийматимуться підприємцями.

Загрози інформаційній безпеці – це сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам підприємств чи підприємців в інформаційній сфері.

Фактори загроз інформаційній безпеці можна класифікувати за видами та ієрархією (рис.1).



Рис. 1. Класифікація факторів загроз інформаційній безпеці

В залежності від виду загроз, інформаційну безпеку можна розглядати як забезпечення стану захищеності (Герасименко, Козак, 2015):

- особистості, суспільства та держави від впливу недостовірної інформації;
- підприємств, організації та інших установ;
- інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;
- інформаційних прав і свобод громадянина.

Належний рівень інформаційної безпеки забезпечується сукупністю економічних, організаційних, політичних заходів, спрямованих на попередження, виявлення і нейтралізацію таких обставин, дій і факторів, які можуть завдати шкоди і збитків або перешкодити реалізації інформаційних прав, потреб та інтересів підприємств (Про основні засади розвитку інформаційного суспільства).

Основним і головним завданням заходів з інформаційної безпеки є мінімізація шкоди за неповноти, несвоєчасності або недостовірності інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації.

Забезпечення інформаційної безпеки має бути спрямоване саме на запобігання ризиків, а не на ліквідацію їх наслідків. Тому прийняття запобіжних заходів для забезпечення цілісності, конфіденційності, а також доступності інформації і є найбільш правильним підходом у створенні системи інформаційної безпеки. Будь-який витік інформації може призвести до серйозних проблем для підприємства – від значних фінансових збитків до повного припинення існування підприємства (Северина, 2016).

Одним з головних елементів системи інформаційної безпеки підприємств виступають принципи, які мають закладатися в основу її побудови. Основними принципами інформаційної безпеки підприємств є: простота, повний контроль, загальна заборона, відкрита архітектура, розмежування доступу, мінімальні привілеї, стійкість, мінімізація дублювання (рис. 2).

Принцип простоти наголошує на тому, що простота в використанні інформаційної системи здатна забезпечити мінімізацію помилок.

Повний контроль полягає в передбаченні підприємством безперервного контролю за станом інформаційної безпеки та моніторингу всіх подій, що впливають на інформаційну безпеку.

Загальна заборона полягає в забороні доступу до інформаційної системи підприємства, без наданого на це дозволу.

Принцип відкритої архітектури полягає в тому, що безпека має забезпечуватися через неясність. Спроби захистити інформаційну систему від комп'ютерних загроз шляхом заплутування, ускладнення, приховування слабких місць і сторін.

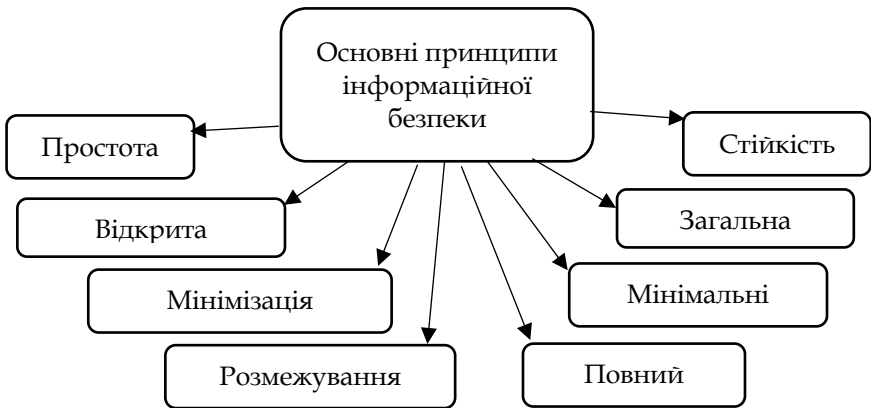


Рис. 2. Основні принципи інформаційної безпеки

Принцип розмежування доступу полягає в тому, що кожному користувачеві надається доступ до інформації, а також її носіїв у відповідності до його повноважень.

Принцип мінімальних привілеїв полягає у виділенні користувачам найменших прав і мінімального доступу до інформаційної системи.

Принцип стійкості інформаційної системи виражається в тому, що потенційні зловмисники мають зустрітися з перешкодами, складними обчислювальними завданнями при потенційній хакерській атаці.

Мінімізація дублювання передбачає мінімізацію ідентичних процедур для декількох споживачів, наприклад, таких як введення паролів.

Побудована за наведеними принципами система інформаційної безпеки має бути налаштована на досягнення визначених цілей, специфіка яких буде великою мірою визначати структуру системи і основні параметри її функціонування (Рудий, Томаневич, Руда, 2014).

Для підприємств основними цілями досягнення високого рівня інформаційної безпеки є забезпечення її основних складових: цілісності, достовірності, конфіденційності (рис. 3).

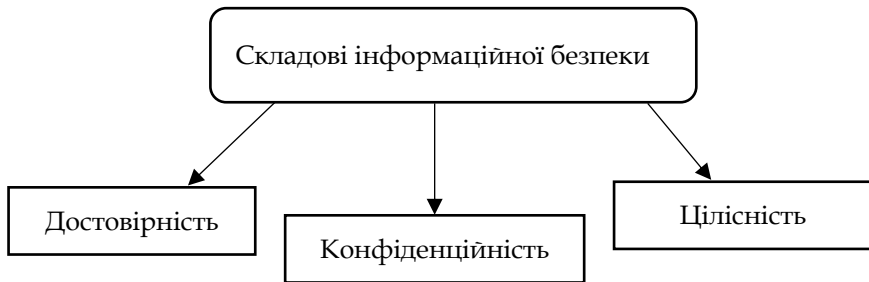


Рис. 3 Складові інформаційної безпеки

Доступність – це можливість за певний період часу одержати необхідну інформаційну послугу.

Цілісність – це актуальність і несуперечність інформації, її захищеність від змін та видалення. В свою чергу цілісність можна розділити на статичну (розуміється як незмінність інформаційних об'єктів) і динамічну (відноситься до коректного виконання певних дій та складних транзакцій).

Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана і поширена серед певного кола індивідів.

Успішність функціонування підприємств у динамічному ринковому середовищі значною мірою визначається станом інформаційної безпеки. Рівень економічної безпеки суб'єкта господарювання залежить від того, наскільки ефективною є інформаційна безпека суб'єкта господарювання, що дає змогу уникнути можливих загроз та негативних наслідків впливу конкурентного середовища.

Отже, безпека підприємства – це такий стан корпоративних ресурсів (ресурсів капіталу, персоналу, інформації і технології, техніки та устаткування, прав) і підприємницьких можливостей, за якого гарантується найбільш ефективно їхнє використання для стабільного функціонування та динамічного науково-технічного й соціального розвитку, запобігання внутрішнім та зовнішнім негативним впливам (загрозам) (Архипов, Скиба, 2013).

Відповідно достатній рівень інформаційної безпеки дає змогу підприємству повною мірою використовувати необхідну інформацію для прийняття результативних управлінських рішень, виконання яких обумовить подальшу фінансову стійкість підприємства і буде сприяти його подальшій ефективній роботі (Войнаренко, Рзаєв, Рзаєва, 2014).

Література

Архипов, О., Скиба, А. (2013). Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації. *Захист інформації*, 15, 4, 350–375.

Василенко, М. (2018). Підвищення стану кібербезпеки інформаційно комунікаційних систем: якість у контексті вдосконалення інформаційного законодавства. *Юридичний вісник*, 3, 17–24.

Герасименко, О. В., Козак, А. В. (2015). *Інформаційна безпека підприємства: поняття та методи її забезпечення*. URL: <http://intkonf.org/ken-gerasimenko-ov-kozak-av-informatsiy-na-bezpeka-pidpriemstva-ponyattya-ta-metodi-yiyi-zabezpechennya/>

Іванова, В. *Інформаційна безпека як підсистема в системі економічної безпеки підприємства*. URL: <http://eprints.kname.edu.ua/38599/1/67-71.pdf>.

Войнаренко, М. П., Рзаєв, Г. І., Рзаєва, Т. Г. (2014). *Інформаційна безпека підприємства у динамічному ринковому середовищі*. Хмельницький.

Закон про сновні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки Закон України 2007 (Верховна Рада України). Офіційний сайт Верховної Ради України. URL: <https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=537-16#Text>

Рудий, Т., Томаневич, Л., Руда, О. (2014). Засади захисту інформації в інформаційних системах підприємств. *Актуальні проблеми економіки*, 2 (152), 351–387.

Северина, С. (2016). Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету. Економічні науки*, 1, 132–154.

Куля Ірина Федорівна

Придунайська філія МАУП, м. Ізмаїл, Україна

ORCID: 0000-0002-8363-1478

Пирлог Олександр Сергійович

Придунайська філія МАУП, м. Ізмаїл, Україна

КІБЕРГІЄНА У ІНФОРМАЦІЙНОМУ ПРОСТОРІ В УМОВАХ ВОЄННОГО СТАНУ

Стратегія розвитку вкрай інтелектуального суспільства в умовах промислової революції тісно пов'язана із сферою інформаційного простору. У контексті Суспільства 5.0, штучний інтелект, робототехніка, обробка великих даних та інтернет речей (IoT) надають вагомий вплив на функціонування сучасних технологій у всіх сферах життя. Інформаційний простір країни охоплює усі інформаційні ресурси та інфраструктуру, які дозволяють забезпечувати безпечну інформаційну взаємодію держави, організацій та громадян на основі загальних принципів та правил через доступ до відкритих інформаційних ресурсів.

Сучасний світ вже здійснив перший крок у напрямку принципово нової технологічної, економічної та соціальної реальності – епохи цифрової глобалізації. Забезпечення кібербезпеки визнається одним із ключових пріоритетів загальної системи національної безпеки України. На початку XXI століття активно формуються ризики, із якими стикається сучасна цивілізація через впровадження передових технологій. Кіберзагрози стають все більш вагомими, і ця тенденція буде зростати в міру розвитку інформаційних технологій та їх злиття з штучним інтелектом в найближчому десятилітті національних, так і міжнародних, створює нову безпекову ситуацію. Між сильними глобальними центрами влади відбувається розподіл сфер впливу у кіберпросторі, і ця тенденція підсилює їх бажання забезпечити реалізацію своїх геополітичних інтересів за рахунок такого розподілу.

Кіберпростір, разом із фізичними просторами, визнається одним із потенційних театрів воєнних дій. Набуває актуальності тенденція створення кібервійськ, яка має завдання не лише захищати критичну інформаційну інфраструктуру від кібератак, але й проводити передбачальні операції у кіберпросторі. Ці операції включають в себе виведення з ладу критичних об'єктів інфраструктури противника через руйнування інформаційних систем, які управляють цими об'єктами. Однак, основою для успішної системи кібербезпеки є ефективна нормативно-правова база, і в цьому контексті, важливим є указ Президента України «Про Стратегію кібербезпеки України», виданий 26 серпня 2021 року. Ця стратегія передбачає розвиток максимально вільного, безпечного, відкритого та стабільного кіберпростору в інтересах захисту прав людини.

У сучасних умовах, коли країна перебуває в стані воєнного конфлікту, це стає актуальним завданням не лише для фахівців у галузі інформаційних технологій, але й для кожного громадянина. Навчання застосуванню цифрової грамотності, дотримання цифрового етикету та правил кібергігієни стає критично важливим. Вже на початку конфлікту фахівці з усієї країни приєдналися до кіберполіції та успішно допомогли вивести з ладу критично важливі інформаційні системи окупанта. Однак українцям також необхідно дотримуватися правил кібергігієни, оскільки інформаційний простір є джерелом поширення фейкових новин, діпфейків, підроблених веб-сайтів, фішингових атак, заволодіння обліковими записами та інших загроз. Розглянемо більше деталей щодо можливих загроз та правил кібергігієни для боротьби з ними.

Фейки. Умови воєнного стану в Україні створюють ситуацію, коли українці практично кожну хвилину оновлюють свої новини, спрямовані на отримання актуальної інформації про ситуацію на фронті та в дипломатичному полі. Проте ворог активно розповсюджує фейки, в яких стверджується, що міста були захоплені, Україна капітулює або проводить евакуацію місцевого населення.

Правило кібергігієни у боротьбі з фейками полягає в тому, щоб довіряти лише офіційним та перевіреним джерелам

інформації, а не сумнівним телеграм-каналам або публікаціям у соціальних мережах. Важливо пам'ятати, що навіть довірені медіа та офіційні особи можуть допустити помилки. Тому після прочитання важливої новини, рекомендується чекати її спростування або підтвердження.

Діпфейки. Ситуація стає складнішою, коли мова йде про діпфейки, які включають в себе підроблені відеоролики, на яких публічна особа виступає та говорить у своєму голосі. Наприклад, Центр інформаційної безпеки попереджав, що в мережі може з'явитися відеозвернення Президента Володимира Зеленського, в якому він, начебто, оголосить про капітуляцію. Проте такі технології машинного навчання можуть бути використані, щоб вводити в оману та підривати моральний дух. Правило кібергігієни в боротьбі з діпфейками полягає в уважному спостереженні за деталями, які можуть вказувати на їхню підробку, такі як неприродний тон і текстура шкіри, неправильне освітлення обличчя, нерівномірне кліпання очей та інше. Основне правило – перевіряти відеозвернення лише на офіційних ресурсах і джерелах. Підробки сайтів та акаунтів офіційних структур стали поширеними явищами під час воєнного конфлікту. З метою дезорієнтації населення з'являється багато аналогічних сторінок, що імітують офіційні структури. Наприклад, можна стикнутися з фейковим акаунтом Верховної Ради України у соціальних мережах або підробленим веб-сайтом Служби безпеки України. Правило кібергігієни для виявлення підробки сайтів та акаунтів офіційних структур включає уважне спостереження за кількістю підписників та публікацій на сторінці в соціальних мережах, а також перевірку наявності верифікаційного знаку (синя галочка) поруч з ім'ям користувача. Щодо веб-сайтів, важливо звертати увагу на адресний рядок браузера, де повинен бути символ замочку, що вказує на наявність сертифіката безпеки. Також сайт можна перевірити через сервіс Whois, щоб дізнатися інформацію про дату реєстрації, власника та інші юридичні дані

Фішингові посилання є одним з найпоширеніших та найнефективніших методів інтернет-шахрайства під час воєнного конфлікту. Зловмисники надсилають різні типи файлів,

включаючи посилання на веб-сайти, архівовані документи чи медіафайли. Такі повідомлення можуть надходити як на електронну пошту, так і в особисті повідомлення у соціальних мережах чи месенджерах. Одним із удосконалених методів фішингу є підробка посилань на підписи електронних петицій.

Правило кібергігієни для захисту від фішингових посилань включає в себе обережне ставлення до незапрошених посилань та файлів. Якщо вам надійшло подібне повідомлення від знайомих контактів, рекомендується уточнити в них, що саме міститься в цьому повідомленні, оскільки навіть сторінки ваших друзів можуть бути під зламом. Також важливо уважно перевіряти адресу веб-сайту в адресному рядку браузера, оскільки зловмисники часто замінюють лише одну літеру чи символ, щоб підробити домен. Україна повинна мати здатність забезпечити свій соціально-економічний розвиток у цифровому світі. Це передбачає необхідність набуття спроможності ефективно запобігати негативним впливам у кіберпросторі, досягати стійкості до кіберзагроз на всіх рівнях та сприяти взаємодії всіх суб'єктів, які забезпечують кібербезпеку, ґрунтуючи цю взаємодію на довірі. Отже, можна зазначити, що настання нової ери кібербезпеки вимагає повністю нового підходу до управління інформаційними ресурсами. Успішна реалізація таких змін значною мірою залежить від гнучкості організації процесів на державному рівні і впровадження нових моделей та методів роботи у боротьбі з потенційними кіберзагрозами.

Література

Кібербезпека: загрози та заходи захисту (2010). Донецьк: Юго-Восток.

Коваленко, М. А., Нагорна, І. І., Радванська, Н. В. (2009). *Кібергігієна: важливість цифрової грамотності в умовах кіберзагроз. Інформаційна безпека. Економічна безпека корпоративного підприємства*. Херсон: Олді-плюс.

Кібератаки під час воєнних конфліктів: аналіз сучасних загроз (2009).

Сімовнова, М., Черкасов, А. В. (2011). *Цифрова гігієна: як захистити себе від інтернет-загроз*. Луганськ: Янтар.

Куля Ірина Федорівна

Придунайська філія МАУП, м. Ізмаїл, Україна

ORCID: 0000-0002-8363-1478

Спиридонова Валерія Володимирівна

Придунайська філія МАУП, м. Ізмаїл, Україна

БЕЗПЕКА ПІДПРИЄМСТВА ЯК ОСНОВНИЙ ВИД ДІЯЛЬНОСТІ МЕНЕДЖЕРА ПІДПРИЄМСТВА

В умовах ринкових відносин, коли держава не несе відповідальності за результати фінансово-господарської діяльності підприємства, забезпечення безпеки стає одним із найважливіших і актуальних питань його життєдіяльності.

Менеджери та фахівці з питань підприємництва, безпеки бізнесу в державних та інших організаціях повинні розуміти закони, принципи та методи ринкової економіки. Ці організації не тільки можуть отримати переваги та успіх, але певні види діяльності часто супроводжуються величезними ризиками, небезпеками та загрозами, а забезпечення безпеки цієї сфери діяльності має свої особливості. Тому лише системне управління підприємством та його безпека може бути запорукою успіху підприємства.

При цьому всі члени команди – від підприємців до менеджерів і рядових співробітників – повинні серйозно ставитися до питань особистої та організаційної безпеки, особливо під час криз, конфліктів і подібних ситуацій. З цією метою менеджери та фахівці з безпеки повинні досконало розуміти та ефективно застосовувати основні методи управління організаціями, людьми та системами безпеки в бізнес-діяльності. Управлінські функції в сучасному менеджменті можуть бути успішно реалізовані лише тоді, коли чітко визначені права та обов'язки керівників. Інакше, як підтверджує зарубіжний і особливо вітчизняний досвід, менеджери стануть бізнес-агентами, рядовими чиновниками, адміністраторами та службовцями.

По-перше, враховуючи жорстку конкуренцію та прояви загроз, небезпек, ризиків і конфліктів у цій благородній, але небезпечній діяльності підприємництва, необхідно вивчити основи ринкової економіки та безпеки підприємництва. Отже, безпека підприємств передбачає сталий розвиток (тобто збалансованість і стійкість), який досягається шляхом використання різноманітних ресурсів і підприємницьких можливостей для забезпечення їх найбільш ефективного використання для досягнення стабільної роботи та динамічного розвитку науки, техніки та суспільства. Розвиток, попередження внутрішніх і зовнішніх негативних впливів (загроз).

Найпоширенішим визначенням безпеки підприємства є стан, за якого підприємство ефективно використовує свої ресурси (капітальні ресурси, персонал, інформаційні технології, обладнання та права) та існуючі ринкові можливості для запобігання внутрішнім і зовнішнім негативним впливам (загрозам) і забезпечення тривалого термін розвитку підприємства. Довгострокове виживання та сталий розвиток на ринку відповідно до обраної місії.

Об'єктами безпеки є країни, соціальні групи, регіони, підприємства та окремі громадяни.

Необхідність постійного дотримання безпеки залежить від об'єктивно наявних завдань кожного суб'єкта господарювання щодо забезпечення функціональної стабільності та досягнення основних цілей його діяльності. Рівень економічної безпеки підприємства залежить від здатності його керівництва та спеціалістів (керівників) ефективно уникати можливих загроз та усувати шкідливу дію окремих негативних факторів зовнішнього та внутрішнього середовища.

Джерелами негативного впливу на безпеку підприємства можуть бути:

1. Свідомі чи несвідомі дії окремих посадових осіб і комерційних структур (органів державної влади, міжнародних організацій, компаній-конкурентів);
2. Збіг об'єктивних обставин (ринковий фінансовий стан компанії, наукові відкриття та технічний розвиток, форс-мажорні обставини тощо). Залежно від умов суб'єкта негативний вплив

на безпеку може носити як об'єктивний, так і суб'єктивний характер. Цей негативний вплив існує об'єктивно і не зумовлений волевиявленням конкретної компанії чи окремого працівника. Суб'єктивний вплив зумовлений неефективністю діяльності підприємства в цілому або окремих працівників (переважно керівників і функціональних керівників) (Коваленко, Нагорна, Радванська, 2009; Родіонов, Черкасов, 2011).

Основна мета безпеки підприємства полягає в тому, щоб підприємство на даний момент було стабільним, функціонувало максимально ефективно і мало високий потенціал розвитку в майбутньому.

Основні функціональні цілі безпеки включають:

- забезпечення високої ефективності фінансової роботи, фінансової стабільності та корпоративної незалежності;
- забезпечення технологічної незалежності того чи іншого суб'єкта господарювання та досягнення високого рівня конкурентоспроможності його технологічного потенціалу;
- досягнення високої ефективності управління, оптимізації та ефективної організаційної структури корпоративного управління;
- досягнення високого рівня кваліфікації та інтелектуального потенціалу співробітників;
- звести до мінімуму згубний вплив результатів виробничо-господарської діяльності на стан навколишнього середовища;
- забезпечення якісного правового захисту всіх аспектів корпоративної діяльності;
- забезпечити захист інформаційних полів і комерційної таємниці, забезпечити необхідний рівень інформаційного забезпечення роботи різних підрозділів підприємства та організації;
- ефективна організація безпеки персоналу підприємства, його капіталу та майна, а також комерційних інтересів (Родіонов, Черкасов, 2011).

Головна та функціональні цілі зумовлюють формування необхідних структуроутворюючих елементів і загальної схеми організації безпеки підприємства.

Забезпечення безпеки передбачає виділення, аналіз і оцінку існуючих загроз з кожної функціональної складової

та розроблення на їх основі системи протидіючих і застережних заходів.

Отже, безпека підприємництва являє собою універсальну категорію, що відбиває захищеність суб'єктів соціально-економічних відносин на всіх рівнях, починаючи з держави і закінчуючи кожним її громадянином. Зміст даного поняття містить у собі систему засобів, що забезпечують конкурентопотенційність і економічну стабільність підприємства а також сприяють підвищенню рівня добробуту робітників і тільки за здійснення в необхідному обсязі зазначених дій можна буде досягти належного рівня безпеки підприємства.

Література

Хвесик, М. А., Степаненко, А. В., Ральчук, О. М., Дорош Й. М. (2010). *Антикризове управління економічною безпекою в умовах викликів фінансово-економічної глобалізації (державний і регіональний виміри)*. Донецьк: Юго-Восток.

Мельник, П., Терангул, Л. та ін (2009). *Економічна безпека*. Київ: Знання.

Коваленко, М. А., Нагорна, І. І., Радванська, Н. В. (2009). *Економічна безпека корпоративного підприємства*. Херсон: Олді-плюс.

Кавун, С. В. (2009). *Система економічної безпеки: методологічні та методичні засади*. Харків: ХНЕУ.

Родіонов, О. В., Черкасов, А. В. (2011). *Формування та розвиток економічної безпеки підприємств*. Луганськ: Янтар.

ასმათ შამუგია

*ეკონომიკის აკადემიური დოქტორი
ახალი უმაღლესი სასწავლებელი- ნიუენი
ავილირებული ასოცირებული პროფესორი
საქართველო, თბილისი*

HR მენეჯერის ინოვაციური სტრატეგია გლობალური პანდემიის გამოწვევის ფონზე

უდავო ფაქტია, რომ HR მენეჯერი საკუთარი დეპარტამენტის საქმიანობის დაგეგმვისას ორგანიზაციის მიზნებსა და ამოცანებს ეყრდნობოდა. ამიტომ, პრიორიტეტული მიმართულებები ყოველწლიურად შეუძლებელია ერთი და იმავე იყოს და მნიშვნელოვანია აუცილებლად იცვლებოდა. ქვემოთ გთავაზობთ 21-ე საუკუნის ადამიანური რესურსების მენეჯერის აქტუალური ამოცანების თანამედროვე მაგალითებს: კომპანიის კადრებისთვის სამუშაო პირობების შექმნა, განვითარება და გაუმჯობესება; თანამშრომლების მოთხოვნილებათა პროგნოზირება – HR მენეჯერს უნდა შეეძლოს დამოუკიდებლად გააანალიზოს მის ხელთ არსებული მონაცემები და მკაფიოდ ჩამოაყალიბოს ხედვა. აქ იგულისხმება, ადამიანური რესურსების უნარი თანხვედრაში მოიყვანოს დეპარტამენტის სტრატეგიული ხედვა და ორგანიზაციის მიმდინარე ამოცანები. იმ შემთხვევაში, თუ HR მენეჯერს დამოუკიდებლად არ შესწევს ამ ამოცანის შესრულების უნარი, იგი გარე რესურსების გამოყენებას არ უნდა თაკილობდეს; მაღალკვალიფიციური კადრების შერჩევა, რომელთაც ორგანიზაციის კორპორაციულ კულტურაზე გავლენის მოხდენა შეუძლიათ – აქ ყურადღება შემდეგ მიმართულებებზე უნდა გამახვილდეს: უნიკალური და ნიჭიერი ადამიანების ძიება, რათა მათ გახსნან ახალი ბიზნესშესაძლებლობები; სხვადასხვა მიმართულებით უწყვეტი მუშაობის წარმართვა, კერძოდ: პროფესიულ წრეებში, ფორუმებზე, სოციალურ ქსელებში და ა.შ. HR მენეჯერმა საჭიროა მკაფიოდ განსაზღვროს პერსონალის

შერჩევის მექანიზმები და ინსტრუმენტები; მოიძებნოს შერჩევის თანამედროვე ტექნოლოგიები, რომლებიც HR მენეჯერებს საშუალებას მისცემს ვაკანსიები სწრაფად და ორგანიზაციისთვის მინიმალური დანახარჯებით შეავსონ; პერსონალის ადაპტაციის სისტემის შექმნა – აუცილებელია ახალი კადრების არა მხოლოდ შერჩევა, არამედ ახალი სპეციალისტის მისაღებად ორგანიზაციის მომზადება. ადაპტაციის სისტემის შექმნა და თანამშრომლის დაკარგვის რისკის მინიმიზაცია; დასაქმებული კადრების კარიერის განვითარება: ტრენინგი, შეფასება, დაგეგმვა და ა.შ. – შეიძლება ითქვას, რომ ახალი თანამშრომლის ადაპტაცია პირველი გასაუბრებიდან იწყება. HR მენეჯერის ერთ-ერთი ამოცანაა, რომ სწრაფად მოხდეს ადამიანის კეთილგანწყობა ორგანიზაციის მიმართ. თანამშრომელი რაც უფრო სწრაფად ადაპტირდება ორგანიზაციაში, მით უფრო მალე მოახდენს საკუთარი რესურსის რეალიზებას. კვლევებით დადასტურებულია, რომ გამოსაცდელი ვადის პერიოდში ადამიანი იყენებს თავისი შესაძლებლობების მხოლოდ 30%-ს. ამ პერიოდში ორგანიზაცია ბევრს კარგავს. თავიდანვე უნდა მოხდეს ახალბედა კადრების გარკვევა იმაში, თუ როგორი კულტურაა კომპანიაში, რისი თქმა შეიძლება და რისი – არა, რათა დასაქმებულმა ნათლად გააცნობიეროს სად იწყებს იგი მუშაობას; ანაზღაურების ადეკვატური სისტემის ჩამოყალიბება, დროული კორექტირება და პერსონალის მოტივაცია; ორგანიზაციის შიგნით სწორი საკომუნიკაციო სისტემის შექმნა – HR მენეჯერისათვის მნიშვნელოვანია არა მხოლოდ ლიდერების განვითარება, არამედ კოლექტიური ეფექტურობის შემუშავება, განყოფილებებში ინტერაქცია და გუნდური შედეგების მიღწევა; კომპანიისთვის ე.წ. HR ბრენდის შექმნა – HR მარკეტინგის განხორციელება, შრომის ბაზრისა და კანდიდატების ანალიზი, ვაკანსიების შესახებ სამიზნე აუდიტორიის ინფორმირება და ა.შ. თანამშრომელთა კმაყოფილების და ჩართულობის გაზრდა – ამ მიმართულებით ადამიანური რესურსების მენეჯერი რეგულარულად უნდა აკონტროლებდეს ვითარებას. მან საჭიროა ამოიცნოს და თავიდან აიცილოს რისკები, რომლებიც დემოტივაციასთან და ძვირფასი თანამშრომლების კონკურენტებთან გადასვლის საფრთხესთან არის

დაკავშირებული. თანამდებობიდან გათავისუფლების პროცესის ორგანიზება – საუბარია არა მხოლოდ დოკუმენტებზე, არამედ სისტემის შემუშავებაზე. კორპორაციული კულტურის შექმნა – კომპანიის კორპორაციულ ცხოვრებაში მაქსიმალური ჩართულობა: მნიშვნელოვან სესიებში, შემაჯგებელ წლიურ ღონისძიებებში მონაწილეობა და ა.შ. სწავლების თანამედროვე მეთოდების, ტექნოლოგიების ძიება და რეალიზება – მაგალითად, დასავლეთის განვითარებული ქვეყნების ბევრ კომპანიაში 2018 წლიდან, მართვის პერსონალიზაციის ტრენდში ახალი იმპულსი შეინიშნება, კერძოდ ე.წ. TALENT MANAGEMENT, ბონუსების ინდივიდუალური სისტემა, თანამშრომლებისთვის პრემიებისა და კომპენსაციების შეთავაზება იდეების განსახორციელებლად, კეთილდღეობის პროგრამების (Well-being) გამოყენება (პირად ცხოვრებასა და საქმეს შორის ბალანსის ხელშეწყობა), კარიერული საკონსულტაციო მომსახურებების უზრუნველყოფა და ა.შ. პერსონალთან მუშაობის ავტომატიზაცია – რაც უფრო მეტი ამოცანაა ავტომატიზებული, მით უფრო მეტი დრო დარჩებათ თანამშრომლებს ინტელექტუალურ მუშაობაზე, რაც კომპანიას მნიშვნელოვან მოგებას მოუტანს. ხელმძღვანელების კონსულტირება – რათა უკეთ მოხდეს თანამშრომლების პოტენციალის რეალიზება. აქვე ხაზი უნდა გაესვას ბიზნესის დამფუძნებლებთან და ტოპ მენეჯერებთან მუდმივი დიალოგის არსებობის აუცილებლობას, ბიზნესის მიზნებისა და სტრატეგიების სინქრონიზაციისთვის. ურთიერთქმედება ბიზნესის მფლობელთან – HR მენეჯერმა ორგანიზაციის ხელმძღვანელებს საჭიროა თავისი საქმიანობის მნიშვნელობა და როლი წარმოუჩინოს. მისი ამოცანაა ასევე წვლილი შეიტანოს კონკრეტული სპეციალისტების სწორი ინსტრუმენტების შერჩევაში, იმის საჩვენებლად, თუ რა პრობლემები აცილია კომპანიამ თავიდან მათი წყალობით.

თანამედროვე მსოფლიოში მაღალკვალიფიციური კადრის, პროფესიონალების (ტალანტების) მოძიებასთან დაკავშირებით ინტენსიური კონკურენცია არსებობს. შემდგომი ორი ათწლეულის განმავლობაში, ეკონომიკის განვითარების პირობებში ორგანიზაციებში არსებული ვაკანტური ადგილების შევსება ახალი

კომპეტენტური კადრით სულ უფრო პლობლემური გახდება. მსოფლიოში არსებული კომპანიების 34% უკვე განიცდის კომპეტენტური ტალანტების დეფიციტს. 2022 წელს ეს სტატისტიკა 35%-ით გაიზარდა. აღნიშნული კრიზისი გლობალურ ხასიათს ატარებს და დღესდღეობით იაპონიაში – 81%, ბრაზილიაში – 71%, ავსტრალიაში – 50%, აშშ-ში – 49%, ინდოეთში დამსაქმებლების 48% და საქართველოში 85% მოიცვა.

ბოლო წლებში აქტიურად იცვლება მენეჯმენტი, მისი ინსტრუმენტები და ტექნიკა. რა თქმა უნდა, გლობალური პანდემია გახდა ამ ცვლილებების ძლიერი კატალიზატორი. COVID-19- ის შემდგომი სამყარო, ცხადია, იგივე აღარაა, თუმცა არავინ იცის ზუსტად როგორი იქნება ინოვაციური რეალობა. აშკარაა, რომ მსოფლიო არ დაუბრუნდება თავის წინა მდგომარეობას. ამიტომ თანამედროვე მენეჯერებმა საჭიროა სისტემატურად აკონტროლონ ტენდენციები და მაჩვენებლები, უნდა ისწრაფონ თამამი ცვლილებების შეტანისკენ ადამიანური რესურსების მართვის ინოვაციურ სტრატეგიაში ორგანიზაციის მოქნილობის გაზრდის უზრუნველსაყოფად. ნებისმიერი კრიზისი, პირველ რიგში, შესაძლებლობებია, უბრალოდ აუცილებელია მისი დანახვა და დროული გაცნობიერება.

ჩატარებული ანალიზის საფუძველზე შეგვიძლია დავასკვნათ: უაღრესად მნიშვნელოვანად მიგვაჩნია, რომ თანამედროვე ორგანიზაციის ანტიკრიზისული მართვის სტრატეგიული ორიენტაციის სრულყოფა მიმდინარეობდეს ქვეყნის ეკონომიკის გლობალურ საბაზრო ურთიერთობებში ჩართვისა და პოზიციების გაძლიერების კვალობაზე, რაზედაც ძირითადად აქცენტს აკეთებდნენ Covid-19-თან ბრძოლის წინააღმდეგ, საქართველოში წარმატებით ფუნქციონირებადი სოციალური პასუხისმგებლობის მქონე ინოვაციური კომპანიები.

ბიბლიოგრაფია

Armstrong`s M. (2020). *Handbook of Human Resource Management Practice*. P. 20-50.

Higginbottom Karen – Top Challenges Facing HR Directors Of Global Firms in 2017 (December 2018). Forbes.com.

Human Resources Degree Levels.
URL: <https://www.humanresourcesmba.net/>

LEADERSHIP 2023 Top Leadership Training Companies.

URL: <https://trainingindustry.com/top-training-companies/leadership/2023-top-leadership-training-companies/>

რა უნდა იცოდეს CEO-მ ადამიანური რესურსის მართვაში.

URL: <http://www.insource.ge/ge/node/228>

Наукове видання

СУЧАСНІ ЗАГРОЗИ ГЛОБАЛЬНІЙ ТА РЕГІОНАЛЬНІЙ БЕЗПЕЦІ

МАТЕРІАЛИ

Міжнародної науково-практичної інтернет-конференції

(м. Одеса, 29 жовтня 2023 року)

Електронне видання

Укладач – Полухіна Аліна

Ум-друк. арк. 24,36.

Зам. № 2311-03.

Видавець ПП «Фенікс»

(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).

Україна, м. Одеса, 65009, вул. Зоопаркова, 25.

e-mail: fenix-izd@ukr.net