Міністерство освіти і науки України
Волинський національний університет імені Лесі Українки

Кваліфікаційна наукова
праця на правах рукопису

ВОЗНЮК ЄВГЕНІЯ ВАСИЛІВНА

УДК 327-049.5]:323.28:001.102

ДИСЕРТАЦІЯ

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ЧИННИК ВПЛИВУ НА МІЖНАРОДНУ ТА НАЦІОНАЛЬНУ БЕЗПЕКУ

23.00.04 – політичні проблеми міжнародних систем
і глобального розвитку

Подається на здобуття наукового ступеня доктора політичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.
_____ Є. В. Вознюк

Луцьк – 2025

АНОТАЦІЯ

Вознюк Є. В. Інформаційний тероризм як чинник впливу на міжнародну та національну безпеку. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора політичних наук за спеціальністю 23.00.04 – політичні проблеми міжнародних систем і глобального розвитку. – Волинський національний університет імені Лесі України (м. Луцьк).

Дисертаційне дослідження стосується комплексного аналізу феномену інформаційного тероризму як нового типу глобальної загрози в системі міжнародних відносин і національної безпеки. У роботі обґрунтовано, що в умовах цифрової епохи та гібридних війн інформаційний тероризм стає одним із ключових інструментів дестабілізації політичних систем, руйнування довіри до інституцій і підриву міжнародної стабільності.

Актуальність теми визначається ескалацією інформаційних загроз, що супроводжують сучасні конфлікти, насамперед російсько-українську війну, а також зростанням впливу медіа- та кіберпростору на процеси прийняття політичних рішень. Інформаційний тероризм розглянуто як багатовимірний феномен, що поєднує елементи когнітивної війни, кібертероризму, дезінформації, пропаганди й інформаційно-психологічних операцій, спрямованих на підрив суверенітету, демократичних інститутів і соціальної єдності.

Мета дослідження – виявлення сутності, форм та механізмів інформаційного тероризму, аналіз його впливу на міжнародну й національну безпеку, а також визначення ефективних моделей протидії на глобальному, регіональному та національному рівнях. Для досягнення мети застосовано міждисциплінарний методологічний підхід, що поєднує засоби політичного аналізу, неоінституціоналізму, конструктивізму, теорії міжнародної безпеки, кібернетики, соціальної психології й стратегічних комунікацій.

Об’єктом дослідження є система міжнародної безпеки в умовах інформаційної епохи, а предметом – інформаційний тероризм як форма деструктивного інформаційного впливу на політичні процеси, державні інститути та глобальний порядок.

У дисертації здобуто низку результатів, що мають теоретичну та практичну новизну. Зроблено вагомий внесок у розвиток сучасної політичної науки, розширено уявлення про інформаційний вимір безпеки й сформовано нову теоретико-практичну парадигму інформаційної стійкості держави як головного ресурсу протидії інформаційному тероризму у XXI ст.

Уперше:

– сформульовано концепцію інформаційної стійкості як ключової складової частини національної безпеки та соціальної згуртованості в умовах гібридних загроз. Визначено її як спроможність держави, інституцій і громадянського суспільства протистояти дезінформації, маніпуляціям та пропаганді шляхом поєднання технічних, правових, освітніх і психологічних механізмів;

– розроблено концептуальні напрями модернізації Закону України «Про боротьбу з тероризмом» з урахуванням цифрової трансформації загроз. Запропоновано ввести поняття «інформаційна стійкість», «інформаційний тероризм», «кібертероризм», «інформаційно-психологічна операція» (ІПсО), що розширює правове поле антитерористичної діяльності;

– обґрунтовано трикомпонентну модель забезпечення інформаційної стійкості, яка включає стратегічні комунікації, медіаосвіту та цифрову безпеку. Уперше системно проаналізовано взаємозв’язок між цими елементами як основою національної й міжнародної інформаційної безпеки;

– здійснено міждисциплінарне дослідження міжнародного тероризму в умовах глобалізації та запропоновано нову концептуалізацію інформаційного тероризму як автономного феномену, що поєднує риси когнітивної війни, кібертерору й ідеологічної агресії;

– проведено системний аналіз українського досвіду протидії інформаційному тероризму в умовах гібридної агресії рф. Визначено нові елементи інформаційної стійкості України – алгоритмічну протидію фейкам і мобілізацію цифрового громадянського суспільства. Запропоновано розглядати український досвід як модель для формування глобальної стратегії цифрової безпеки;

– надано нову інтерпретацію подій 11 вересня 2001 р. як переломного етапу трансформації світової парадигми безпеки та початку ери інформаційно-психологічного й асиметричного протиборства.

Перший розділ має концептуально-теоретичний характер. У ньому розглянуто еволюцію поняття тероризму – від класичних форм політичного насильства до його сучасних проявів у цифровому середовищі. Здійснено огляд ключових підходів до інтерпретації тероризму в політичній науці, міжнародному праві, безпекових студіях і комунікативних теоріях. Визначено, що тероризм у XXI ст. виходить за межі традиційних методів фізичного впливу, набуваючи інформаційного, психологічного, ідеологічного та технологічного вимірів. Проведено аналіз теоретико-методологічних основ дослідження – неореалізму, конструктивізму, неоінституціоналізму, теорії гібридних війн і когнітивних комунікацій. Окремо окреслено методологію та джерельну базу дослідження тероризму: нормативно-правові документи, міжнародні угоди, наукові публікації, аналітичні звіти, емпіричні дані й приклади реальних інформаційних операцій. Підсумком розділу є формування методологічного підґрунтя для подальшого аналізу інформаційного тероризму як окремого феномену.

У другому розділі розкрито сутність, структурні характеристики та механізми інформаційного тероризму. Доведено, що події 11 вересня 2001 р. стали рубежем у трансформації тероризму – саме тоді відбувся перехід від фізичного насильства до інформаційно-цифрових форм впливу. У цьому контексті проаналізовано появу таких феноменів, як:

– медіатероризм (використання мас-медіа для залякування, шантажу, пропаганди);

– кібертероризм (атаки на інформаційну інфраструктуру);

– символічний тероризм (маніпуляція образами та символами, що впливають на масову свідомість).

Досліджено механізми інформаційного впливу, як-от: створення фейкових наративів, поширення паніки, утручання в комунікаційні мережі, підрив довіри до урядів і міжнародних організацій. Розділ завершується висновком, що інформаційний тероризм є системним елементом гібридної війни, де інформація використовується як зброя для досягнення політичних цілей без прямого застосування сили.

У третьому розділі спрямований осмислено інформаційну війну як найвищу форму сучасного інформаційного конфлікту. Обґрунтовано те, що інформаційна війна та інформаційний тероризм – це взаємопов’язані феномени, які функціонують у єдиному полі глобальної боротьби за свідомість. Розглянуто інституційні характеристики інформаційних війн, виокремлено їхні основні інструменти: фейкові новини, ботоферми, кібератаки, когнітивні впливи, «інформаційне дзеркало» (імітація альтернативної реальності). Окрему увагу приділено інформаційній зброї як системі засобів неконвенційного тиску, спроможних досягати політичних ефектів, співмірних із військовими. Важливою новацією цього розділу є введення поняття інформаційної стійкості як антиподу інформаційному терору. Обґрунтовано, що формування стійкості передбачає розвиток стратегічних комунікацій, цифрової освіти та медіаграмотності, а також побудову державної системи реагування на дезінформаційні кампанії. Зроблено висновок, що інформаційна війна є головною площиною гібридного протиборства XXI ст., де боротьба ведеться за контроль над знанням, наративом і довірою.

Четвертий розділ має аналітико-порівняльний характер. У ньому розглянуто національні моделі інформаційної безпеки таких провідних держав

світу, як США, країни ЄС, Японія, Китай, Індія, а також країни Африки й Латинської Америки. Порівняльний аналіз дає змогу виявити різні підходи до інформаційного контролю:

– американську модель, орієнтовану на баланс між безпекою та свободою слова;

– європейську модель, засновану на праві, демократії й кіберетичній відповідальності;

– китайську модель з акцентом на державному контролі та цензурі;

– японську модель із перевагою технологічного й превентивного кіберзахисту;

– африканську модель із розвитком систем інформаційної безпеки, що поєднують національну стабільність з обмеженими технологічними ресурсами та міжнародними ініціативами з підвищення цифрової стійкості;

– латиноамериканську модель із посиленням регіональної співпраці, боротьбою з дезінформацією й просуванням цифрових прав в умовах політичної поляризації та нерівномірного кіберуправління.

У розділі також розкрито досвід країн Глобального Півдня, які формують власні стратегії протидії інформаційним загрозам у межах обмежених ресурсів. Виявлено спільні риси, зокрема необхідність правового регулювання, координації між інституціями, підвищення цифрової грамотності населення. На основі цього здійснено узагальнення, яке дає змогу визначити оптимальні елементи для побудови національної моделі інформаційної безпеки України.

П’ятий розділ має прикладний і синтетичний характер. Увагу зосереджено на українському кейсі протидії інформаційному тероризму російської федерації, що став одним із наймасштабніших прикладів інформаційної війни у світі. Проаналізовано етапи, цілі та інструменти російської інформаційної агресії проти України з 2014 р.: створення фейкових наративів, пропагандистські кампанії, кібератаки, операції впливу в соціальних мережах, підрив міжнародного іміджу України. Досліджено

інституційні відповіді держави – діяльність Центру протидії дезінформації, кіберпідрозділів, Міністерства цифрової трансформації, а також зусилля громадських ініціатив і волонтерських мереж. Обґрунтовано, що українська модель інформаційного спротиву базується на поєднанні державних, медійних, громадянських та технологічних ресурсів, що створює новий тип інформаційної оборони. Особливу увагу приділено формуванню інформаційної стійкості суспільства – через підвищення медіаграмотності, розвиток стратегічних комунікацій, партнерство держави й громадського сектору, участь України в міжнародних ініціативах ЄС та НАТО.

Розділ завершено визначенням перспективних напрямів державної політики у сфері протидії інформаційному тероризму, серед яких:

- удосконалення законодавства;
- розвиток інформаційно-аналітичних центрів;
- посилення кіберспроможностей;
- формування українських наративів у міжнародному просторі;
- інтеграція українського досвіду в глобальні стандарти інформаційної безпеки.

У висновках зазначено, що інформаційний тероризм є системною загрозою міжнародній та національній безпеці, яка трансформує сучасну архітектуру глобальних відносин. Доведено, що ефективна протидія можлива лише за умови формування інформаційної стійкості держави, суспільства й особистості. Український досвід у цій сфері став вагомим внеском у розвиток нової безпекової парадигми, орієнтованої на демократичні цінності, критичне мислення та цифрову свідомість.

Практичне значення результатів полягає в тому, що вони можуть бути використані під час розроблення державних стратегій у сфері інформаційної безпеки, удосконаленні законодавчої бази, формування системи інформаційної освіти й стратегічних комунікацій, а також у навчальному процесі з дисциплін міжнародної безпеки, політичних комунікацій і кібербезпеки.

Ключові слова: інформаційний тероризм, інформаційна стійкість, національна безпека, міжнародна безпека, громадянське суспільство, російсько-українська війна, гібридна війна, стратегічні комунікації, дезінформація, ЄС, Україна, НАТО, міжнародні організації, конфлікти.

ABSTRACT

Vozniuk Ye. V. Information Terrorism as a Factor of Influence on International and National Security. – Qualification scientific work in the form of a manuscript.

Dissertation for the degree of Doctor of Political Sciences in the speciality 23.00.04 – Political Problems of International Systems and Global Development. – Lesya Ukrainka Volyn National University (Lutsk).

The dissertation research is devoted to a comprehensive analysis of the phenomenon of information terrorism as a new type of global threat in the system of international relations and national security. The work substantiates that information terrorism is becoming one of the key tools for destabilising political systems destroying trust in institutions and undermining international stability in the conditions of the digital era and hybrid wars.

The relevance of the topic is determined by the escalation of information threats accompanying modern conflicts, primarily the Russian-Ukrainian war, as well as the growing influence of media and cyberspace on political decision-making processes. Information terrorism is considered as a multidimensional phenomenon that combines elements of cognitive warfare, cyberterrorism, disinformation, propaganda and information and psychological operations aimed at undermining sovereignty, democratic institutions and social unity.

The purpose of the study is to identify the essence, forms and mechanisms of information terrorism, analyse its impact on international and national security, as well as determine effective models of counteraction at the global, regional and national levels. An interdisciplinary methodological approach is used in the combination with the means of political analysis, neo-institutionalism,

constructivism, international security theory, cybernetics, social psychology and strategic communications to achieve the purpose.

The object of the study is the system of international security in the information age and the subject is information terrorism as a form of destructive information influence on political processes, state institutions and global order.

The dissertation has obtained several results that have theoretical and practical novelty. The dissertation makes a significant contribution to the development of modern political science expanding the understanding of the information dimension of security and forming a new theoretical and practical paradigm of the information stability of the state as the main resource for countering information terrorism in the 21st century. For the first time:

– the concept of information stability is formulated as a key component of national security and social cohesion in the context of hybrid threats. It is defined as the ability of the state, institutions and civil society to resist disinformation, manipulation and propaganda by combining technical, legal, educational and psychological mechanisms:

– conceptual directions for the modernisation of the Law of Ukraine «On Combating Terrorism» are developed, taking into account the digital transformation of threats. It is proposed to introduce the concepts of information resilience, information terrorism, cyberterrorism, information and psychological operation (IPSO) which expands the legal field of anti-terrorist activity;

– a three-component model for ensuring information resilience is substantiated including strategic communications, media education and digital security. For the first time, the relationship between these elements was systematically analysed as the basis of national and international information security;

– an interdisciplinary study of international terrorism in the context of globalisation is carried out and a new conceptualisation of information terrorism is proposed as an autonomous phenomenon that combines the features of cognitive warfare, cyberterrorism and ideological aggression;

– a systematic analysis of the Ukrainian experience of countering information terrorism in the context of the Russian Federation's hybrid aggression is conducted. New elements of Ukraine's information resilience are identified such as algorithmic counteraction to fakes and mobilisation of digital civil society. It is proposed to consider the Ukrainian experience as a model for forming a global digital security strategy;

– a new interpretation of the events of September 11, 2001 as a turning point in the transformation of the global security paradigm and the beginning of the era of information-psychological and asymmetric confrontation is provided.

The first chapter is conceptual and theoretical in nature. It examines the evolution of the concept of terrorism from classical forms of political violence to its modern manifestations in the digital environment. The author reviews key approaches to the interpretation of terrorism in political science, international law, security studies and communication theories. It is determined that terrorism in the 21st century goes beyond traditional methods of physical influence, acquiring informational, psychological, ideological and technological dimensions. The chapter contains an analysis of the theoretical and methodological foundations of the study namely neorealism, constructivism, neo-institutionalism, the theory of hybrid warfare and cognitive communications. The methodology and source base for the study of terrorism are separately outlined: regulatory and legal documents, international agreements, scientific publications, analytical reports, empirical data and examples of real information operations. The conclusion of the chapter is the formation of a methodological basis for further analysis of information terrorism as a separate phenomenon.

The second chapter is devoted to revealing the essence, structural characteristics and mechanisms of information terrorism. The author proves that the events of September 11, 2001 became a turning point in the transformation of terrorism – it was then that the transition from physical violence to informational and digital forms of influence took place. In this context, the emergence of such phenomena as:

– media terrorism (use of mass media for intimidation, blackmail, propaganda);

– cyberterrorism (attacks on information infrastructure);

– symbolic terrorism (manipulation of images and symbols that influence mass consciousness) is analysed.

The mechanisms of informational influence such as the creation of fake narratives, the spread of panic, interference in communication networks, and the undermining of trust in governments and international organisations are investigated. The chapter concludes the conclusion that information terrorism is a systemic element of hybrid warfare, where information is used as a weapon to achieve political goals without the direct use of force.

The third chapter is aimed at understanding information warfare as the highest form of modern information conflict. It argues that information warfare and information terrorism are interrelated phenomena that operate in a single field of the global struggle for consciousness. The institutional characteristics of information warfare are considered and their main tools are highlighted: fake news, bot farms, cyberattacks, cognitive influences, and «information mirror» (imitation of alternative reality). Special attention is paid to information weapons as a system of unconventional pressure tools capable of achieving political effects comparable to military ones. An important innovation of this chapter is the introduction of the concept of information resilience as the antithesis of information terror.

It is argued that building resilience involves developing strategic communications, digital education, and media literacy as well as building a state system for responding to disinformation campaigns.

The chapter concludes the conclusion that information warfare is the main area of hybrid warfare in the 21st century where the struggle is for control over knowledge, narrative, and trust.

The fourth chapter is analytical and comparative in nature. It examines the national models of information security of the world’s leading countries such as the USA, the EU countries, Japan, China, India, as well as the countries of Africa and

Latin America. Comparative analysis allows us to identify different approaches to information control:

– the USA model focused on the balance between security and freedom of speech;

– the European model based on law, democracy and cyber-ethical responsibility;

– the Chinese model with an emphasis on state control and censorship;

– the Japanese model with the advantage of technological and preventive cyber protection;

– the African model with the development of information security systems that combine national stability with limited technological resources and international initiatives to increase digital resilience;

– the Latin American model with strengthening regional cooperation, combating disinformation, and promoting digital rights in a context of political polarization and uneven cyber governance.

The chapter also reveals the experience of countries of the Global South forming their own strategies for countering information threats within limited resources. Common features are identified namely the need for legal regulation, coordination between institutions, and increasing the digital literacy of the population. Based on this, a generalisation is made which allows us to determine the optimal elements for building a national model of information security of Ukraine.

The fifth chapter is of an applied and synthetic nature. It focuses on the Ukrainian case of countering information terrorism of the Russian Federation, which has become one of the largest examples of information warfare in the world. The stages, goals and tools of Russian information aggression against Ukraine since 2014 are analysed: the creation of fake narratives, propaganda campaigns, cyberattacks, influence operations in social networks, and undermining the international image of Ukraine. The following institutional responses of the state are studied such as the activities of the Centre for Countering Disinformation, cyber units, the Ministry of Digital Transformation, as well as the efforts of public initiatives and volunteer

networks. The author substantiates that the Ukrainian model of information resistance is based on a combination of state, media, civil and technological resources, which creates a new type of information defence.

Particular attention is paid to the formation of information resilience of society through increasing media literacy, developing strategic communications, state and public sector partnership, and Ukraine's participation in international initiatives of the EU and NATO.

The chapter concludes with the definition of promising directions of state policy in the field of countering information terrorism, including:

– improving legislation;

– developing information and analytical centres;

– strengthening cyber capabilities;

– forming Ukrainian narratives in the international space;

– integrating Ukrainian experience into global information security standards.

The conclusions summarise that information terrorism is a systemic threat to international and national security, which is transforming the modern architecture of global relations. It is proven that effective counteraction is possible only if the information resilience of the state, society, and the individual is formed. Ukrainian experience in this area has become a significant contribution to the development of a new security paradigm focused on democratic values, critical thinking, and digital awareness.

The practical significance of the results lies in the fact that they can be used in the development of state strategies in the field of information security, improving the legislative framework, forming a system of information education and strategic communications, as well as in the educational process in the disciplines of international security, political communications and cybersecurity.

Key words: information terrorism, information resilience, national security, international security, civil society, Russian-Ukrainian war, hybrid war, strategic communications, disinformation, EU, Ukraine, NATO, international organisations, conflicts.

СПИСОК ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації

Статті у виданнях, що індексуються у міжнародних наукометричних базах даних Scopus та Web of Science:

1. Vozniuk Ye., Kunytskyy M., Mykhaliuk N., Novak O. International Information Security. *AD ALTA: Journal of Interdisciplinary Research.* 2021. Vol. 11, Issue 01. P. 381–385. (авторський внесок 25%). **Web of Science, Scopus, Q3.**

DOI: 10.33543/1101.

URL: https://www.magnanimitas.cz/ADALTA/1101/papers/A_voznyuk.pdf.

2. Shuliak A., Vozniuk Ye., Patlashynska I. [et al.]. The Impact of the 4.0 Technological Revolution on the Hybrid War of the Russian Federation in Ukraine. *AD ALTA: Journal of Interdisciplinary Research.* 2022. Special Issue (12/02-XXX). P. 159–164. (авторський внесок 30%). **Web of Science, Scopus, Q3.**

DOI: 10.33543/1202.

URL: http://www.magnanimitas.cz/ADALTA/120230/papers/K_15.pdf.

3. Kachkovska L., Blahovirna N., Vozniuk Ye. [et al.]. Documentary-Information Communication in Public Administration: Legal Aspects and Digital Transformation. *International Journal of Basic and Applied Sciences.* 2025. 14 (3) P. 42–47. (авторський внесок 30%). **Scopus, Q4.**

DOI: 10.14419/v1jmq034.

URL: www.sciencepubco.com/index.php/IJBAS.

4. Shuliak A., Voznyuk Ye, Patlashinska I., Shuliak N. Info-Analytic Support for Ukrainian-Polish Cross-Border Cooperation: a Case Study of Euro-Regions. *Codrul Cosminului*. 2020. Issue 2. Vol. 26. P. 431–454, (авторський внесок 30%) **Scopus, Q2.**

DOI: 10.4316/CC.2020.02.007.

URL: https://codrulcosminului.usv.ro/article-7-vol-26-2-2020/

5. Kotsan N., Kopachinska G., Vozniuk Ye., Kotsan R. Basic Models of Protection and Functioning of the Ukrainian Border in Modern Geopolitical Realities: a View from Ukraine. *European Spatial Research and Policy*. 2022. Vol. 29. N. 1. P. 79–95. (авторський внесок 25%). **Web of Science**, **Scopus, Q2.**

DOI: 10.18778/1231-1952.29.1.04.

URL: https://czasopisma.uni.lodz.pl/esrap/article/view/9908.

Статті у наукових фахових виданнях України:

6. Vozniuk E. North Korea Nuclear Program as the Main Source of Instability in Northeast Asia. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2017. № 6 (355). С. 4–11.

URL: http://nbuv.gov.ua/UJRN/Nvvnum_2017_6_3.

7. Hych I., Vozniuk E. The Threats and Opportunities of Crisis on Ukraine's Accession to the EU. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2017. № 6 (355). С. 12–16. (авторський внесок 80%).

URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Nvvnum_2017_6_4.

8. Shimuleni M. S., Vozniuk E. Regional Integration and Development: a Theoretical Review of the SADC Region. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2017. № 10 (359). С. 111–116. (авторський внесок 80%).

URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21

REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Nvvnum_2017_10_21.

9. Vozniuk E. Principles and Features of Japan's Information Security System. *Політичне життя.* 2017. № 4. С. 8–12.

URL: https://jvestnik-politology.donnu.edu.ua/index.php/pl/article/view/4933.

10. Hrynchuk V., Vozniuk E. Information Security of India. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини.* 2018. № 1 (374). С. 15–20. (авторський внесок 75%).

11. Ничипорчук Н., Вознюк Є. Секрет успіху США у сфері інформаційної безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2018. № 1 (3). С. 66–71. (авторський внесок 75%).

DOI: 10.29038/2524-2679-2018-01-66-71.

URL: https://relint.vnu.edu.ua/index.php/relint/article/view/28.

12. Vetrov K., Voznyuk Ye. Information Terrorism as a Modern Threat for Information Security of European States. *Міжнародні відносини, суспільні комунікації та регіональні студії*, 2019. № 1 (5). С. 34–42. (авторський внесок 80%).

DOI: 10.29038/2524-2679-2019-01-34-41.

URL: https://relint.vnu.edu.ua/index.php/relint/article/view/88.

13. Вознюк Є. Поширення впливу мексиканських картелів засобами інформаційних технологій і пропаганди. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини.* 2019. № 8 (392). С. 35–41.

URL: https://evnuir.vnu.edu.ua/bitstream/123456789/22741/1/35-41.pdf.

14. Бекеша О., Матюшок В., Вознюк Є. Розвиток кібербезпеки Бразилії на сучасному етапі. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2020. № 2 (406). С. 52–58. (авторський внесок 70%).

URL: https://evnuir.vnu.edu.ua/bitstream/123456789/22730/1/%d0%9d%d0%92_%d0%9c%d0%92_2020_2-52-58.pdf.

15. Вознюк Є., Романцов Д., Рошко І. Кібербезпека в умовах російської агресії. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2020. № 2 (406). С. 58–66. (авторський внесок 70%)

URL: https://evnuir.vnu.edu.ua/handle/123456789/22733.

16. Вознюк Є. Громадські об'єднання на захисті інформаційного простору України. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2021. № 3 (11). С. 48–61.

DOI: 10.29038/2524-2679-2021-03-48-61.

URL: https://relint.vnu.edu.ua/index.php/relint/article/view/230.

17. Вознюк Є. Особливості поширення російських фейків в Україні. *Історико-політичні проблеми сучасного світу: зб. наук. ст*. Чернівці: Чернівец. нац. ун-т, 2021. Т. 44. С. 52–63.

URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Ippss_2021_44_8.

18. Вознюк Є. SWOT-аналіз стану інформаційної безпеки України. *Науковий часопис НПУ імені М. П. Драгоманова. Серія 22: Політичні науки та методика викладання соціально-політичних дисциплін.* 2021. 22 (30). С. 116–124.

DOI: 10.31392/pnspd.v22i30.1147

URL: https://sj.udu.edu.ua/index.php/pnspd/article/view/116-129.

19. Вознюк Є., Андрюхіна В. Порівняльний аналіз кібербезпеки Європейського Союзу. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2025. № 2 (22). С. 161–180. (авторський внесок 75%).

DOI: 10.29038/2524-2679-2025-02-136-154.

URL: https://relint.vnu.edu.ua/index.php/relint/article/view/454.

20. Kachkovska L., Vozniuk Ye. Countering Information Threats in Ukraine: Current Issues for Solving at the State Level. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2024. № 1 (18). С. 85–102. (авторський внесок 60%)

DOI: 10.29038/2524-2679-2024-01-85-102.

URL: https://relint.vnu.edu.ua/index.php/relint/article/view/367.

Статті в іноземних журналах:

21. Novak O., Vozniuk Ye. The Influence of the Information Society Development on Political Ideologies. *Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate.* 2021. 11 (1). P. 19–26. (авторський внесок 70%)

DOI: 10.24917/26578549.11.1.2.

URL: https://studiadesecuritate.uken.krakow.pl/wp-content/uploads/sites/43/2021/06/2_Novak_Vozniuk.pdf.

22. Morenchuk A., Vozniuk Ye., Morenchuk A. junior Sources of Russian Policy Aggressiveness. *Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate*. 2024. 14 (1). P. 91–105. (авторський внесок 60%)

DOI: 10.24917/26578549.14.1.5.

URL: https://studiadesecuritate.uken.krakow.pl/wp-content/uploads/sites/43/2025/04/5.-Andriy-Morenchuk.pdf.

23. Bairak S., Buslenko V., Vozniuk Ye. State Policy in the Field of Information Security Providing in Ukraine. *Annales Universitatis Paedagogicae Cracoviensis*. *Studia de Securitate.* 2024. 14 (1). P. 107–117. (авторський внесок 35%)

DOI: 10.24917/26578549.14.1.6

URL: https://studiadesecuritate.uken.krakow.pl/wp-content/uploads/sites/43/2025/04/6.-Serhii-Bairak.pdf.

Розділи у монографіях:

24. Vozniuk E. Information Terrorism as a Modern Dynamic Part of International Terrorism. *International and National Security: Politics, Information, Ecology, Economy: collective monograph* / ed. by A. Mytko. Kyiv: MPBP «Hordon», 2018. P. 165–174. 320 p.

ISBN 978-966-8398-55-1

URL: https://evnuir.vnu.edu.ua/handle/123456789/23755

25. Вознюк Є. Європейський інспектор із захисту даних. *Зелений і безпечний Європейський Союз: монографія* / [А. О. Бояр (кер. авт. кол.), І. В. Кицюк, Н. І. Романюк та ін.]; за ред. А. О. Бояра, В. Й. Лажніка. Луцьк: Вежа-Друк, 2023. С. 82–85.

ISBN 978-966-940-505-0,

URL: d084d0a1-d0bad0bdd0b8d0b3d0b0_final.pdf (wordpress.com).

Наукові праці,
які засвідчують апробацію матеріалів дисертації:

26. Підлісний А. Ю., Вознюк Є. В. Участь України у миротворчих операціях НАТО. *Актуальні проблеми країнознавчої науки:* матеріали ІІ Міжнар. наук.-практ. інтернет-конференції (м. Луцьк, 14–15 травня 2015 р.) / за ред. В. Й. Лажніка. Луцьк: Вежа-Друк, 2015. С. 187–189.

27. Подолець С. В., Вознюк Є. В. Особливості забезпечення сучасної інформаційної безпеки держави. *Проблеми і перспективи практичної реалізації наукових досліджень:* матеріали XXXVI Міжнар. наук.-практ. конф., Чернівці, 15–16 берез. 2016 р. Т. 2. Київ: Наук.-вид. центр «Лабораторія думки», 2016. С. 31–33.

28. Voznyuk E. V., Voinkova A. O. The Features of Providing Information Security of European Countries. *Актуальні проблеми регіональних досліджень*: матеріали І Міжнар. наук.-практ. інтернет-конференції (м. Луцьк, 11–12 груд. 2017 р.) / за ред. В. Й. Лажніка. Луцьк: Вежа-Друк, 2017. С. 236–240.

29. Ничипорчук Н. С., Вознюк Є. В. Нормативно-правове регулювання інформаційної безпеки США. *Проблеми та перспективи наукових досліджень:* матеріали LX Міжнар. наук.-практ. конф. (Чернівці, 15–16 червня 2018 р.). Київ: Науково-видавничий центр «Лабораторія думки», 2018. С. 28–30.

30. Джигалюк Н., Вознюк Є. Особливості стратегічних комунікацій у німецькомовному інформаційному просторі з точки зору національної безпеки України. *Інформаційна війна як новий вимір геополітичної ривалізації:* матеріали ІІ міжнар. наук.-практ. конф. Луцьк, 2019. С. 8-12

31. Вознюк Є. В. Особливості політичної комунікації сьогодні. *Міжнародні та регіональні системи: актуальні питання міжнародних відносин і регіональних студій*: зб. тез Міжнар. наук-практ. конф. (м. Луцьк, 17 трав. 2019 р.) / за ред. В. Й. Лажніка та С. В. Федонюка. Луцьк: Вежа-Друк, 2019. С. 96–98.

32. Вознюк Є., Дідух Д. Ботоферми як загроза інформаційній безпеці. *Інформаційна гігієна як напрям національної безпеки*: матеріали І міжнар. наук. онлайн-конф. Луцьк, 2021. С. 23–25.

33. Horbach A., Vozniuk Ye. Influence of Non-Governmental Organizations on Information Security of Ukraine. *Актуальні проблеми міжнародних відносин і регіональних досліджень*: матеріали Міжнар. наук.-практ. інтернет-конф. (м. Луцьк, 6 груд. 2021 р.) / за ред. В. Й. Лажніка. Луцьк: Вежа-Друк, 2021. С. 167–170.

URL: https://wiki.vnu.edu.ua/images/d/df/%D0%9A%D0%9E%D0%9D%D0%A4-2021-%D0%B3%D1%80%D1%83%D0%B4.pdf.

34. Шуляк А., Вознюк Є. Інформаційна сингулярність російсько-української війни 2022 р. *Стратегічні комунікації в контексті безпекової політики: європейський і глобальний рівні*: матеріли інтернет-конф. / за заг. ред. Н. Карпчук. Луцьк: ВНУ ім. Лесі Українки, 2022. С. 67–72.

URL: https://inter-dep.vnu.edu.ua/wp-content/uploads/2022/06/%D0%9C%D0%B0%D1%82%D0%B5%D1%80-%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80-19.05.22.pdf

35. Вознюк Є., Крищук А. Початок активного російсько-українського протистояння в кіберпросторі. *Мультидисциплінарні підходи до аналізу суспільно-політичних проблем в умовах російсько-української гібридної війни*: матеріали. міжнар. круглого столу (28 квіт. 2022 р.). Львів: Вид-во Львів. політехніки, 2022. С. 18–21.

URL: https://lpnu.ua/sites/default/files/2022/6/24/news/20253/tpp-verstkatezikrugliystil2022-1.pdf.

36. Baranyk O. S., Vozniuk Ye. V. Global Impact of Information Weapons. *Актуальні проблеми міжнародних відносин і регіональних досліджень:* матеріали III Міжнар. наук.-практ. інтернет-конф. (м. Луцьк, 15 лист. 2023 р.) / укладачі: С. Кулик; О. Борисюк (технічна підтримка). Луцьк: Волин. нац. ун-т ім. Лесі Українки, 2024. С. 250–253.

37. Вознюк Є. Кібербезпека Європейського Союзу: інституційна архітектура та сучасні виклики. *Зовнішнє інформаційне маніпулювання та втручання в умовах сучасних конфліктів*: матеріли інтернет-конф. / за заг. ред. проф. Н. Карпчук. Луцьк: ВНУ ім. Лесі Українки, 2025. С. 106–110.

URL: https://fimieu.wordpress.com/%d0%ba%d0%be%d0%bd%d1%84%d0%b5%d1%80%d0%b5%d0%bd%d1%86%d1%96%d1%97/

38. Завадська В., Вознюк Є. Інформаційна та кібербезпека країн Африки. *Європейська інтеграція України: виклики, досвід, перспективи:* матеріали міжнар. наук.-практ. конф. (Луцьк, 21 трав. 2025 р.) / за заг. ред. С. Федонюка. Луцьк: ВНУ ім. Лесі Українки, 2025. С. 76–79

URL: https://euaccession.wordpress.com/wp-content/uploads/2025/06/d09ad09ed09dd0a4d095d0a0d095d09dd0a6d086d0af-euaccession-2025-1-1.pdf

Наукові праці,

які додатково відображають наукові результати дисертації:

39. Khoma N. Vozniuk E Turkey's Middle East Policy: Vectors, Aims and Results *Studia Politica. Romanian Political Science Review.* Vol. XXI, No. 2, 2021. P. 577-601. **Scopus, Q4**

URL: https://www.researchgate.net/profile/Nataliya-Khoma-2/publication/361182581_Turkey's_Middle_East_Policy_Vectors_Aims_and_Results_Studia_Politica_Romanian_Political_Science_Review_2021_Vol_XXI_No_2_R_578-601/links/62a18d4bc660ab61f86df60a/Turkeys-Middle-East-Policy-Vectors-Aims-and-Results-Studia-Politica-Romanian-Political-Science-Review-2021-Vol-XXI-No-2-R-578-601.pdf.

40. Kotsan R., Kotsan N., Kopachinska G. Vozniuk E Transformations of Ukrainian-Polish border regions transformation: experience of Ukraine. *Forum Geographic* Vol. 21, Issue 1, 2022, pp. 92-101. ***Web of Science***

DOI 10.5775/fg.2022.071.i.

URL: http://forumgeografic.ro/wp-content/uploads/2022/1/Kopachinska.pdf

41. Кулик С., Вознюк Є. Фейк російської пропаганди: Олена Підгрушна – снайпер АТО. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2021. № 1 (9). С. 83–101. ***Фахове видання України.***

DOI: 10.29038/2524-2679-2021-01-82-101

URL: https://relint.vnu.edu.ua/index.php/relint/uk/article/view/125.

42. Вознюк Є. Війна свідомості (консцієнтальна війна), гібридні загрози, інформаційна війна, інформаційний омбудсмен, інформаційний тероризм, культура інформаційної безпеки, методи боротьби з інформацією в електронних засобах масової інформації, операційна безпека «OPSEC». *Глосарій: навчальний енциклопедичний словник-довідник з питань інформаційної безпеки* / за заг. ред. д-ра. політ. наук, проф. А. М. Шуляк, 2019. С. 42–45; 54–56; 135–138; 165–166; 168–170; 242–244; 289–293; 343–345.

43. Wozniuk E. Informacyjny ombudsman; Metody walki z informacją w elektronicznych środkach masowego przekazu. *Vademecum bezpieczeństwa informacyjnego* / red. nauk. Olga Wasiuta, Rafał Klepka. T. 1. Kraków: AT Wydawnictwo, Wydawnictwo LIBRON – Filip Lohner, 2019. P. 452–454, 647–651.

44. Wozniuk E. Terroryzm informacyjny. *Vademecum bezpieczeństwa informacyjnego* / red. nauk. Olga Wasiuta, Rafał Klepka. T. 2. Kraków: AT Wydawnictwo, Wydawnictwo LIBRON – Filip Lohner, 2019. P. 466–468.

ЗМІСТ

ВСТУП……..……26

РОЗДІЛ 1. ДОСЛІДЖЕННЯ ТЕРОРИЗМУ В КОНТЕКСТІ СУЧАСНИХ МІЖНАРОДНИХ ВІДНОСИН…….45

1.1.Генеза та концептуалізація поняття «тероризм» у політологічному дискурсі…….....45

1.2.Теоретико-методологічні підходи до аналізу глобалізаційних і цифрових трансформацій тероризму……..…62

1.3.Методологія та джерельна база дослідження тероризму в контексті міжнародної безпеки…….……73

Висновки до Розділу 1……..87

РОЗДІЛ 2. ІНФОРМАЦІЙНИЙ ВИМІР ТЕРОРИЗМУ В ГЛОБАЛЬНОМУ СЕРЕДОВИЩІ БЕЗПЕКИ ……..……90

2.1. Події 11 вересня 2001 р. як детермінанта цифрової трансформації тероризму…….....90

2.2. Інформаційний тероризм у структурі сучасного міжнародного тероризму: сутність, механізми, прояви ……..…….…….……..99

2.3. Інформаційний тероризм як компонент інформаційної війни……..……..……..119

Висновки до Розділу 2……..……..150

РОЗДІЛ 3. ІНФОРМАЦІЙНА ВІЙНА ЯК ФОРМА ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОТИСТОЯННЯ……..……152

3.1. Інформаційний тероризм у системі інформаційних війн: взаємозв’язки та інституціональні характеристики …….……152

3.2. Інформаційна війна та інформаційна зброя: функції, цілі, інструменти впливу ……..…165

3.3. Формування інформаційної стійкості як напряму протидії інформаційному тероризму ……..…..…187

Висновки до Розділу 3……...……..211

РОЗДІЛ 4. ПОРІВНЯЛЬНИЙ АНАЛІЗ НАЦІОНАЛЬНИХ СТРАТЕГІЙ ПРОТИДІЇ ІНФОРМАЦІЙНОМУ ТЕРОРИЗМУ……...213

4.1. Нормативно-інституційні засади забезпечення інформаційної безпеки та кіберстійкості в США і ЄС…….…213

4.2. Моделі державного інформаційного контролю: порівняльний аналіз практик Китаю, Японії та Індії……....239

4.3. Національні стратегії протидії інформаційному тероризму в країнах Африки та Латинської Америки: регіональні особливості……..273

Висновки до Розділу 4……...……..301

РОЗДІЛ 5. Протидія України інформаційному тероризму РФ: виклики, досвід та перспективи……303

5.1. Інформаційна агресія Російської Федерації проти України: етапи, цілі, інструменти впливу…….……303

5.2. Стратегічні напрями удосконалення державної політики протидії інформаційному тероризму в Україні…….…….…….319

5.3. Роль інститутів громадянського суспільства у формуванні системи інформаційного захисту держави ……..345

Висновки до Розділу 5……...……..367

ВИСНОВКИ……...……..……..370

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……..……384

ДОДАТКИ……..……....443

ВСТУП

Актуальність дослідження. Актуальність дослідження проблематики інформаційного тероризму в контексті міжнародної безпеки зумовлюється постійним зростанням загроз інформаційному суверенітету держави, що потребує дедалі більше зусиль для його захисту. У цьому контексті державна інформаційна політика постає ключовим елементом як зовнішньої, так і внутрішньої політики, охоплюючи всі сфери функціонування суспільства. Стрімкий розвиток інформаційного простору супроводжується виникненням нових, раніше невідомих викликів, що безпосередньо впливають на інтереси особистості, суспільства та держави, а також становлять загрозу її національній безпеці. В умовах інформаційної епохи, позначеної масштабними інформаційними війнами й активним використанням цифрових комунікаційних технологій, питання забезпечення інформаційної безпеки набуває особливої значущості.

Замість очікуваної відкритості політичного процесу, сучасна інформаційна революція призвела до зростання неконтрольованих потоків інформації, де правдивість і точність повідомлень часто залишаються поза перевіркою. Це створює широкі можливості для маніпуляцій, особливо з боку медіа. Інтернет-простір перетворився на арену поширення політичних меседжів, дезінформації, викривлених фактів про діяльність лідерів та результати перемовин. Усе це потребує від авторів інформаційних кампаній постійного моніторингу й оперативного реагування. Медіа стали фактично новою гілкою влади – «віртуальною», – що, завдяки своїй мобільності, оперативності та глибині впливу, переважає традиційні гілки влади. Політичне протистояння дедалі більше переміщується у сферу інформаційного простору, набуваючи нових посттрадиційних форм.

У сучасній політичній науці дослідники, які аналізують інформаційні процеси та проблеми забезпечення інформаційної безпеки, наголошують на необхідності переосмислення підходів до державної інформаційної політики в

умовах тотального інформаційного впливу. Науковці підкреслюють важливість розробки системної концепції інформаційного управління, що передбачає чітке планування й реалізацію стратегій, спрямованих на мінімізацію ризиків, попередження кризових ситуацій і подолання зростаючої інформаційної нерівності між розвиненими країнами та державами, що розвиваються. Динаміка політичних і соціальних трансформацій, характерна для постіндустріальної доби, стимулює дослідників епохи інформаційного суспільства до переосмислення глобальних структур управління. У цьому контексті все частіше йдеться про формування нового типу світової спільноти, заснованого на принципах мережевої взаємодії між державними інститутами та громадянським суспільством.

Інформаційний тероризм – це новітня форма терористичної діяльності, спрямована на дестабілізацію суспільств через дезінформацію, маніпуляції, паніку або кібернапади. Він є частиною гібридних війн і дедалі частіше використовується не лише терористичними угрупованнями, а й окремими державами для досягнення політичних цілей. На відміну від класичного терору, який впливає на фізичну безпеку, інформаційний терор б’є по свідомості, руйнуючи довіру до інституцій, провокуючи хаос і послаблюючи стійкість держав. Особливо небезпечним він стає під час воєн, криз та виборів, коли суспільства вразливі до фейків і пропаганди. Приклади втручання в інформаційний простір США, ЄС та України свідчать про масштабність цієї загрози. Отже, протидія інформаційному терору потребує нових механізмів – цифрової грамотності, кіберзахисту, міжнародної співпраці й підвищення критичного мислення в суспільстві, інформаційної стійкості.

У межах теорії міжнародних відносин інформаційний тероризм розглянуто як одну із загроз нетрадиційного характеру, що дестабілізують глобальну безпеку без застосування традиційної військової сили. Його суть полягає в цілеспрямованому поширенні дезінформації, маніпулятивному впливі на масову свідомість, утручанні в інформаційні системи держав, інституцій та громад із метою посіяти паніку, підривати довіру до урядів,

викликати соціальні заворушення або змусити до політичних рішень, вигідних агресору. На відміну від класичного тероризму, який використовує фізичне насильство, інформаційний тероризм діє через символічне насильство, підрив легітимності, поширення страху й руйнування ціннісних систем. Згідно з конструктивізмом, інформаційний тероризм – це боротьба за контроль над інтерпретацією реальності, за домінування певного наративу в глобальному дискурсі. У реалізмі – це інструмент державного чи недержавного впливу для зміни балансу сил у свою користь. Інформаційний тероризм є складовою частиною гібридної війни, а також інструментом «м'якої сили навпаки», коли, замість приваблення через культурну дипломатію, використовуються засоби підриву й деморалізації. Його впливи можуть бути спрямовані на делегітимацію інституцій, зниження міжнародної підтримки певної країни, посилення внутрішніх протиріч. Отже, у сучасній теорії міжнародних відносин інформаційний тероризм – це міждисциплінарний феномен, що поєднує елементи безпекових студій, теорій комунікації, психології, міжнародного права й глобальної політики, потребуючи нових підходів до аналізу та протидії.

Дослідження інформаційного тероризму є актуальним у контексті зростання гібридних загроз, оскільки це явище становить серйозну небезпеку для політичної стабільності, громадської безпеки й функціонування демократичних інститутів. Його вивчення дає змогу глибше зрозуміти механізми деструктивного впливу на свідомість суспільства, удосконалити нормативно-правову базу та розробити ефективні стратегії протидії.

У контексті російсько-української війни з 2014 р. інформаційний тероризм набув особливої актуальності як інструмент психологічного впливу, дезінформації й маніпуляції громадською думкою як в Україні, так і за її межами. Масовані інформаційні атаки супроводжують воєнні операції, спрямовані на деморалізацію населення, підрив довіри до державних інституцій та дестабілізацію внутрішньополітичної ситуації. Вивчення цього

явища потрібне для посилення інформаційної стійкості України й формування ефективної системи протидії ворожим інформаційним кампаніям.

Дисертацію виконано в рамках науково-дослідних робіт факультету міжнародних відносин ВНУ ім. Лесі Українки, а саме: «Актуальні проблеми формування та розвитку європейського інформаційного простору» (2010–2012 рр.), «Інформація та комунікація в сучасному світі» (2012–2014 рр.) (держреєстраційний №0112U001779); держбюджетної теми «Інформаційна підтримка транскордонного співробітництва України» (2013–2015 рр.) (держреєстраційний №0113U002221); 2018–2019 рр. – НДР «Інформаційна війна як новий вимір геополітичної ривалізації» згідно з наказом Міністерства освіти і науки України від 25.06.2018 р. № 695»; «Про фінансування спільних українсько-польських науково-дослідних проектів у 2018 р.» (співвиконавець – Інститут наук про безпеку Краківського педагогічного університету ім. Національної освітньої комісії) (держреєстраційний №0119U001621), а також міжнародних грантових проєктів програми ERASMUS+ напряму Модуль Жана Моне: 2022–2025 рр. – «Стратегічні комунікації ЄС: протидія деструктивним впливам»; 2024–2027 рр. – «EU Counteraction to FIMI» (№101172342 ERASMUS-JMO-2024-MODULE).

Мета й завдання дослідження. Мета дослідження – комплексний аналіз інформаційного тероризму як феномену сучасної системи безпеки – його теоретико-методологічних засад, форм і механізмів прояву, впливу на національну та міжнародну безпеку, а також вивчення практик протидії на глобальному, регіональному й національному рівнях.

Відповідно до поставленої мети сформульовано такі **завдання:**

1. Проаналізувати еволюцію концепту тероризму в теорії міжнародних відносин, розглянути різні термінологічні та концептуальні підходи до його тлумачення, зокрема в контексті глобалізаційних викликів і багатовимірності явища.

2. Систематизувати наукову та джерельну базу досліджень тероризму й антитероризму, виявити особливості інтерпретації проблематики в академічному та експертному дискурсах.

3. Визначити сутність і типологію інформаційного тероризму як складової частини міжнародного тероризму, дослідити такі його прояви, як медіатероризм і кібертероризм, ін.

4. Розкрити зміст категорії міжнародної інформаційної безпеки, охарактеризувати її складові частини, уключаючи національний рівень захисту інформаційного простору.

5. Дослідити характер і структуру сучасних інформаційних війн, зокрема гібридного типу, а також їхні ключові форми: iWar, війна четвертого покоління, асиметрична та посередницька війни, медіавійна.

6. Проаналізувати основні виклики й загрози міжнародній інформаційній безпеці в цифрову епоху, зокрема роль соціальних медіа, ботоферм і маніпулятивного контенту в умовах інформаційного терору.

7. Визначити інструменти, механізми та практики протидії інформаційному тероризму, уключаючи роль мас-медіа, омбудсменів, цифрових регуляторів і державних ініціатив.

8. Проаналізувати досвід окремих держав світу (США, країни ЄС, Японія, КНР, Індія, країни Африки, Латинської Америки тощо) в протидії кібер- та інформаційному тероризму й забезпеченні інформаційної безпеки.

9. Оцінити стан і виклики інформаційної безпеки в Україні в умовах війни з російською федерацією, зокрема в частині інституційного забезпечення, медіаполітики, кіберзахисту та протидії російській дезінформації.

10. Розробити рекомендації щодо зміцнення інформаційної стійкості до інформаційних загроз з урахуванням міжнародного досвіду й специфіки інформаційної війни в українському контексті.

Об’єкт дослідження – система міжнародної безпеки в умовах інформаційної епохи. **Предметом дослідження** є феномен інформаційного

тероризму як форми деструктивного інформаційного впливу та його дія на безпекове середовище сучасних держав і міжнародних інституцій.

Хронологічні рамки дослідження Хронологічні рамки дослідження охоплюють період із початку 2000-х років до 2024 р., що спричинено динамікою розвитку інформаційного простору та появою якісно нових загроз у цифрову добу. Нижня межа обумовлена тим, що саме на початку XXI ст. відбуваються інституціоналізація поняття інформаційної безпеки, формування перших міжнародних стратегій кіберзахисту, а також поява концепту «інформаційного тероризму» як окремого явища в системі глобальної безпеки. Цей період характеризується поступовим переходом від класичних форм інформаційного впливу до високотехнологічних, гібридних і мережевих практик, що поєднують політичні, психологічні та кіберінструменти. Верхня межа – 2024 р. – обрана як умовна, оскільки саме тоді простежено найвищий рівень інтенсивності інформаційних протистоянь, зокрема в контексті триваючої російсько-української війни, яка стала епіцентром глобальної боротьби за контроль над інформаційним простором. Водночас, процес дослідження феномену інформаційного тероризму є тривалим і незавершеним, адже розвиток цифрових технологій, штучного інтелекту та інформаційних платформ постійно змінює його форми, масштаби й наслідки. Це зумовлює потребу в подальшому міждисциплінарному аналізі та уточненні наукових підходів до оцінки інформаційних загроз і формування ефективних механізмів інформаційної стійкості.

Гіпотеза дослідження ґрунтується на міждисциплінарному поєднанні теорій неореалізму, конструктивізму та неоінституціоналізму, які дають змогу осмислити інформаційний тероризм як нову форму політичного насильства, що постає на перетині безпеки, технологій і комунікації. Це випливає із припущення, що у XXI ст. війна, насильство та агресія набувають нематеріального, когнітивного характеру, а головною ареною боротьби стає не територія, а інформаційний простір. Інформаційний тероризм у такому розумінні є структурним чинником трансформації міжнародної безпеки. Його

деструктивна сила полягає не у фізичному знищенні, а в підриві довіри, делегітимації політичних інститутів і руйнуванні наративів, на яких ґрунтується соціальна єдність. Загострення глобальної конкуренції, гібридизація міжнародних конфліктів та стрімкий розвиток цифрових технологій зумовили появу нового виміру політичної боротьби – інформаційно-терористичного, у межах якого інформація використовується як інструмент примусу, тиску й маніпуляції. У цьому контексті особливого значення набуває концепт інформаційної стійкості, який розглянуто як ключову умову протидії інформаційному тероризму. Саме розвиток інформаційної стійкості держави, суспільства та особистості – через формування критичного мислення, стратегічних комунікацій, цифрової безпеки й довіри до інституцій – стає визначальним чинником збереження національної ідентичності та стабільності міжнародного порядку в добу гібридних загроз.

Отже, гіпотеза дисертації має системний, політико-інституційний характер й виходить із розуміння, що інформаційний тероризм є новим типом глобальної загрози, який не лише підриває національну безпеку, а й трансформує всю архітектуру міжнародних відносин. Рівень інформаційної стійкості, своєю чергою, є новим виміром політичної могутності держави – поряд із військовим, економічним і дипломатичним потенціалами. Отже, стійка держава XXI ст. – це не лише озброєна чи економічно сильна, а й передусім, інформаційно захищена держава, спроможна зберегти свій суверенітет, ідентичність і довіру громадян у цифровому світі.

Методи дослідження. Дослідження інформаційного тероризму здійснено на основі комплексного методологічного підходу, який передбачає інтеграцію загальнонаукових, спеціально-наукових і міждисциплінарних методів аналізу. Серед загальнонаукових методів ключове значення мають аналіз та синтез, що використані для виокремлення основних складових частин феномену інформаційного тероризму (змістових характеристик, форм реалізації, інструментарію впливу) і їх узагальнення у формі цілісної концептуальної

моделі. Методи індукції й дедукції дали змогу здійснити перехід від емпіричного аналізу окремих випадків до формулювання загальних закономірностей, а також перевірки теоретичних гіпотез на прикладах із реальної практики. Методологічний інструментарій також уключав класифікацію та типологізацію, що сприяли систематизації видів інформаційного тероризму (зокрема медіа- й кібертероризму), форм інформаційного впливу та методів протидії.

До спеціально-наукових методів політичної науки й міжнародних відносин належить метод порівняльного аналізу, який забезпечив можливість зіставлення національних стратегій боротьби з інформаційним тероризмом у різних країнах (зокрема в США, Франції, Китаї, Польщі, Японії, Україні). Інституціональний аналіз дав змогу оцінити роль державних і міжнародних інституцій у формуванні політики інформаційної безпеки, тоді як метод аналізу політики використано для дослідження нормативно-правових документів, стратегій кібербезпеки та інформаційних доктрин у контексті їх ефективності.

У межах міждисциплінарного підходу застосовано дискурс-аналіз для вивчення наративів, фейкових повідомлень, пропагандистських практик і відповідей на них із боку офіційних джерел; контент-аналіз, який дав змогу ідентифікувати змістові, структурні та емоційні характеристики повідомлень, пов’язаних з інформаційним терором, насамперед у соціальних мережах і цифрових медіа; метод case study – для глибокого аналізу конкретних випадків інформаційних атак (утручання у вибори, кампанії дезінформації, хакерські атаки, діяльність ботоферм). Історико-ретроспективний метод дав змогу простежити еволюцію концептів тероризму, інформаційної безпеки та інформаційного тероризму в міжнародному дискурсі, а також проаналізувати трансформацію відповідних загроз у XX–XXI ст.

Окрему групу становлять емпіричні методи, зокрема моніторинг відкритих джерел (OSINT), який уключав аналіз наукових публікацій, матеріалів медіа, звітів міжнародних організацій, баз даних й офіційних

ресурсів урядових і міжурядових структур. Статистичний метод використано для обробки кількісних даних щодо масштабів поширення інформаційних атак, кіберзагроз, дезінформаційних кампаній та інших форм інформаційного терору.

Отже, дослідження ґрунтується на поєднанні якісного й кількісного підходів, що забезпечує комплексне осмислення феномену інформаційного тероризму та дає змогу здійснити як глибокий теоретичний аналіз, так і практичну оцінку актуальних загроз на національному й міжнародному рівнях.

Наукова новизна одержаних результатів. У процесі дослідження здобуто результати, новизна яких конкретизується в таких положеннях:

Уперше:

– запропоновано концептуалізацію поняття інформаційної стійкості. У сучасних умовах гібридної війни та інформаційної конфронтації дедалі більшого значення набуває цей концепт, який розглядається як ключова складова частина національної безпеки й соціальної згуртованості. Під інформаційною стійкістю розуміємо спроможність держави, інституцій і громадянського суспільства протистояти зовнішнім та внутрішнім інформаційним загрозам, уключаючи дезінформацію, маніпуляції, пропаганду й інші форми інформаційного впливу, що мають на меті дестабілізацію політичного, соціального або культурного середовища. Інформаційна стійкість є комплексним міждисциплінарним феноменом, який уключає технічні, організаційні, нормативно-правові, освітні та психологічні складові частини;

– запропоновано концептуальні напрями модернізації Закону України «Про боротьбу з тероризмом», що відображають трансформацію терористичних загроз у цифрову добу. Запропоновано ввести до національного законодавства категорію «інформаційна стійкість» як ключовий індикатор безпеки й розширити суб’єктний склад боротьби з тероризмом через закріплення правового статусу неурядових структур у сфері

інформаційного захисту. Наукову новизну становить також розширення термінологічного апарату антитерористичного законодавства шляхом уведення до нормативного поля нових дефініцій, як-от: інформаційний тероризм, кібертероризм, інформаційно-психологічна операція (ІПсО). Уточнення цих понять створює правову основу для визнання інформаційних і кібернетичних атак формами терористичної діяльності, що дає змогу розширити коло об'єктів та суб'єктів безпеки, підвищити ефективність моніторингу, кваліфікації й запобігання сучасним загрозам у гібридному середовищі;

– обґрунтовано новий підхід до протидії інформаційному тероризму, що полягає у виокремленні та теоретичному узагальненні трикомпонентної моделі забезпечення інформаційної стійкості, яка охоплює стратегічні комунікації (як інструменту консолідації національного наративу, формування довіри до держави й нейтралізації ворожих інформаційних операцій), медіаосвіту (як чинника формування критичного мислення, інформаційної гігієни та спроможності до самостійної ідентифікації інформаційних загроз) і цифрову безпеку (як складову частину інформаційної оборони держави, що включає технологічні та організаційні засоби кіберзахисту, у тому числі на основі національного й міжнародного співробітництва). Уперше здійснено системний аналіз взаємозв'язку між стратегічними комунікаціями, медіаосвітою та цифровою безпекою як ключовими інструментами у структурі національної й міжнародної інформаційної безпеки;

– здійснено комплексне міждисциплінарне дослідження міжнародного тероризму в умовах глобалізації, у якому запропоновано нову концептуалізацію інформаційного тероризму як автономного феномену, що поєднує риси когнітивної війни, кібертерору та ідеологічної агресії. Визначено інституційні, цивілізаційні й правові аспекти інформаційної агресії; виявлено її вплив на структури міжнародної безпеки, політичну стабільність і правовий режим міжнародного гуманітарного права. Обґрунтовано необхідність

перегляду засад міжнародного права та безпеки в контексті викликів інформаційної епохи;

– здійснено аналіз унікального українського досвіду протидії інформаційному тероризму в умовах повномасштабної гібридної агресії, що триває з 2014 р. та інтенсифікувалася після 2022 р. Уперше на основі системного підходу досліджено, як держава, перебуваючи в умовах постійного зовнішнього інформаційного тиску, змогла сформувати цілісну модель інформаційного спротиву, що поєднує інституційні, технологічні, суспільні й дипломатичні інструменти. У роботі обґрунтовано такі нові компоненти української інформаційної стійкості, як алгоритмічна протидія фейкам, мобілізація цифрового громадянського суспільства (зокрема волонтерських ініціатив, кіберспротиву), які ще не були належно осмислені в науковій літературі. Досвід України розглянуто як перспективну модель, що вже частково імплементується в політики безпеки ЄС, НАТО й окремих країн. Запропоновано авторське бачення українського кейсу як джерела універсальних рішень, придатних до адаптації в інших регіонах, які зазнають інформаційного терору. У цьому контексті акцентовано на необхідності міжнародно-правової інституалізації механізмів боротьби з інформаційним тероризмом з урахуванням українського внеску як одного з головних орієнтирів для формування глобальної стратегії цифрової безпеки;

– запропоновано нову інтерпретацію терористичних атак 11 вересня 2001 р. не лише як воєнного виклику, але як і переломного моменту в трансформації глобальної парадигми безпеки, що започаткував якісно нову еру інформаційно-психологічного, асиметричного й неконвенційного протиборства. Переосмислено роль подій 11 вересня як тригера для еволюції нових типів конфліктів – від традиційного терору до інформаційних та проксі-війн. Доведено, що гасло «боротьби з тероризмом» стало основою для формування нових стратегічних доктрин, які легітимізували втручання в інші країни поза рамками колективної безпеки.

Дістали подальшого розвитку:

– твердження стосовно особливого значення інформаційної стійкості в контексті протидії інформаційним операціям іноземних держав, що можуть впливати на демократичні процеси, створювати соціальну напругу, підривати легітимність влади й дезорієнтувати громадянське суспільство. Отже, інформаційна стійкість є важливою передумовою національного суверенітету в умовах цифрової епохи;

– теза про те, що громадянське суспільство в Україні стало ключовим суб'єктом протидії інформаційним загрозам, особливо після початку російської агресії у 2014 р. Доведено, що ініціативи громадських організацій заповнили прогалини в державному управлінні інформаційною безпекою, запровадили нові практики OSINT-розвідки, цифрового моніторингу, протидії дезінформації й підвищення медіаграмотності. На тлі гібридної війни роль громадянського сектору у сфері інформаційної безпеки зростає. Його залучення до формування національної стратегії захисту інформаційного простору, зміцнення партнерства з державою, розвиток цифрових компетентностей суспільства є критично важливими для стійкості України перед зовнішніми загрозами. Отже, громадські організації підтвердили свою ефективність у протидії інформаційним атакам та повинні залишатися невід'ємною частиною загальнонаціональної системи інформаційної безпеки;

– аналіз інформаційної війни як самостійної вісі гібридної агресії**,** що змістила фокус із фізичної конфронтації до когнітивного впливу, розмиття ідентичності й делегітимації держав. Такий підхід дав змогу визначити інформаційну війну як домінантну форму сучасного глобального конфлікту. Доповнено концепт інформаційної зброї як системного інструменту неконвенційного впливу, що поєднує дезінформацію, психологічний тиск, кібератаки, фейковий контент і маніпулятивні наративи. Доведено, що інформаційна зброя спроможна чинити ефекти, співмірні із застосуванням збройної сили, але з нижчими витратами й вищою адаптивністю. Систематизовано вплив інформаційної зброї на внутрішню стабільність держави в умовах гібридної війни, зокрема на прикладі конфлікту росії проти

України. Показано, що інформаційні атаки – не супровід воєнних дій, а самостійна фаза стратегічного наступу, спрямована на руйнацію довіри, деморалізацію населення та політичну дезінтеграцію;

– порівняння моделей забезпечення інформаційної безпеки, що охоплює досвід США, держав Європейського Союзу, Японії, Китаю, Індії й країн Латинської Америки. Такий комплексний підхід дає змогу виявити спільні виклики та відмінні стратегії у відповідь на кіберзагрози. Систематизовано чинники вразливості національних цифрових інфраструктур із виокремленням таких критичних елементів, як фрагментарність правової бази, брак міжвідомчої координації, недостатня цифрова грамотність, обмеженість ресурсів, цифрова диктатура;

– трактування інформаційної агресії російської федерації як стратегічно спланованої форми гібридної війни, що поєднує інформаційно-психологічні операції, кібератаки, дезінформацію та маніпулятивні кампанії в цифровому середовищі. Обґрунтувано комплексну модель інформаційного терору рф як багаторівневу, технологічно адаптивну стратегію, що мімікрує під демократичні цінності з метою делегітимізації української державності й деморалізації суспільства.

Поглиблено:

– знання щодо таких аспектів, як інституційна спроможність держави забезпечувати кібербезпеку та контроль за інформаційним середовищем; рівень медіаграмотності населення і його здатність до критичного мислення; ефективність стратегічних комунікацій, спрямованих на посилення довіри до демократичних інституцій; інклюзивна державна політика щодо інформаційної безпеки, спрямована на захист прав людини та свободи слова;

– сучасні підходи до інформаційного тероризму, із виокремленням його ключових рис: транснаціональність, мережевість, когнітивна маніпуляція, цифрова анонімність, інституційна невизначеність. Доведено, що інформаційний тероризм має тенденцію до інституціоналізації на рівні державної політики авторитарних режимів і використовується як інструмент

зовнішньополітичного тиску. Зокрема, наголошено на ролі таких суб'єктів, як російська федерація, Китайська Народна Республіка й ін., що активно використовують інформаційний простір як поле для невоєнної агресії;

– засади національної інформаційної безпеки в умовах нових типів воєн, що включають цифрову стійкість, розвиток критичного мислення громадян, інформаційну гігієну, стратегічну комунікацію та міжнародну кооперацію в межах НАТО, ЄС й ООН;

– обґрунтування ролі стратегічних комунікацій, медіаграмотності, інфомаційної гігієни в національній і міжнародній безпеці, зокрема як елементів інформаційної оборони. Показано, що ключовим викликом для держави у XXI ст. є не лише захист територіальної цілісності, а й оборона інформаційного суверенітету. Проаналізовано структурні вразливості України в інформаційній сфері (низький рівень цифрової грамотності, фрагментарність політики, повільна реакція на ШІ-загрози) та визначенні стратегічних пріоритетів для формування сталої інформаційної стійкості;

– розуміння інституційно-суспільної взаємодії в інформаційній обороні України, зокрема визначено унікальну роль громадянського суспільства як рівноправного суб'єкта протидії інформаційній агресії (на прикладі OSINT-спільнот, цифрових волонтерів, проєктів StopFake, Detector Media тощо). Систематизовано виклики у співпраці між державою та громадськими ініціативами, зокрема правової неврегульованості, етичних дилем (випадок із «Миротворцем»), що дає змогу сформувати підґрунтя для розроблення національної моделі врегулювання партнерства в інформаційній безпеці. Посилено аргументацію потенціалу українського досвіду як моделі для транснаціонального використання в системах інформаційної безпеки держав, що протидіють авторитарному інформаційному впливу.

Практичне значення одержаних результатів. На підставі проведеного дослідження здійснено узагальнення та зроблено висновки, евристичність яких зумовлює використання здобутків дисертації в подальших дослідженнях явища гібридної війни й політик протидії гібридній агресії. Загалом,

результати дисертаційного дослідження формують теоретичний та емпіричний базис для формування державної доктрини гуманітарної безпеки й політики культурної безпеки. Робота поглиблює теоретичне осмислення феномену інформаційного тероризму та його місця в системі міжнародної безпеки. Запропоновано міждисциплінарний підхід до аналізу деструктивних інформаційних впливів, розроблено типологію інформаційних загроз й узагальнено досвід різних країн щодо протидії інформаційному тероризму. Дослідження може стати підґрунтям для подальших наукових розвідок у сфері інформаційної безпеки, політичної комунікації, міжнародних відносин, медіастудій і кібербезпеки.

Напрацювання дисертаційного дослідження можуть бути використані на рівні урядових інституцій, які виконують діяльність з інформаційної боротьби Зокрема, результати дослідження спроможні слугувати аналітичною основою для розроблення державної стратегії у сфері інформаційної безпеки, формування політик протидії гібридним загрозам і дезінформації. Висновки роботи сприятимуть підвищенню інформаційної грамотності населення, формуванню стійкості до маніпулятивного впливу, підтримці національної єдності та захисту демократичних цінностей в умовах глобальної інформаційної війни.

Також напрацювання дисертаційного дослідження можуть бути використані в навчальному процесі в межах курсів із міжнародної безпеки, стратегічних комунікацій, міжнародної інформації, конфліктології, кібербезпеки, а також під час розробки нових навчальних програм і спецкурсів. Робота є актуальним джерелом для підготовки курсових, бакалаврських, магістерських і дисертаційних робіт. Заданий контекст дослідження може слугувати основою для створення на базі закладів вищої освіти відповідних аналітичних центрів, діяльність яких буде спрямована на вироблення теоретичних та практичних підходів до ізоляції соціогуманітарного простору від російського впливу, формування україноцентричних наративів і практик уведення їх у масову свідомість,

поглиблення інтеграції українського соціогуманітраного (й особливо культурного) простору в загальноєвропейський простір.

Особистий внесок здобувача. Дисертаційна робота є завершеною науковою працею. Наукові положення, висновки, рекомендації та пропозиції, які винесені на захист, були одержані здобувачем особисто. Із наукових праць (додаток А), опублікованих у співавторстві, у дисертації використано лише ті ідеї й положення, які є результатом особистої роботи здобувача. Внесок дисертанта в працях, опублікованих у співавторстві, зазначено в переліку основних публікацій за темою дисертації. Особистий внесок здобувача в науковий доробок, представлений у наведених публікаціях, полягає в послідовному та системному розвитку концепції інформаційної безпеки, стратегічних комунікацій і протидії інформаційному тероризму в міжнародних відносинах. Праці здобувача охоплюють широкий тематичний спектр – від аналізу регіональних систем безпеки (Північно-Східна Азія, ЄС, САДК) до розробки теоретико-методологічних засад кібербезпеки, інформаційної політики держав і формування інформаційної стійкості України.

Здобувач однією з перших у вітчизняній політологічній науці обґрунтувала інформаційний тероризм як структурний чинник гібридних війн, розкривши його когнітивну, технологічну й комунікативну природу. У низці публікацій сформульовано аналітичну модель інформаційно-терористичних впливів і розроблено класифікацію їхніх інструментів – від дезінформації й пропаганди до кібердиверсій та когнітивних операцій.

У співавторських працях здобувачем зроблено суттєвий внесок у порівняльний аналіз систем інформаційної безпеки провідних держав світу (США, Японія, Індія, Бразилія, країни ЄС), висвітлено інституційні моделі кіберзахисту й нормативно-правові підходи до забезпечення цифрової стійкості. Ці дослідження створили емпіричну базу для формування власної аналітичної моделі України у сфері кібер- та інформаційної безпеки.

Особливе місце в науковій діяльності здобувача посідають праці стосовно інформаційної стійкості України як ключового компонента протидії інформаційному тероризму. У статтях «Громадські об'єднання на захисті інформаційного простору України» (2021), «Особливості поширення російських фейків в Україні» (2021), «SWOT-аналіз стану інформаційної безпеки України» (2022), здобувачем запропоновано концептуальну трикомпонентну модель інформаційної стійкості, яка поєднує стратегічні комунікації, медіаграмотність і кіберзахист.

Крім того, у наукових монографіях та колективних виданнях здобувачем здійснено систематизацію базових понять і категорій інформаційної безпеки; розроблено термінологічний апарат, який нині використовується в навчальних та науково-аналітичних цілях.

Отже, особистий внесок здобувача полягає в поглибленні теоретико-методологічного розуміння інформаційного тероризму як феномену міжнародних відносин; розробленні типології інформаційних загроз і засобів протидії їм; обґрунтуванні концепції інформаційної стійкості як інструменту національної безпеки; узагальненні міжнародного досвіду кіберзахисту; формуванні власного наукового підходу до аналізу гібридних інформаційних конфліктів, який поєднує політологічний, комунікативний і безпековий виміри.

Зазначені вище публікації засвідчують самостійний науковий внесок здобувача в становлення сучасної школи дослідження інформаційної безпеки, кіберполітики та стратегічних комунікацій в Україні. Усі теоретико-методологічні, науково-аналітичні висновки й рекомендації дисертантом зроблено самостійно.

Апробація результатів дисертації. Основні результати дисертаційного дослідження апробовано на таких 19 наукових заходах (додаток Б): IV Всеукр. наук. конф. з міжнар. участю «Сучасні соціально-гуманітарні дискурси» (м. Дніпропетровськ, 2014 р.), Міжнар. наук.-практ. конф. «Перспективи розвитку науково-практичних досліджень у сфері гуманітарних та суспільних

наук» (м. Київ, 2014 р.), Міжнар. наук.-практ. інтернет-конф. «Актуальні проблеми країнознавчої науки» (м. Луцьк, 2015 р.), XXVI Міжнар. наук.-практ. конф. «Зміни в соціально-економічному розвитку країни» (м. Чернівці, 2015 р.), IX Міжнар. наук.-практ. конф. студентів та молодих вчених «Актуальні проблеми зовнішньої політики України» (м.Чернівці, 2015 р.), III Міжнар. наук.-практ. інтернет-конф. «Актуальні проблеми країнознавчої науки» (м. Луцьк, 2015 р.), XXXVI Міжнар. наук.-практ. конф. «Проблеми і перспективи практичної реалізації наукових досліджень» (м. Чернівці, 2016 р.), I Міжнар. наук.-практ. інтернет-конф. «Актуальні проблеми регіональних досліджень» (м. Луцьк, 2017 р.), LX Міжнар. наук.-практ. конф. «Проблеми та перспективи наукових досліджень» (м. Чернівці, 2018 р.), II міжнар. наук.-практ. конф. «Інформаційна війна як новий вимір геополітичної ривалізації» (м. Луцьк, 2019 р.), Міжнар. наук-практ. конф. «Міжнародні та регіональні системи: актуальні питання міжнародних відносин і регіональних студій» (м. Луцьк, 2019 р.), II міжнар. наук.-практ. конф. «Інформаційна війна як новий вимір геополітичної ривализації»: матеріали (м.Луцьк, 2019 р.), Міжнар. наук.-практ. конф. «Інформаційна гігієна як напрям національної безпеки» (м. Луцьк, 2021 р.), Міжнар. наук.-практ. інтернет-конф. «Актуальні проблеми міжнародних відносин і регіональних досліджень» (м. Луцьк, 2021 р.), Міжнар. наук.-практ. інтернет-конф. «Стратегічні комунікації в контексті безпекової політики: європейський і глобальний рівні» (м. Луцьк, 2022 р.), міжнар. круглого столу «Мультидисциплінарні підходи до аналізу суспільно-політичних проблем в умовах російсько-української гібридної війни» (м. Львів, 2022 р.), III Міжнар. наук.-практ. Інтернет-конф. «Актуальні проблеми міжнародних відносин і регіональних досліджень» (м. Луцьк, 2023 р.), Міжнар. наук.-практ. інтернет-конф. «Зовнішнє інформаційне маніпулювання та втручання в умовах сучасних конфліктів», (м.Луцьк, 2025 р.), Міжнар. наук.-практ. конф. «Європейська інтеграція України: виклики, досвід, перспективи: матеріали міжнародної науково-практичної конференції» (м.Луцьк, 2025 р.). Також

здійснено апробацію основних положень дисертаційного дослідження у професійній діяльності в соціокультурній сфері. Так, здобувачем пройдено низку курсів та тренінгів. Крім того, основні ідеї дисертації пройшли апробацію на науково-методологічних семінарах кафедр міжнародних відносин і регіональних студій, міжнародних коумнікацій та політчиного аналізу ВНУ ім. Лесі України.

Публікації. Основні положення та висновки дисертаційного дослідження опубліковано дисертанткою у 44 працях, у тому числі 7 статей опубліковано в наукових виданнях, що входять у наукометричні бази Scopus та Web of Science, 16 – публікації у наукових фахових виданнях України та 3 – у зарубіжному фаховому виданні Польщі, 2 підрозділи – у колективних монографіях, 3 – у довідково-енциклопедичних виданнях, 13 – тези доповідей.

Структура та обсяг дисертаційного дослідження. Дисертація складається зі вступу, 5 розділів, 15 підрозділів та висновків, 8 додатків. Загальний обсяг дисертації становить 470 сторінок, із них 360 сторінок – основний текст, 57 сторінок – список використаних джерел (567 найменувань).

РОЗДІЛ 1
ДОСЛІДЖЕННЯ ТЕРОРИЗМУ В КОНТЕКСТІ СУЧАСНИХ МІЖНАРОДНИХ ВІДНОСИН

1.1. Генеза та концептуалізація поняття «тероризм» у політологічному дискурсі

У сучасному світі тероризм є одним із найгостріших викликів глобальній безпеці, що набув транснаціонального характеру й безпосередньо впливає на міжнародну стабільність. У зв'язку з цим концепт тероризму посідає важливе місце в теорії міжнародних відносин, хоча його визначення й трактування залишаються неоднозначними як у науковій, так і в політичній площині. Загальноприйнятого визначення тероризму досі не існує. Причиною цього є не лише складність самого явища, а й значна політична заангажованість, що ускладнює його нейтральне концептуалізування.

У глобалізованому світі тероризм більше не є локальною проблемою (додаток В). Він вийшов за межі традиційного розуміння «точкового насильства» й дедалі частіше набуває ознак системної загрози, що використовує інформаційні технології, кіберпростір, мережеві структури. Це потребує від міжнародного співтовариства нового підходу до осмислення природи тероризму, його мотивів і механізмів впливу. Отже, концепт тероризму в теорії міжнародних відносин є багатовимірним і динамічним. Він уключає не лише фізичний вимір насильства, а й символічний – комунікативний простір страху, політичного тиску й стратегічного сигналу. Поглиблене осмислення тероризму як міжнародного феномену дає змогу краще зрозуміти сучасну архітектуру загроз і вибудовувати ефективну політику протидії на національному та глобальному рівнях.

Передусім, подаємо тлумачення деяких основних термінів і понять, що використовуються в дослідженні. Потрібно чітко дефініювати такі споріднені поняття, як «терор», «тероризм», «терористичний акт», оскільки досі існує

чимало різних термінів, що відповідно позначається на виробленні спільного підходу до цих суспільно-політичних феноменів та винайдення ефективних засобів боротьби з ними.

Термін «терор» вперше ввів Арістотель, описуючи особливий вид страху, який відчували глядачі давньогрецьких трагедій. Цей страх стосувався неминучості загибелі та втілювався у болі, хаосі й руйнуванні. Використання реального жаху для завоювання та підтримки влади має таку ж давню історію, як і сама влада. Наприклад, єгипетські фараони застосовували штучний голод як засіб залякування: вони перекривали зрошувальні канали, спричиняючи посуху на великих територіях і викликаючи голод. Такий жах охоплював цілі покоління, забезпечуючи беззаперечне підпорядкування владі фараонів.

Взаємозв'язок між поняттями «терор» і «тероризм» є очевидним, адже обидва походять від латинського *terror* – страх. Вони означають застосування сили або загрозу її застосування з політичними чи економічними цілями, коли сильніша сторона впливає на слабшу. Однак у сучасному інформаційному суспільстві «застосування сили» не завжди передбачає фізичне насильство. Сьогодні однією з форм такого впливу є юридичні приписи та норми, невиконання яких призводить до санкцій, тобто механізму примусу, спрямованого на формування підсвідомого сприйняття встановлених правил [110].

У такому контексті суворість покарання – чи то штраф, громадські роботи або навіть смертна кара – має другорядне значення, оскільки головна мета досягається через страх відповідальності. Саме тому в рамках соціального управління доцільніше визначати терор як метод примусу до дотримання норм через створення віртуального страху перед покаранням. Терор, у цьому розумінні, є управлінським інструментом, що формує в більшості членів суспільства усвідомлення відповідальності за потенційні порушення через приклади публічного покарання тих, хто вже порушив правила.

Отож терор – це загальне поняття, що містить як ознаки попередньо зазначених близькоспоріднених термінів, так і акумулює значно ширше розуміння й тлумачення всього спектра вчинення насильницьких дій з відповідним кваліфікуванням їх як терористичних проявів.

Поняття «тероризм» має багатозначний зміст і може розглядатися як ідеологія, соціальний процес або конкретна дія. Це унікальний вид злочинної діяльності, який передбачає подвійний об'єкт впливу: безпосередню жертву терористичного акту та опосередковану жертву – суспільство, що піддається психологічному тиску. При цьому вид злочину, що використовується в терористичних актах, не має чіткої специфікації – це може бути будь-яка незаконна дія як із жертвами, так і без них. У правовому полі сутність тероризму як конкретного вчинку зазвичай визначається кримінальним кодексом або сформованими в суспільстві уявленнями. Водночас саме трактування тероризму нерідко відображає стиль управління тієї чи іншої влади.

Уперше як термін використано в 1790-х р. для позначення терору, який революціонери застосовували проти своїх опонентів під час Французької революції. Якобінська партія Максимільєна Робесп'єра здійснила правління терору, що передбачало масові страти на гільйотині. Хоча тероризм у такому вживанні означає акт насильства держави проти своїх внутрішніх ворогів, із XX ст. цей термін найчастіше застосовувався до насильства, спрямованого, прямо чи опосередковано, проти урядів із метою впливу на політику або повалити наявний режим.

У міжнародному та національному праві немає єдиного визначення тероризму, проте, проаналізувавши більшість міжнародних документів, визначили, що вони містять схожі критерії. Наприклад, Конвенція ООН про боротьбу з фінансуванням тероризму (1999 р.) визначає терористичний акт як дію, спрямовану на залякування населення або примушення уряду до певних дій: «Будь-яка дія, спрямована на спричинення смерті або серйозних тілесних ушкоджень цивільній особі або будь-якій іншій особі, яка не бере активної

участі у воєнних діях у ситуації збройного конфлікту, якщо метою такої дії є залякування населення або примушення уряду чи міжнародної організації до учинення або утримання від вчинення будь-яких дій» [400]. Своєю чергою, Європейська конвенція про боротьбу з тероризмом (1977 р., доповнена 2005 р.) акцентує увагу на політичній мотивації таких злочинів: «Терористичні акти – це злочини, спрямовані на залякування населення або незаконний тиск на державні органи з політичних чи ідеологічних мотивів» [347]. З іншого боку, Рамкове рішення Ради ЄС 2002/475/ЈНА про боротьбу з тероризмом (зі змінами 2008 р.) визнає терористичні злочини як умисні акти, що «можуть завдати серйозної шкоди країні або міжнародній організації», «учиняються з метою залякування населення, примушення уряду чи організації до певних дій або дестабілізації основних політичних, економічних чи соціальних структур» [344]. Згідно з Кодексом США (18 U.S. Code § 2331), тероризм – це «незаконне застосування сили та насильства проти осіб або майна з метою залякування чи примусу уряду, цивільного населення або будь-якої його частини для досягнення політичних або соціальних цілей» [357].

Відомий вітчизняний дослідник природи тероризму В. Ліпкан [124] тлумачить тероризм із трьох позицій: а) у широкому розумінні – як соціально-правового явища, спричиненого дією низки політичних, економічних та соціальних чинників і такого, що «характеризується об’єднанням агресивно налаштованих прошарків організованої злочинності з розподілом на ієрархічні рівні і виділенням лідерів, що особисто не беруть участі у вчиненні актів тероризму, але здійснюють ідеологічні, управлінські й організаційно-розпорядчі функції»; б) у загальноправовому розумінні – як негативного соціального явища, вираженого в застосуванні (чи погрозах) насильницьких дій особою або групою осіб, які намагаються примусом досягти поставленої мети; в) у кримінально-правовому тлумаченні – як погрози або небезпечних дій, спрямованих на заподіяння небезпеки життю або здоров’ю людей та майнової шкоди й загалом –на підрив стабільності в суспільстві [124, с. 227–228].

Один з американських політологів В. Волтер визначає тероризм як «погрозу або застосування насильства в політичних цілях, здійснювану окремими особами чи групами як на підтримку, так і проти чинного уряду, із метою впливу на ширше коло людей, ніж безпосередні жертви» [40]. Це визначення підкреслює головний механізм тероризму – залякування, створення суспільного резонансу та введення більшості населення в стан постійного страху. Як соціальна система, тероризм має кінцеву мету – зміну механізмів управління суспільством через страх, незалежно від форми цього управління. Ідеться як про політичний режим, так і про глобальний порядок, принципи функціонування злочинних угруповань або навіть трудових колективів.

Тероризм, розрахований на застосування насильства для створення загальної атмосфери страху серед населення й, отже, досягнення певної політичної мети. Тероризмом займаються політичні організації як із правими, так і з лівими цілями, націоналістичні та релігійні групи, революціонери й навіть державні установи, такі як армія, розвідувальні служби та поліція [282].

Отже, тероризм кваліфікується як антилюдський і антисоціальний злочинний акт, що призводить до вчинення антигуманних дій і характеризується зловмисною спрямованістю та організаційним забезпеченням. Власне ж, терористичний акт – це вчинена дія будь-якого виду насильства задля залякування соціуму й створення умов, сприятливих для реалізації певних корисливих цілей окремої групи людей.

Зазначимо, що в політичній риториці тероризм часто використовуються як інструмент легітимації або делегітимації дій певних акторів. Із позицій неореалізму тероризм розглядають як засіб боротьби недержавних суб’єктів за владу чи вплив у міжнародній системі, де панує анархія. Натомість неолібералізм акцентує увагу на інституційному співробітництві й необхідності міжнародної координації в протидії терористичним загрозам. У конструктивістському підході тероризм сприймається як соціальний конструкт, що залежить від контексту, ідеологічної інтерпретації та

комунікативного впливу. Тут важливу роль відіграють наративи: хто і як позначає терориста, із якою метою і на яких ціннісних засадах. Такий підхід дає змогу зрозуміти, чому одна й та сама дія може трактуватися як «терористична» одними акторами і як «визвольна» – іншими.

Деякі визначення розглядають усі акти тероризму, незалежно від їх політичної мотивації, як звичайну злочинну діяльність. Наприклад, Федеральне бюро розслідувань США (ФБР) трактує міжнародний і внутрішній тероризм як «насильницькі злочинні дії» [353], де міжнародний тероризм – насильницькі злочинні дії, учинені особами та/або групами, які надихаються або пов'язані з визначеними іноземними терористичними організаціями чи державами (підтримуваними державою), а внутрішній тероризм – насильницькі, злочинні дії, учинені особами й/або групами для подальших ідеологічних цілей, що випливають із внутрішніх впливів, таких як політичні, релігійні, соціальні, расові чи екологічні природи. Однак елемент злочинності є проблематичним, оскільки він не розрізняє різні політичні та правові системи й, отже, не може пояснити випадки, коли насильницькі напади на уряд можуть бути законними.

Протягом XIX ст. поняття тероризму поступово втрачало асоціацію з державним терором і все більше пов'язувалося з діяльністю внутрішніх груп, які прагнули повалити чинну владу. Революційні рухи по всій Європі часто застосовували насильство як засіб боротьби з правителями та державними режимами, які вважали репресивними або несправедливими. Найпоширенішим методом було політичне вбивство.

У XX ст., відзначеному масштабними людськими втратами й надзвичайною жорстокістю методів, як уряди, так і субдержавні угруповання активно використовували насильство для досягнення своїх цілей. Відповідальність за багато з цих кривавих подій була як на державних посадовцях, так і на нелегальних групах. Однак до кінця століття саме останні стали здебільшого класифікуватися як терористичні організації. Часто ці

угруповання отримували озброєння, фінансування й навіть військову підготовку від інших держав, що сприяло їхній діяльності.

Починаючи з XX ст., ідеологічні переконання та політичний опортунізм спонукали низку держав до участі в міжнародному тероризмі, часто під прикриттям підтримки національно-визвольних рухів. У зв'язку з цим поширилася відома фраза: «Для однієї людини – терорист, для іншої – борець за свободу». Розмежування між тероризмом та іншими формами політичного насильства стало нечітким, оскільки багато партизанських угруповань удавалися до терористичних методів, а питання юрисдикції й правової оцінки залишалися суперечливими.

Ці труднощі спонукали частину дослідників визначати тероризм не через його злочинний характер, а з огляду на те, що жертвами терористичних атак здебільшого стають невинні цивільні особи. Водночас і таке визначення залишається гнучким: його часто розширюють, ураховуючи додаткові аспекти, наприклад прихований або таємний характер терористичних дій та їхню основну мету – поширення всепоглинаючого страху.

Зі свого боку, М. Девіт описує тероризм як явище, коріння якого – не у фундаменталістській ідеології, релігії чи цінностях, а в реальних потребах, що визначають мотивацію. Він зазначає, що військові методи боротьби з тероризмом лише загострюють проблему, оскільки сам тероризм є, власне, симптомом глибших глобальних криз. На його думку, для ефективної протидії тероризму потрібно змінити підхід до його розуміння, розробити нові стратегії та способи мислення. Соціолог указує, що тероризм виник як наслідок політики нафтових магнатів і став способом відволікання уваги від внутрішніх проблем країн Близького Сходу, перенісши конфлікт на Захід [110]. Наголошено, що цей зсув не відбувся б, якби Захід залишався вірним своїм ідеалам свободи, законності та рівності можливостей. В останній чверті XX ст. ці ідеали перетворилися на порожні декларації, що зробило Захід вразливим і перетворило його на ціль для терористичних атак [328].

Тероризм як явище не може існувати без терористичної діяльності, яка передбачає здійснення окремих актів або серії дій, спрямованих на досягнення певних цілей. Терористична діяльність охоплює широкий спектр дій, зокрема:

1) підготовку, координацію та здійснення терористичних атак;

2) підбурювання до вчинення терористичних актів;

3) створення й керування незаконними збройними формуваннями, злочинними угрупованнями або організованими злочинними структурами;

4) поширення ідеології тероризму та пропагандистську діяльність;

5) фінансування терористичних організацій і підтримку їхніх дій [6].

А. П. Шмід у звіті до Сектору із запобігання злочинності ООН (1991 р.) визначив, що терористичний акт є еквівалентом воєнного злочину в мирний час [28]. Терористичні акти, зазвичай, є разовими, одноразовими й мають руйнівну силу та прагнуть створити найбільший шум і якомога швидше досягти бажаної мети: вплинути на психіку людей, поширити в них паніку, невпевненість у майбутньому, страх, недовіру до влади тощо.

Аналізуючи поняття «терористичний акт», наголосимо, що це насильницькі дії або загроза їх учинення з метою залякування суспільства, впливу на державні органи або міжнародні організації для досягнення політичних, ідеологічних, релігійних чи інших цілей. Ключовими рисами є:

– насильницький характер, який уключає фізичне насильство, вибухи, викрадення людей, кібератаки тощо;

– цілеспрямованість на досягнення певної мети (зміна політики, залякування, дестабілізація ситуації);

– масовий ефект, мета якого – не лише безпосередньо завдати шкоди, а й викликати страх у великої групи людей;

– політична, ідеологічна або релігійна мотивація, яка й відрізняє тероризм від звичайних злочинів;

– символічність, оскільки досить часто спрямований на знакові об’єкти (урядові установи, транспорт, громадські місця).

Нижче окреслено низку критеріїв, що дають змогу визначити, чи можна певну дію класифікувати як терористичний акт [28]:

Наявність політичної мотивації. Терористичні дії, зазвичай, спрямовані на досягнення ширших стратегічних цілей, що виходять за межі безпосереднього ефекту конкретного акту. Наприклад, атаки на цивільне населення можуть здійснюватися з метою впливу на громадську думку або створення тиску на органи влади.

Застосування насильства чи реальна загроза його застосування. Для терористичних актів характерна не лише фактична реалізація насильницьких дій, а й можливість їх загрози. У багатьох випадках навіть загроза застосування насильства, якщо вона є переконливою, може розглядатися як терористичний акт, оскільки вона породжує страх серед цільової аудиторії, що використовується з політичною метою.

Терористичний акт як аналог воєнного злочину в умовах миру. Як зазначає А. П. Шмід у доповіді для Сектору з попередження злочинності ООН (1991), тероризм може розглядатися як форма воєнного злочину, яка вчиняється поза умовами збройного конфлікту.

Прагнення до потужного психологічного впливу. Терористичні акти, хоча й можуть видаватися довільними, зазвичай ретельно плануються з урахуванням психологічного ефекту на суспільство. Терористи обирають цільові групи, які забезпечать максимальний суспільний резонанс. Часто об’єктами атак стають символи політичного режиму, що підсилює інформаційний ефект.

Цільова орієнтованість на цивільне населення. Ще одним критерієм, що викликає суперечки серед дослідників, є спрямованість терористичних дій на цивільних осіб. Такий підхід ускладнює класифікацію атак на військових, політичних діячів або представників силових структур як терористичних, хоча такі дії також можуть мати ознаки тероризму залежно від контексту.

На думку В. Кончаковської та А. Кравчук стаття «Тероризм як злочинне явище: еволюція та заходи запобігання» [100], причинами зазначених дій можуть бути:

– існування таємних релігійних або сектантських угруповань, які прагнуть нав'язати свої переконання іншим, вважаючи їх єдино правильними й заперечуючи будь-які альтернативні ідеї чи доктрини;

– низький рівень добробуту населення, психологічна втома, а також нерозв'язані соціально-економічні проблеми в державі;

– співіснування економічно розвинених країн із державами третього світу та нав'язування першими своїх правил й умов. При цьому такі вказівки не завжди відповідають інтересам місцевого населення або окремих соціальних груп, що створює ґрунт для радикалізації та використання терористичних методів як інструменту досягнення політичних цілей;

– пропаганда злочинцями можливості легкого збагачення, що підриває авторитет закону й знижує його ефективність як засобу впливу на кримінальне середовище.

Досліджуючи явище інформаційного тероризму, приділимо увагу питанню відмінностей між терористичними та диверсійними актами. Цю проблему розглядали у публікаціях такі науковці, як Д. Артеменко [8], Г. Зайцев, Н. Коломієць [69], А. Климосюк [95], К. Нагорна [153], Ю. Степанова 213[] та інші.

Диверсія відрізняється від терористичного акту кінцевою метою. Її ціль – завдати шкоди державі, військовій інфраструктурі чи економіці противника (знищення об'єктів, підрив виробництва, дезорганізація управління), здебільшого орієнтована на матеріальні цінності та стратегічні об'єкти. Терористичний акт, своєю чергою, прагне залякати населення або тиснути на владу. Його основна мета – психологічний ефект, поширення страху, дестабілізація суспільства. З іншого боку, їх відрізняють об'єкти посягання. Диверсія націлена на інфраструктуру, транспорт, підприємства, військові об'єкти, енергетику, тероризм – на людей, громадські місця, символічні

об’єкти, щоб викликати максимальний резонанс. Відмінності також є і в масштабах та контексті скоєння. Диверсія часто здійснюється у воєнний час або в умовах протистояння держав, має більш цільовий характер. Теракт може відбуватися як у мирний, так і у воєнний час, часто пов’язаний із політичними, ідеологічними чи релігійними мотивами.

Водночас низка рис їх об’єднує. Насильницький характер – обидва злочини передбачають використання зброї, вибухів чи інших методів руйнування. Протиправність – і диверсія, і тероризм є тяжкими злочинами проти безпеки держави та суспільства. Мета дестабілізації – обидва підривають безпеку, створюють хаос і шкодять противнику. Конспіративність зазвичай вимагає таємної підготовки, залучення групи людей чи спеціальних засобів.

Д. Артеменко, фіксуючи відмінності між диверсією та терористичним актом указує, що якщо диверсія є безпосередньою дією, направленою на нанесення шкоди державній безпеці, обороноздатності тощо, то терористичний акт може бути як дією, так і погрозою вчинення такої дії. Погроза, яка характеризує другу форму терористичного акту, є інформаційною дією, яка полягає в повідомленні певному адресату відповідної інформації [8].

Г. В. Зайцев і Н. В. Коломієць відзначають, що диверсія відрізняється від терористичного акту за метою вчинення кримінально караних дій. У диверсії – це мета ослаблення держави, а в складі терористичного акту – це: 1) порушення громадської безпеки; 2) залякування населення; 3) провокація воєнного конфлікту, міжнародного ускладнення; 4) вплив на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об’єднаннями громадян, юридичними особами; 5) привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста) [69].

Окрім того, спосіб учинення злочину для диверсії, зазвичай, є таємним, а для терористичного акту – навпаки. Це потрібно для привернення уваги ЗМІ та населення. Також диверсія відрізняється від терористичного акту тим, що завжди чітко направлена на конкретний об'єкт, пов'язаний із функціонуванням держави. Водночас терористичний акт може зачіпати випадкових жертв, об'єктів атак, не завжди напряму пов'язаних із тими, кому транслюються сигнали терористів. Звідси й основа терміна «тероризм» – «жахаючий», «поширюючий страх». Наприклад удари ЗСУ по НПЗ рф можна трактувати як диверсії. Вони ослаблюють військовий потенціал росії, ускладнюють для неї логістику, підривають економіку. А росіяни, своєю чергою, здійснюють тактику терору, наносячи удари по цивільних об'єктах України – житлових будинках, лікарнях, зокрема Охмадиту тощо.

Зазвичай, проблема зіставлення диверсії та терористичного акту розглядається в ширшому, юридичному контексті. Однак їх можна застосувати й у сфері інформаційної безпеки. Так, за ст. 113 Кримінального кодексу України, диверсія – це вчинення з метою ослаблення держави вибухів, підпалів або інших дій, спрямованих на масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, на зруйнування або пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення, а також учинення з тією самою метою дій, спрямованих на радіоактивне забруднення, масове отруєння, поширення епідемій, епізоотій чи епіфітотій [108]. Відповідно, «іншими діями» можуть бути кібератаки, націлені на критичну інфраструктуру України, що забезпечують роботу державних органів влади, банків, операторів зв'язку, систем енергетики тощо.

Диверсію й терористичний акт у сфері інформаційної безпеки розглядаємо як кібердиверсію та кібертероризм. В інформаційній сфері вони можуть здійснюватися з метою підриву інформаційної інфраструктури держави чи організації. Прикладами є виведення з ладу енергомереж через хакерську атаку, знищення або підміна даних, блокування серверів держустанов. Об'єктами вважають насамперед системи управління (SCADA-

системи, бази даних, урядові портали). Їх характеризує спрямована дія проти конкретної інфраструктури, щоб зменшити обороноздатність чи економічну стійкість.

Терористичний акт у кіберпросторі здійснюється задля посилення психологічного ефекту, залякування населення чи тиску на уряд. Прикладами можуть слугували масові злами сайтів із поширенням панічних повідомлень, атаки на медіа з дезінформацією, «захоплення» інформаційних ресурсів з метою пропаганди. Об'єктами таких атак є громадська свідомість і відчуття безпеки, а не лише інфраструктура. Вони забезпечують ефект резонансу – важливо, щоб про атаку дізналося якомога більше людей.

У контексті інформаційної безпеки їх об'єднує:

– використання кіберзасобів (шкідливе ПЗ, фішинг, DDoS-атаки, соціальна інженерія);

– нелегітимність і спрямованість проти безпеки держави чи суспільства;

– можуть мати міжнародний вимір (державні й недержавні актори);

– створюють довгострокову недовіру до системи безпеки, ЗМІ, державних інститутів.

Якщо узагальнити, то кібердиверсія – це прихований, точковий удар по критичній інформаційній інфраструктурі, а кібертероризм – це демонстративна атака, яка має на меті паніку, дестабілізацію та привернення уваги.

На жаль, поняття кібердиверсія й кібертероризм не мають належного відображення у вітчизняному законодавстві. На цю проблему, зокрема, звертає увагу О. Р. Пелещак. Зокрема, він зауважує, що незаконне втручання в роботу АЕОМ, їх систем чи комп'ютерних мереж, носіїв комп'ютерної інформації, її перекручення, знищення, розповсюдження комп'ютерного вірусу, програмні засоби треба тлумачити як дефініції новітніх форм диверсії, тобто як способи учинення кібердиверсії [173].

Водночас у ст. 258 Кримінального кодексу України доволі широко трактується поняття «терористичний акт» – як застосування зброї, учинення

вибуху, підпалу чи інших дій, які становили небезпеку для життя чи здоров’я людини або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо такі дії були вчинені задля порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади або органами місцевого самоврядування, службовими особами цих органів, об’єднаннями громадян, юридичними особами, міжнародними організаціями, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста), а також погроза вчинення зазначених дій із тією самою метою [108].

Загалом, визначення терористичного акту залишається предметом дискусій, особливо щодо ролі держави як потенційного суб’єкта терористичної діяльності. Обмеження поняття тероризму винятково до дій недержавних акторів автоматично позбавляє нас можливості оцінювати державне насильство крізь призму терористичних практик, навіть у випадках, коли воно має аналогічні за наслідками риси. Аналізуючи види терористичних актів, прогнозуємо їхні наслідки починаючи з людських жертв і психологічного впливу (паніка, страх, соціальна напруга), економічних збитків (руйнування інфраструктури, зниження довіри до держави), політичних змін (посилення заходів безпеки, обмеження громадянських свобод).

Отже, терористичний акт – це складне явище, яке поєднує насильство, політичну або ідеологічну мотивацію та соціальний ефект. Його аналіз уключає юридичний, соціальний і безпековий аспекти, а ефективна боротьба потребує комплексного підходу.

Терористичні акти можуть бути як локальними, так і масштабними, мати фізичні, психологічні або інформаційні наслідки. Розглянемо основні види терористичних актів, які найчастіше використовуються у світовій практиці. Одним із найпоширеніших є фізичний терористичний акт, що передбачає

застосування насильства проти людей або об’єктів інфраструктури. Це можуть бути вибухи, масові розстріли, захоплення заручників, підпали, напади на публічні місця або державні установи. Такі дії мають прямі жертви й спрямовані на привернення уваги до певної справи або помсти.

Із початку XXI ст. поширюється новий вид та термін – «стохастичний тероризм», який використовується для позначення неодноразового використання мови ненависті чи іншої образливої, дегуманної риторики політичним лідером чи іншим громадським діячем, що надихає одного або кількох прихильників учиняти злочини на ґрунті ненависті чи інші акти насильства проти цільової особи, групи чи спільноти. Оскільки стохастичні терористи не надають своїм послідовникам жодного детального плану нападу, конкретний час і місце остаточного насильства є непередбачуваними. Стохастичний тероризм як форма політичного насильства, викликана ворожою публічною риторикою, спрямованою проти групи чи окремої людини. На відміну від підбурювання до тероризму, стохастичний тероризм здійснюється за допомогою непрямих, розпливчастих або закодованих формулювань, які надають підбурювачу правдоподібне заперечення будь-якого пов’язаного насильства [513]. Ключовим елементом стохастичного тероризму є використання медіа для пропаганди, коли особа, яка чинить насильство, може не мати прямого зв’язку з іншими користувачами насильницької риторики [514].

У розгалуженому типологічному ряді окреме місце посідає «політичний тероризм». У дослідженні В. Ліпкан визначає його так: «Застосування чи погроза застосування насильства або інших всезагально небезпечних дій особою або групою, якщо такі дії спрямовані на дестабілізацію стану правових норм і відповідних їм інститутів безпеки, які гарантують захист суверенітету, територіальної цілісності, політичної належності та конституційного ладу держави з метою прийняття державою, міжнародною організацією, фізичною чи юридичною особою будь-якого рішення чи утримання від нього» [124, с. 223]. Таке тлумачення, з огляду на еволюцію тероризму й появу такого

різновиду, як «коаліційний тероризм», не є вичерпним, точніше – не зовсім відповідає реаліям сьогодення. Аргументованішим було б, скажімо, таке уточнення: «…якщо такі дії спрямовані на досягнення шляхом антитерористичної війни певних політичних цілей (реалізації стратегічних доктрин) окремою державою…». Крім суто політичного аспекта, така дефініція водночас повною мірою відображає спроможність тероризму як системи до власної самоорганізації, як концептуально до цього підходить автор, ґрунтуючи своє дослідження на положеннях теорії синергетизму.

Із цим поняттям тісно пов’язаний термін «державний тероризм» як чинник впливу на стан міждержавних відносин і насаджування якоюсь країною за допомогою вчинення терористичних або антитерористичних актів власних ідеологічних та ціннісних орієнтирів. Практично для цього використовуються сукупні ресурсні можливості не лише однієї країни (ініціатора), а й залучаються до цієї акції так звані «коаліційні сили». Отже, можна говорити про появу сучасного різновиду державного тероризму, який умовно можна кваліфікувати як «коаліційний тероризм».

Іншою небезпечною формою є кібертероризм – використання інформаційних технологій для порушення життєво важливих функцій держави, фінансових систем, об’єктів критичної інфраструктури (енергомережі, водопостачання, систем зв’язку). Цей вид тероризму зростає на тлі цифровізації та глобальної мережевої залежності.

Окрему категорію становить інформаційний тероризм – поширення фейків, маніпуляцій, дезінформації з метою викликати паніку, розколоти суспільство або підірвати довіру до державних інституцій. Він часто використовується в гібридних війнах, коли фізичні атаки поєднуються з інформаційними кампаніями. Щодо інформаційної сутності тероризму, то зазначимо, що воно відрізняється від загального переконання, що політичні цілі досягаються опосередковано. Насильство слугує приводом для маніпуляцій. Тероризм – це завжди інформація, незалежно від того, чи йдеться про глобальні події чи події локального характеру, оскільки його основне

завдання – маніпулювання (або у вигляді залякування населення з метою виникнення паніки, або у формі прямих загроз, тощо). Отже, принципова відмінність тероризму від інших форм насильницької політичної боротьби полягає в тому, що він перебуває на межі того факту, що застосування насильства проти мирного населення все ще використовується для досягнення політичних цілей [142].

Також існує ідеологічний тероризм, що ґрунтується на релігійних, політичних або расових переконаннях. Його характерною рисою є глибока радикалізація учасників, які вважають свої дії «священними» або виправданими вищою метою.

Не менш загрозливим є біологічний і хімічний тероризм, що передбачає застосування отруйних речовин або патогенів для ураження людей, тварин чи навколишнього середовища. Такі атаки можуть мати довгострокові катастрофічні наслідки, уключаючи епідемії, екологічні катастрофи й соціальну паніку. Нарешті, у новітній історії розвивається форма екотероризму –насильницьких дій в ім’я захисту природи або навколишнього середовища. Йдеться про підпали промислових підприємств, атаки на інфраструктуру, яка, на думку терористів, шкодить екології.

Отже, тероризм охоплює не лише фізичні дії, а й цифрові, психологічні та біоекологічні виміри. Розуміння видів терористичних актів необхідне для ефективної протидії й формування комплексної стратегії безпеки в сучасному світі. Суспільства та уряди повинні бути готовими до нових викликів, адже тероризм постійно еволюціонує, використовуючи слабкі місця відкритого світу.

Отже, тероризм у теорії міжнародних відносин постає як складне багатовимірне явище, що включає не лише фізичне насильство, а й інформаційний вплив та політичну маніпуляцію. Його багатозначність і транснаціональний характер зумовлюють потребу в комплексному міждисциплінарному підході до протидії.

1.2. Теоретико-методологічні підходи до аналізу глобалізаційних і цифрових трансформацій тероризму

Передумовою формування чіткіших уявлень про сутність міжнародного тероризму є глибоке розуміння понять «глобалізація» та «тероризм». Сьогодні існує багато визначень глобалізації. Одне з них належить колишньому Генеральному секретарю ООН Кофі А. Аннану. За його словами, глобалізація – це загальний термін, який означає все більш складний комплекс транскордонних взаємодій між окремими особами, підприємствами, установами й ринками [549].

Дослідження науковців свідчить про зважену інтерпретацію сучасних процесів глобалізації, що дає змогу визначити характерні риси цього явища та показати загрози й виклики людству. Нинішній усебічний процес глобалізації свідчить не тільки про початок нового етапу розвитку цивілізації, але й водночас супроводжується все більшим антиглобалістським заколотом, що спричинює появу низки інших непередбачуваних подій та конфліктів, які набули значного міжнародного резонансу.

Передусім, це стосується такого суспільно-політичного явища, як тероризм. Традиційно тероризм визначали як замах на життя державного чи громадського діяча, насильство або загрозу насильства, спрямовану на те, щоб змусити владу приймати рішення, вигідні терористам чи терористичним організаціям [286]. На нашу думку, проблему міжнародного тероризму потрібно розглядати всебічно й, передусім, у форматі «глобалізація – антиглобалізація», певною мірою як «відповідь на заклик». Концептуально важливо виходити з того факту, що фактичні явища глобалізму, як і тероризм, не є візитною карткою сьогодення: вони мають відповідні виміри переважно місцевого масштабу та значну історію. Отже, феномен міжнародного тероризму, який, окрім ролі в системі міжнародних відносин, окремих країн, їхніх лідерів, також використовується як ефективний механізм реалізації

певної стратегії глобалізації, зокрема, всебічного поширення стабілізувальної гегемонії прагнення.

Не можемо погодитися з поширеним твердженням, що після 11 вересня 2001 р. світ, власне, змінився. Це дещо перебільшення, адже фактично зазнала змін лише система міжнародної безпеки, а відтак і почала трансформуватися нова система міжнародних відносин. Тобто можна говорити лише про початок процесу кардинальних змін традиційного формату, а не про доконаний факт, тим більше, що розпочатий процес супроводжується безліччю непередбачуваних ускладнюючих обставин, отже, буде тривалим у часі й непрогнозованим щодо можливих наслідків.

Тим часом дедалі очевиднішою стає його обумовленість традиційними закономірностями суспільного розвитку, що ставить під сумнів доцільність спроб застосувати ситуативний підхід до оцінок несподіваних аномальних суспільно-політичних явищ. Б. Канцелярук зазначив: «Досі, здається, не бракує теоретичних пояснень і всіляких наукових обґрунтувань процесу трансформувань, що охопив нашу планету. Багатовимірний концептуальний підхід до оцінки цього явища, ґрунтований на цілісному, соціоприродному сприйнятті і тлумаченні власне процесу, дає підстави вважати сам перебіг його логічно обумовленим, отже, закономірним» [83]. Це стосується, зокрема, дослідження такої актуальної нині проблеми, як міжнародний тероризм, загальний вимір якої видається спрощувально-тривіальним, що, відповідно, позначається на об’єктивності її вивчення. Мається на увазі зосередження уваги дослідників лише на безпекових та кримінально-правових аспектах тероризму, які взагалі не дають цілісного уявлення про сутність цього явища без урахування сукупного впливу низки політичних, соціальних, конфесійних, культурних, історичних і цивілізаційних детермінант.

Синтезуємо аналітичні узагальнення й висновки, аби встановити роль і місце міжнародного тероризму в умовах глобалізації, а також виявити можливі тенденції в реалізації традиційних домінант зовнішньополітичної стратегії офіційного Вашингтону в ситуації, що склалася.

Як зазначено раніше, тероризм кваліфікується як антилюдський та асоціальний злочин, що призводить до нелюдських вчинків і характеризується шкідливими тенденціями та організаційною безпекою. Насправді терористичний акт – це акт будь-якого виду насильства з метою залякування суспільства й створення умов, що призводять до реалізації певних егоїстичних цілей окремої групи людей. Тероризм розвивається разом із суспільством, яке його породжує. Сучасний тероризм характеризується широкомасштабною участю великої кількості людей, добре структурований та організований. Діяльність терористичних організацій часто спрямована не тільки на загострення й дестабілізацію ситуації в певному регіоні, а й на досягнення набагато серйозніших цілей, як-от: захоплення чи перерозподіл влади, насильницькі зміни в державному устрої, нав'язування власних наказів, мораль і правила спільного проживання.

Масштаби терористичних операцій потребують, по-перше, залучення значних людських ресурсів, уключаючи спеціалістів високого рівня в різних галузях знань, поповнення та розширення його кількісного складу, розвиток розвідувальної мережі по всьому світу. Адже нинішній тероризм – це не лише диверсанти – сингltони та викрадачі літаків. По-друге, широкий масштаб цілей сучасного тероризму потребує залучення матеріальних і фінансових ресурсів, необхідних для оснащення терористичних організацій технічними засобами та зброєю, створення спеціалізованих шкіл, навчальних баз для тренування учасників терористичних угруповань. І по-третє, для цього потрібна добре розвинена інфраструктура. Ідеться про встановлення складних відносин між терористичними угрупованнями з різних країн, що поєднують такі сфери, як оперативна бойова підготовка, матеріально-технічне співробітництво, у тому числі у сфері озброєння, а також спільні дії.

Тероризм стає своєрідною галуззю, орієнтованою на експорт, перетворюючись на бізнес, де можна заробляти великі гроші. У теорії світової практики відомі три основні види терору:

– внутрішній (відповідні дії громадян однієї держави проти співвітчизників на їхній власній території);

– транснаціональний (відповідні дії громадян однієї держави проти співвітчизників на території інших держав);

– міжнародний (відповідні дії груп громадян, окремих чи змішаних за національним складом, проти будь-яких осіб на території третіх країн).

Сьогодні міжнародний тероризм виріс до такої міри й резонансу, що він фактично набув планетарного масштабу. Поняття «міжнародний тероризм» з'явилося в науковому обігу на початку сімдесятих років минулого століття та має так само низку різнотлумачень. Зокрема, він трактується як міжнародний злочин, що загрожує миру й безпеці, принижує людську гідність [545]; як насильницькі акти, які спрямовані на підрив міжнародних відносин, усталеної міжнародної політичної системи та суперечать наявним нормам моралі й права [359]; як застосування насильства проти (або за) чинного правлячого режиму, аби залякати певний суспільний прошарок [475]; як терористична діяльність, спрямована проти іноземних громадян, організацій або урядів із метою повалення державного устрою або підриву міжнародного порядку [475]; трактується як особливий вид ведення державами таємних воєнних дій [413]; як не якийсь особливий вид тероризму, а лише пролонгування внутрішнього тероризму за межі країни [221] і т. ін. Ураховуючи реалії, вважаємо доцільним тлумачити поняття «міжнародний тероризм» як організовані насильницькі дії, спрямовані на зміну конфігурації нового світового порядку.

На VII Конгресі Організації Об'єднаних Націй у 1990 р. у доповіді Ради Безпеки ООН зазначалося: «Міжнародний тероризм можна охарактеризувати як терористичні акти, під час створення яких виконавці планують свої дії, отримуючи певні вказівки з різних країн, утікати, шукати притулку або отримувати допомогу в будь-якій формі не в країні чи країнах, де вони створюють цей акт» [493].

Вивчення проблеми тероризму в Україні перебуває у фокусі уваги провідних вітчизняних науковців, які здійснюють ґрунтовні дослідження як із

погляду правової регламентації, так і з позицій національної безпеки, інформаційної стійкості та протидії гібридним загрозам.

Засадничий внесок у розробку теоретичних і практичних підходів до боротьби з тероризмом зробив доктор юридичних наук, професор В. А. Ліпкан. Він розглядає тероризм як одну з ключових загроз для національної безпеки, аналізує нормативно-правові засади протидії цьому явищу, а також розробляє концептуальні засади антитерористичної політики держави. Зокрема, у монографії «Тероризм і національна безпека України» дослідник пропонує системне бачення терористичних загроз у контексті геополітичних трансформацій та закладає основу для формування державної політики у сфері протидії тероризму в Україні [121].

Отже, сучасні українські дослідження тероризму демонструють міждисциплінарний характер і поєднують правові, політичні, інформаційні й безпекові підходи, що дає змогу формувати більш стійкі механізми національної протидії як класичним, так і новітнім формам терористичних впливів.

Масштабно розгорнута антитерористична кампанія засвідчила нагальну потребу пошуку адекватних моделей міжнародної безпеки у XXI ст., проте водночас показала, наскільки це проблематично з огляду на неоднозначну реакцію світової спільноти на односторонні агресивні дії керівництва Білого дому. «Нова геополітична ситуація, яка виникла після терористичних актів у вересні 2001 р., і створення міжнародної антитерористичної коаліції, до якої увійшла й Україна, вносить суттєві корективи в концепцію протистояння Захід–Схід. Росія тоді пішла на блискавичне зближення зі США, було створено «двадцятку» Росія–НАТО» [198].

Виходячи зі ступеня загроз і масштабів поширення, міжнародний тероризм становить серйозний глобалізаційний виклик світовій спільноті. Як зазначає Г. Токаревський, «від самого початку третього тисячоліття міжнародний тероризм став однією з найпекучіших проблем світової спільноти. У зв’язку із цим виникла потреба опрацювати нові підходи до

вивчення сутності цієї глобальної загрози та побудови нової архітектури безпечного співіснування у геополітичному просторі. Події 11 вересня 2001 р. в США значно актуалізували цю проблему, адже, на думку багатьох експертів, глобалізація терористичної діяльності розвивається і трансформується значно швидше, ніж глобалізація економічна» [223]. Відмінності передусім політичного характеру, на переконання Г. Токаревського, заважають виробленню спільних ефективних заходів із нинішнім «інтернаціоналізованим» тероризмом.

Під враженням терористичних актів й антитерористичних воєн у відповідь деякі дослідники поспішили заявити, що прогнозована С. Гантінгтоном війна між цивілізаціями вже розпочалася. Ми думаємо, що можна говорити фактично про зростання (загострення) протистояння Заходу з іншими цивілізаціями, зокрема з ісламською. Після подій 11 вересня 2001 р., як підкреслює С. Удовик, американська геостратегія зазнала переорієнтації. Якщо одразу після терактів Президент США Джордж Буш використав вислів «хрестовий похід», що сприймався як релігійне протиставлення ісламському світові, то згодом подібна риторика зникла з офіційного дискурсу. Американська політична еліта поступово відмовилася від бінарного поділу світу на «своїх» і «чужих», змістивши увагу на визнання його культурного й релігійного різноманіття. Наголошено, що боротьба США спрямована не проти ісламу як релігії, а проти явища тероризму [208]. При цьому С. Удовик наголошує, що активізація міжнародного тероризму безпосередньо пов’язана з глобалізаційними процесами, однак тут важливо мати на увазі ступінь впливу глобалізації на стан цивілізаційної свідомості. Адже загалом сучасні цивілізаційні конфлікти спричинюються не суто релігійними, етнічними чи культурними чинниками, а, передовсім:

а) бідністю та пов’язаними з нею наслідками;

б) майновою нерівністю етнічних груп;

в) історичною несправедливістю (насильницькими переселеннями на територію іншої країни);

г) статусними відмінностями;

ґ) зростаючою конкуренцією за оволодіння природними ресурсами;

д) соціальною конкуренцією [208, с. 322].

Глобалізаційні імперативи провідних потуг світу каталізують пошуки ефективних механізмів реалізації стратегії, використовуючи для цього традиційні силові засоби. «Глобальний егоїзм країн-лідерів, – підкреслює О. Білорус, – одна з найбільших сучасних загроз людству. Він призводить до глобальної нерівності країн і людей світу через нерівність технологій та умов життя...» [15]. Саме егоїстичні інтереси спонукають ці суперпотуги будувати свої стратегії «...на тому, щоб перемогти в конкурентній боротьбі ослаблені країни. Вони не розуміли і ще не розуміють, що перемога над слабкими ослаблює "переможців" і веде їх до неминучої деградації, яка матиме незворотній характер» [15, с. 31]. Глобалізаційні тенденції сьогодення з усією очевидністю показують, що домінування західної цивілізації втрачає перспективу, оскільки не відповідає новітнім викликам часу. Отже, робить висновок аналітик, «глобальні країни-лідери (такими він вважає США, ФРН, Великобританію, Францію, Японію, Китай, Індію та Росію. *Є. Вознюк*) сьогодні поставлені перед стратегічною альтернативою: або забезпечити поступовий, еволюційний, якісно новий розвиток всього глобалізаційного світу, або зіткнутися з такими новими глобальними проблемами, з якими вони будуть самі не в змозі справитись, а світ і світовий ресурс для них вже буде втрачено назавжди» [15, с. 32]. І яскравою ілюстрацією цього є проблема міжнародного тероризму, спроби розв'язати котру традиційними силовими засобами виявляються не лише безуспішними, а й спричинюють появу нових видів загроз світовій спільноті.

Отже, потрібен новий загальнометодологічний підхід, ґрунтований на синергетичних положеннях про те, що системи за своєю природою перебувають переважно в стані нестійкої рівноваги внаслідок сукупної дії різних чинників, у тому числі й спонтанних змін, які так само можуть спричинити кардинальні зміни. Такий підхід, як вважають Е. Морін та А-Б.

Керн, «...уможливлює врахування як найважливішої обставини руху людства або його дискретних співтовариств (цивілізацій, держав, окремих народів) свободу волі та вибору окремих індивідів. Саме в ній у непідвладній до кінця жодним зовнішнім обставинам іманентній пристрасті й свободі творчої самореалізації людини і слід, очевидно, убачати причину спонтанних відхилень, а отже, і випадкових, наперед непередбачуваних змін, що призводять до далекосяжних наслідків» [452].

Тероризм як глобалізаційний виклик сучасності переважно фокусується у форматі відносин Схід–Захід, які загалом мають дихотомічний характер із давніх часів. Предмет нашого дослідження обумовлює потребу оцінки цієї посутньої складової частини системного аналізу. Філософ Ю. Павленко звертає увагу на те, що витоки протиставлення Заходу й Сходу сягають в глибину історії та мають неоднозначне тлумачення, з огляду на істотні цивілізаційні відмінності фігурантів. «Перед нами два шляхи, дві лінії розвитку доіндустріальних суспільств: східний – із провідною роллю державного апарату в усіх сферах суспільної життєдіяльності, включаючи економіку, і західний – з розвинутою приватною власністю і громадянським правом, де держава не відіграє самодостатньої ролі. На рівні давнини такими будуть, наприклад, Передня Азія часів імперії Ахеменідів і антична Греція, в Новітні часи – Мусульманський світ, Китай або Індія, з одного боку, і Західна Європа – з іншого, у XX ст. – СРСР і Північноатлантичне співтовариство» [109]. Можна, звичайно, посперечатися щодо останнього твердження: адже Радянський Союз некоректно зіставляти зі Сходом і, крім того, загальновизнано, що він (як і нинішня росія) сповідував євразійський варіант розвитку й водночас жорстко протистояв як Сходові (як приклад – десятилітня афганська війна), так і Заходові загалом («холодна війна»). Зважаючи на це, потрібно, очевидно, у цьому випадку говорити вже про інший вимір протистояння на цивілізаційному рівні.

Політолог В. Кушніренко, досліджуючи проблему вестернізації мусульманського світу, звертає увагу на те, що «...стрибок у розвитку науки,

техніки, економіки та інших сфер в Європі вже в XVII столітті засвідчив, що співвідношення сил змінюється на користь динамічного західного світу. З XVIII століття інші частини світу, зокрема і мусульманська, потрапляють в колоніальну залежність європейців. Мусульманський світ наштовхується на незрозумілу йому потугу "невірних". І перед ним постає питання: як реагувати на цей виклик?» [114]. Реакція зазвичай зводиться до пошуку механізмів спротиву переважаючій силі експансії з метою відстояти політико-правову систему мусульманської автентичної традиції, зберегти усталені віками духовні цінності. Учений робить висновок: «Не можна не розуміти, що конфлікт масової свідомості з політичною ідеологією, якщо вона спрямована проти традиційних цінностей, завжди є руйнівним, навіть якщо він відбувається у не досить виражених формах, оскільки неможливо за допомогою чужої ідеології змінити архетипи та культурні коди певного соціуму» [114, с. 141].

Передусім, цим можна пояснити те, чому Захід не бажає зрозуміти природу ісламського світу, нав'язуючи йому свої ціннісні орієнтири, що призводить наразі до трагічних наслідків. «...Сьогодні ясно, що за незаперечного воєнного переважання НАТО у світовому масштабі про жодне торжество євроатлантичних цінностей не може бути й мови. Скоріше навпаки: реакцією на квазівестернізацію став глобальний поворот до традиційних цінностей незахідних цивілізацій, інколи в їхніх крайніх, доведених до абсурду з європейсько-американської точки зору, формах» [109, с. 702].

Не применшуючи ролі численних інших чинників порушуваної проблеми, хочемо зазначити, що домінантним усе-таки є політико-ідеологічний. Навіть якщо враховувати вагомість економічного чинника (за нинішнього стану зменшення ресурсного потенціалу планети), треба визнати, що він є лише спонукальним (точніше – каталізуючим) політико-ідеологічних імператив експансіоністської стратегії Заходу. Нинішній масштабний прояв феномену тероризму, отже, потрібно оцінювати як відповідну реакцію на ускладнений, крайньо загострюваний процес світового глобалізаційного

розвитку, який опинився в черговій пороговій фазі глибинних трансформувань. З огляду на це, нинішній небувалий спалах тероризму можна кваліфікувати як його новітній різновид, обумовлений дією сукупної низки чинників сучасного цивілізаційного поступу, зокрема станом міжнародних відносин, геополітичними колізіями, соціальним дисбалансом, науково-технічними досягненнями у військовій сфері, інформаційними технологіями тощо. Принагідно напрошується певний аналог з рівнем здобутків у галузі винайдення і виготовлення зброї масового знищення, унаслідок чого створилася та постійно тяжіє безпосередня загроза самому існуванню спільноти.

Водночас тероризм не можна вважати знаковим явищем поточного століття, оскільки немає достатньо підстав стверджувати, що він спроможний визначально впливати на реальний перебіг процесу глобалізації світу (так само й на явища антиглобалізму). Радше, тероризм можна вважати однією з багатьох складових частин нинішнього динамічного поступу, котра, між іншим, також може виконувати не лише винятково деструктивістську функцію. За відповідний аналог може слугувати феномен кризових явищ, який із нетрадиційних позицій дослідили політологи Б. Канцелярук [84] та А. Черній [239], котрі доводять наявність в означеному суспільно-політичному явищі й конструктивістського елементу як своєрідної детермінанти поступу.

Не можна не погодитися також із тезою відомого політолога С. Телешуна, що «міжнародний тероризм (до речі, як і корупція) не є традиційним злочином, а, насамперед, соціальним і політичним явищем, що проявляє себе в конкретних злочинних акціях, таких як захоплення заручників, напади на урядові установи, викрадення літаків тощо, за які в національному законодавстві та в міжнародному праві настає кримінальна відповідальність. Від загальнокримінальних злочинів тероризм відрізняється політичною мотивацією скоєння вчинків» [220, с. 166]. На думку науковця, «політизація» тероризму у вигляді політичного насилля є невід'ємною складовою частиною суспільно-політичних відносин.

Глобалізаційний вимір тероризму доповнюється логічно обґрунтованими міркуваннями Ю. Павленка про те, що ми є свідками дедалі більшого відставання у своєму розвиткові країн «третього світу», а прагнення держав-лідерів повсюдно декларувати наявність рівних можливостей та вільної конкуренції є не чим іншим, як лицемірством. «...Основною контраверзою глобалізації є дедалі посилювана суперечність між групою найбільш розвинутих країн Заходу та рештою людства, яке експлуатують світові лідери і яке дедалі більше у своїй більшості відстає від них» [109, с. 659].

Потребує уточнення й «антитерористичний світ», що загалом сприймається як знакова характеристика сьогодення, а можливо, й нинішньої епохи. Однак це віртуальне сприйняття. Фактично йдеться, радше, про так звані «коаліційні сили», зорганізовані Сполученими Штатами для боротьби з тероризмом, тобто про групу країн, які з різних міркувань долучилися до антитерористичної кампанії на чолі з Америкою. При цьому, як відомо, більшість держав, політичних і громадських діячів не схвалюють запропонований Білим домом силовий варіант розв’язання проблеми міжнародного тероризму, яка набрала планетарного значення саме після того, як було вчинено повітряні атаки на саму Америку. Через те, мабуть, правомірніше говорити не про настання антитерористичного світу (так само відповідно, і терористичного), а про наявну ознаку чи тенденцію, що загалом супроводжує складний і непередбачуваний процес глобалізування світу [29].

Термін «антитерористична війна» тлумачимо теж у дещо ширшому контексті, оскільки очевидно, що вона обумовлена й фактично велася не стільки проти конкретного ворога – міжнародних терористів, скільки проти уявного, від чого постраждали цілі держави, запідозрювані в підтримці терористичних груп або у вірогідних зв’язках із ними; проти народів, зрештою, проти владних режимів, обраних самим народом цієї країни. Потрібно зважити ще й на суто політичні аспекти (новий геополітичний поділ світу, формування центрів сили, отже – нового світопорядку), а також

економічні (загострення боротьби за оволодіння природними багатствами – передусім, значними нафтовими копалинами). Лише зазначене дає підстави для суттєвого уточнення семантичного забарвлення цього терміна.

Якщо коротко підсумувати здійснений у підрозділі аналіз, то треба констатувати: терористичні акти 11 вересня 2001 р. багато в чому також обумовлені традиційними імперативами зовнішньої політики країн Заходу; міжнародний тероризм є суттєвою складовою частиною нинішнього динамічного глобалізаційного процесу; суперечлива позиція Вашингтону щодо скоєних злочинних терористичних актів підтверджує його традиційну політику «подвійних стандартів»; події «чорного вівторка» спричинили зростання напруги між Заходом і Сходом (ісламським світом). Аналіз феномену міжнародного тероризму в контексті глобалізаційних процесів свідчить про його багатовимірну природу, що потребує міждисциплінарного підходу до дослідження. Системний розгляд цього явища дає змогу виявити вплив політичних, економічних, соціокультурних й історичних чинників на формування його транснаціонального характеру. Дослідження демонструє, що традиційні силові методи протидії все частіше виявляються неадекватними, що зумовлює необхідність перегляду концепцій безпеки. Отже, актуальним є формування нових парадигм міжнародної безпеки, які враховують як глобальні, так і локальні особливості сучасного світопорядку. Усвідомлення сутності міжнародного тероризму стає основою для розробки ефективних стратегій протидії й забезпечення стабільності в умовах динамічної глобалізованої реальності.

1.3. Методологія та джерельна база дослідження тероризму в контексті міжнародної безпеки

Аналіз наукового доробку свідчить, що здебільшого в оцінці суспільно-політичних та соціальних явищ науковці виходили з таких концептуальних імператив: 1) патерналістської, 2) консервативно-цивілізаційної, 3) протестно-

глобалістської. Означені й інші концепти, безперечно, дають можливість ґрунтовно досліджувати складні процеси нинішніх динамічних трансформувань, однак таке явище, як міжнародний тероризм, потребує специфічного підходу, з огляду на його сутнісну неоднорідність, теоретичну невизначеність, політичну неідентифікованість і надмірну ситуативну зактуалізованість.

Авторське бачення проблеми ґрунтується на використанні основоположних принципів багатовимірності суспільно-політичних явищ, що дає можливість системно досліджувати феномен сучасного тероризму у форматі його тісної пов'язаності зі стратегічними політичними імперативами Вашингтону на тлі глобалізаційних процесів сучасності. Зокрема, це передбачає з'ясування: 1) ролі та місця тероризму як чинника геополітичних трансформувань; 2) використання його як засобу для досягнення гегемоністських устремлінь світовою суперпотугою; 3) впливу на процес трансформування системи міжнародної безпеки; 4) співвідношення деструктивно-конструктивних функцій; 5) політичної обумовленості генези; 6) безперспективності воєнно-силових методів подолання тероризму як явища.

Тобто, йдеться про парадигмальне переосмислення цього суспільного явища, що, відповідно, обумовлює не традиційно-негативістський підхід до нього, а об'єктивно-пізнавальний. Сукупність творчо застосованих у дисертації методів аналізу теми (системного, структурно-функціонального та івент-аналізу) дає змогу виявити й дослідити основні закономірності американської зовнішньополітичної стратегії в контексті антитерористичної кампанії як складової частини глобального процесу вестернізації планети та формування нового світового порядку (у цьому сенсі можна говорити про своєрідну конструктивістську роль тероризму, який за певних обставин здатний посутньо впливати (каталізувати) нинішні глобалізаційні трансформування).

Обрана методика дослідження проблеми уможливлює не лише комплексний, об'ємний аналіз основних аспектів теми, отримання логічно вмотивованих і науково обґрунтованих узагальнень, висновків та пропозицій, а й перевірку їх на предмет наукової верифікації. Відповідно до поставлених завдань, аналіз здійснювали на локальному регіональному та глобальному рівнях. При цьому перевагу надано методу структурно-функціонального аналізу, за допомогою якого досліджували функціональні традиційні особливості зовнішньополітичних стратегій, роль і місце в ній національних інтересів. Метод івент-аналізу, зокрема, застосовано для пояснення ступеня узалежненості тероризму від політичних стратегічних імператив щодо глобалізації міжнародної системи. Системний метод слугував для з'ясування спонукальних мотивів поведінки політичних акторів у великій політичній грі сучасності під кодовою назвою «антитерористична кампанія».

Серед джерел, використаних у роботі, є російськомовні видання. Російськомовні наукові джерела в дисертації використовуються, оскільки дослідження стосується інформаційної безпеки, гібридної війни та міжнародних комунікацій, які стосуються ведення інформаціної війни рф проти України. Використання таких джерел дає змогу отримати більш повну картину досліджуваного явища.

Стрімко змінювані реалії глобалізуючого світу з усією переконливістю показують неможливість адекватно пояснювати їх за допомогою традиційних лінеарних підходів. Нагальні «виклики» часу ставлять складні проблеми перед науковим пізнанням. Як зазначає політолог Б. Канцелярук, «…наприкінці XX – на початку поточного століть цивілізаційний розвиток набув такої динаміки та розмаху, котрі не завжди піддаються поясненню за допомогою положень теорії самоорганізації, а це означає, що найновіша пізнавальна модель світу вже себе вичерпує на тлі тотальної кризи у відносинах природи та людини, загалом кризи світоглядних норм, культури, ідеалів і т. ін. При цьому слід зауважити, що йдеться не про традиційно негативістське явище, а про назрілі передумови переходу до якісно нових форм буття» [85].

Учений обґрунтовує потребу переосмислення епістемологічної наукової парадигми. Одним із варіантів убачається коеволюційна пізнавальна модель, «...за якою світ розглядається як своєрідний комплекс сполучуваних, взаємозалежних, коеволюціонуючих рядів». На думку науковця, така модель найбільшою мірою може прислужитися потребам нинішньої політичної науки, але застосування її потребує не лише критичного осмислення, а й сприйняття як своєрідного продовження, удосконалення вже наявної системи наукового пізнання. «...Вироблення коеволюційної парадигми політології має відбуватися, скажімо, у синтезному форматі співставлення функціональних параметрів парадигм діалектики (еволюції) – синергетики (самоорганізації) – коеволюції (взаємозв'язок – людина, суспільство, природа), причому концептуальний підхід має ґрунтуватися на творчому поєднанні випробуваних часом основоположних імператив кожної з цих теорій, які слід розглядати як єдину систему наукового пізнання явищ дійсності, котрі у своєму невпинному розвиткові дедалі більше ускладнюються для сприйняття, отже, розуміння, пояснення і прогнозування процесів нинішнього глобалізуючого світу» [85, с. 12–13].

Зіткнувшись із величезним масивом наукової й публіцистичної літератури стосовно тероризму у його історичних ідентифікаційних, політичних, юридично-правових, геополітичних, економічних, цивілізаційних, глобалізаційних та інших вимірах, спостерігаємо надзвичайно великий «розкид» тлумачень, оцінок, підходів, рекомендацій та прогнозів. Скажімо, з'ясовано, що самих лише дефініцій понять «терор» існує понад сто. Не простіша ситуація з тлумаченням таких термінів, як «тероризм», «терористичні акти», «терористичні організації», «терористичні групи», «терористична епоха», «терористичні дії», «антитероризм», «антитерористична кампанія», «антитерористична коаліція», «антитерористичні заходи», «антитерористична війна», «антитерористичний світ» і т. ін., які різні дослідники намагаються трактувати по-своєму. Загалом, зрозуміла розбіжність думок і, власне, індивідуальних підходів до розуміння

цього явища негативно позначається на його ідентифікаційній оптимізації, необхідній для вироблення спільних, колективних методів і механізмів захисту. Це щодо спільних політичних рішень. Водночас відчутно дається взнаки така плутанина в юридично-правовій сфері: законодавство кожної країни майже по-різному класифікує поняття тероризму й, відповідно, так само визначає міру відповідальності за скоєння терористичних актів. Тим часом міжнародний тероризм ефективно використовує таку невизначеність у юридичному полі, уніфікація якого, як засвідчують реалії, поки що досить проблематична.

Аналіз доктринальних засад зовнішньої політики, здійснений, американськими дослідниками, показує, що її іманентним чинником традиційно є силовий, який, зазвичай, застосовується сукупно з інформаційним і дипломатичним. Більшість західних аналітиків загалом обґрунтовує виправданість такої поведінки Вашингтону його намаганням обстоювати таким способом не лише національні інтереси США, а й світової спільноти. Інтернаціональні мотиви апологети американського способу життя традиційно використовують для обґрунтування такої тактики Білого дому в розв'язанні міжнародних проблем, зокрема тероризму. Різною мірою це відбито в працях Б. Дженкіса [403]; Р. Бейснера [547]; Д. Белла [531]; Р. Гантера [511]; Г. Ангейєра, М. Гласіуса, М. Келдора [370]; С. Гука, Дж. Спеніера [268]; Р. Кагана [525]; Р. Родмена [361]; А. Гарфінкла [365]; Дж. Торопа [273]; В. Подгореца [483]; Д. Пайпса [529]; С. Купчана [532]; К. Гіршмана [378]; А. Конте [307]; П. Девіса [326].

Зазначимо, що проблеми міжнародного тероризму й, зокрема, його прояв як інформаційного тероризму, відображені в значному перегляді сучасних вітчизняних і зарубіжних учених. Це аналіз кримінально-правових та політологічних вимірів сучасного міжнародного тероризму (В. Антипенко, В. Євдокимов, В. Комісаров, В. Ліпкан, Є. Ляхов, К. Салімов, О. Бардін, В. Вознюк, Н. Лазарєв, С. Телешун, А. Яцько й ін.); концепція інформаційного тероризму, ознаки та основні тенденції його еволюції (А. Баринов, О.

Бойченко, К. Герасименко); прояви інформаційної складової частини політичного тероризму [415, С. 97–122; 541, с. 23; 287]. Кібербезпеку як форму міжнародного тероризму досліджувала О. Л. Доброжанська [58]. Загрози для міжнародних відносин і глобальної безпеки в кіберпросторі розглянула В. Ю. Лук'янчикова [126]. Однак, незважаючи на велику кількість праць із цього питання, воно потребує подальшої наукової розробки, а також більш детального розгляду проблеми.

Проблематикою тероризму й антитероризму цікавляться та досліджують українські науковці, серед яких – В. Ліпкан, Д. Никифорчук, М. Руденко [19]; Б. Канцелярук [42]; В. Грєбцов [107]; П. Ковальов [86]; О. Сушко [105]; Г. Токаревський [223].

Відомий політолог С. Телешун пропонує оригінальні концептуальні підходи до оцінки явища тероризму, що можуть стати принципово значущими для перспективи формування такої підгалузі знання, як терорологія. Він стверджує: «Тероризм з'являється там, де утворюються геополітичні порожнини, "гарячі точки", де суттєво ослаблено владу, неспроможну професійно реалізовувати інтереси громадян і яку ці громадяни не зацікавлені підтримувати, де не працюють міжнародні механізми політичного і правового регулювання розвитку суспільства. Від сплесків тероризму не застраховані ні високорозвинені, ні малорозвинені в економічному й соціальному плані країни з будь-якими політичними режимами та державним ладом» [220]. Як приклад, можна назвати роботу науковця М. Руденка «Інформаційний чинник політики США і Росії щодо міжнародного тероризму», де автор принагідно торкається проблеми тероризму в контексті свого предмету дослідження.

Отже, наявна розбіжність у поглядах науковців на феномен тероризму/антитероризму водночас позначена їхніми суб'єктивістськими підходами, обумовленими традиційним одновимірним сприйняттям та ідеологічними нашаруваннями. Об'єктивне вивчення проблеми передбачає парадигмальне переосмислення традиційного підходу до оцінки цього суспільного явища. Зокрема, ідеться про врахування геополітичних імператив

антитерористичної кампанії. Джерелознавча база дослідження проблеми політичних імператив Заходу в антитерористичній кампанії свідчить загалом, що синдрому антитероризму не вдалось уникнути більшості західних науковців. Альтернативна позиція незначної групи арабських дослідників залишається малопоміченою. Учені неоднозначно оцінюють воєнно-силові методи вирішення міжнародних конфліктів. Тлумачення явища тероризму часто ґрунтується на традиційних імперативах силових методів розв'язання проблем. Дотеперішній досвід антитерористичної боротьби засвідчує, що ефективних альтернатив воєнній силі не знайдено; силовий спосіб розв'язання проблеми тероризму себе не виправдав – навпаки, часто спричинював її загострення.

Науковці, вивчаючи різноманітні проблеми феномену терору, справедливо зазначають, що лише комплексний підхід до їх розуміння може дати підстави для вироблення спільнотою дійових механізмів боротьби з цим явищем. Міркування, безперечно, слушне, однак такою ж мірою й тривіальне. Неформалізований підхід передбачає необхідність акцентування уваги на першопричинах терористичних дій, що пов'язано з потребою здійснення радикальних змін у сферах соціальної справедливості, політичної та ідеологічної толерантності.

У цьому сенсі доводиться визнати, що загалом науково-теоретичне забезпечення потреб розв'язання проблеми міжнародного тероризму ще не є адекватним суворим викликам часу. Наявні наукові доробки з цієї тематики можна вважати, таким чином, лише першою фазою в її гіпотетично фундаментальній розробці.

Експерт із питань тероризму, фашизму й стратегій міжнародних відносин В. Лакер, ґрунтовно досліджуючи феномен тероризму, звертає увагу на реальну загрозу можливого застосування терористськими групами зброї масового знищення на тлі неготовності світової спільноти до самозахисту. Науковець посилається на думку відомого теоретика міжнародного права Т. Дж. Лоуренса, який зазначав свого часу, що «...спроби завадити

використанню знаряддя, яке спричинить руйнування у величезному масштабі, приречені на провал. Людина завжди вдосконалювала своє озброєння й робитиме це доти, поки матиме в цьому потребу» [374]. Нині тероризм набуває нових форм та різновидів, що формуються на симбіозі традиційних видів і проявів. Унаслідок цього розмивається розподільна лінія між терористами й партизанами, між політичними терористами та кримінальними бандами, що ускладнює можливості ефективної боротьби з ним і, зокрема, правової ідентифікації таких злочинів.

Серед низки чинників В. Лакер виокремлює релігійний фанатизм ісламістів Талібану в Афганістані та алжирських терористів, які вдаються до вчинення терористичних актів невеликими групами злочинців – членів різних екстремістських сект й угруповань. Наскільки поширюється зростання такої загрози, можна судити з того, що, наприклад, у такій країні, як Франція, де загалом створення сект перебуває під суворим державним контролем, їх на сьогодні нараховується понад 170. Що тоді говорити про арабські країни та Сполучені Штати, звідки, до речі, інтенсивно імплантується сектантство в постраднянські країни й, особливо, в Україну.

Найбільше занепокоєння у В. Лакера викликає можливість застосування зброї масового знищення терористами, яких підтримує певна держава. Ідеться про вірогідність ведення так званих «сурогатних війн», заохочуваних державою, і це – різновид тероризму завтрашнього дня. Як ілюстрацію наведено приклад Лівії – невеликої країни з населенням 5 млн людей, яка має річний прибуток від добування нафти не більше ніж 1 млрд дол. США, однак її амбіційний правитель намагався розширити сферу свого впливу за допомогою придбання зброї масового знищення (випадок застосування хімічної зброї проти армії Чаду в 1987 р.). Ідеться про традиційну тенденцію бідних країн розв’язувати свої економічні та соціальні проблеми за допомогою територіальної експансії в сусідні країни.

Дослідник визначає найбільш небезпечні, тобто сприятливі для поширення тероризму зони світу: Перу й Мексика з їхніми дошкульними

проблемами корінного населення; Південна Африка, де ситуація з етнічними конфліктами ускладнюється соціальною напругою; Південно-Східна та Центральна Азія з традиційними конфліктними колізіями; Палестина з проблемами арабського населення; Іран із загостреними релігійними й етнічними протистояннями; розпалювання конфлікту між Афганістаном і Таджикистаном, між Індією та Пакистаном і т.ін. При цьому потрібно зазначити, що зазвичай світова спільнота й медіа акцентують увагу лише на значних терористичних актах, учинених у країнах, які відіграють провідну роль у міжнародних справах або є важливими стратегічними об'єктами. Терористичні акти, здійснювані в запеклій боротьбі за владу в Африці, Центральній Азії, Лаосі або Камбоджі, не мають особливого резонансу, а такі дії в Перській затоці або на Індійському субконтиненті кваліфікуються як безпосередня загроза всьому світові [374, с. 20–21]. Можемо принагідно навести приклад такого підходу – це антитерористична війна в Іраку.

Потрібно зазначити, що В. Лакер слушно наголошує на наявності основної причини виникнення тероризму – дедалі зростаючій соціально-економічній поляризації в багатьох країнах «третього світу» й навіть у найбільш багатих суспільствах, де вражаючі соціальні контрасти спричинюють масові протести, заворушення, погроми (як це трапилося в Лос-Анджелесі та інших містах США). Означене, на переконання вченого, може призвести до встановлення жорсткішої (певного різновиду авторитаризму) форми правління, яка довела спроможність успішно протидіяти проявам тероризму.

Німецький аналітик К. Гіршман визначає тероризм, як «...недержавне застосування або загрозу застосування насильства, щоб здійняти паніку в суспільстві, ослабити або навіть ліквідувати його зобов'язання й призвести до політичних змін» [358]. Аналітик вважає, що загалом терористи керуються у своїх діях такими спонукальними мотивами:

– ідеологічними (спрямованими на досягнення політичних або соціальних цілей);

– етнополітичними (здобуття політичної або культурної автономії чи навіть створення власної держави);

– релігійними (нав'язування певних релігійних норм поведінки);

– вузько цільовими (войовнича активність окремих груп або індивідів, спрямована проти дій (бездіяння) урядів у певному питанні);

– ідеями «обраних» (такими вважають себе індивіди з порушеною психікою, котрі переконані в потребі здійснення месіанської місії).

При цьому вчений підкреслює специфічну комунікаційну стратегію терористів: «Партизани хочуть завоювати територію, терористи – мислення» [378]. Пройшовши певні еволюційні етапи, тероризм успішно вдосконалює форми й методи своїх дій, найчастіше виступаючи як знаряддя в рамках ширших конфліктів і протистоянь: у багатьох «внутрішньоцивілізаційних конфліктах він залишається привабливим знаряддям для будь-якої малої групи, яка претендує на непропорційно великий вплив» [378, с. 300]. Водночас дослідник звертає увагу й на іншу взаємопов'язаність тероризму з релігійністю. У другій половині XX ст. втричі зросла кількість різноманітних фундаментальних рухів і, відповідно, різко збільшилася чисельність релігійних терористичних груп (вони становлять четверту частину наявних теругруповань).

К. Гіршман убачає потенційну загрозу з боку кібертероризму, який кваліфікує, як «...навмисну, політично мотивовану атаку на інформацію» з метою досягнення певних цілей. А взагалі можливості хакерів, на думку американських фахівців, дають змогу за відповідної фінансової підтримки зруйнувати таку державу, як Сполучені Штати. «Тероризм – це дещо більше, ніж наявна зброя, дійові особи та мотивації, – підкреслює вчений. – Це один із різновидів боротьби на політичній арені» [378, с. 309], – проти цього зла можливо боротися лише консолідованими зусиллями світової спільноти.

В іншій своїй праці [377] згадуваний вище дослідник фокусує увагу на потребі нових вимірів сучасного тероризму, який пов'язаний так само з діяльністю «Аль-Каїди». Спонукальні мотиви тероризму – націоналістичні та

світоглядні – позначалися на трансформуванні його основних видів, поєднанні традиційних і новітніх форм його прояву (звичайного тероризму, тероризму із застосуванням зброї масового знищення, кібертероризму). При цьому підкреслюється явно політичний характер вимог Усами бен Ладена, в основі яких – суто релігійне рішення: убивати американців та їхніх друзів у всьому світі – обов'язок кожного мусульманина. Ширше його політична програма передбачає повалення чинного політичного режиму в мусульманських країнах; звільнення ісламських країн від американської військової присутності; відмову від західних цінностей і стандартів у політиці та економіці; боротьбу з Ізраїлем та його панування над Палестиною; контролювання й використання мусульманами енергетичних ресурсів і корисних копалин на ісламських територіях; політичне облаштування ісламських держав на основі принципів шаріату.

На початку 2000-х рр. К. Гіршман висунув припущення, що найбільшу загрозу в найближчі часи становитиме так званий «технологічний тероризм», ґрунтований на застосуванні сучасних засобів масового знищення людей. Зросте загроза використання хімічних, мікробіологічних та біологічних знарядь терору, що мають переваги над атомною зброєю в сенсі технологічного виготовлення. З огляду на надзвичайну вразливість нинішніх систем господарювання розвинутих країн світу (факти розкрадання урану на атомних станціях, незадовільна охорона хімічної й бактеріологічної зброї, яка легко може опинитися в руках терористів), обумовлено потребу створення в Америці кризового уряду або конституційної диктатури (зі збереженням конституційних основ правління, але наділеної необмеженими повноваженнями).

Нинішня епоха тероризму, на думку французького аналітика А. Котта, характеризується чітко позначеними його видами – економічний, політичний, соціальний та інформаційний. Щодо політичного, то він ґрунтується на ігноруванні лідерів країн, його важко перемогти, бо він використовує слабкість і «дряблість» західних суспільств, які прагнуть будь-що зберегти

свій комфортний стан і бояться ризику та жертв, особливо в політиці. Отже, об'єктами політичного тероризму зазвичай є уряди, довіру до котрих силкуються підірвати своїми діями терористи з метою збільшення кількості прихильників зміни чинного режиму влади [309].

Італійський дослідник феномену тероризму В. Парсі зосередив увагу на з'ясуванні таких трьох аспектів, пов'язаних із вчиненням терористичного акту 11-го вересня. Перший – кваліфікувати його як війна чи терор? За масштабами заподіяного зла ця подія аналогічна тому, що вчинив свого часу А. Гітлер: «...тотальна й абсолютна зневага до людського життя і навмисність наміру знищення» [473]. За статутом НАТО, збройна агресія щодо його учасників вважається нападом, на який має бути дана адекватна відповідь. В. Парсі, беручи до уваги сукупність чинників акції «чорного вівторка», вважає, що «масштаби цієї бійні та спосіб її здійснення змушують припускати, що 11 вересня – це перший день неоголошеної війни» [473, с. 414].

Із цим пов'язаний безпосередньо другий аспект, суть котрого полягає в тому, чи можна стверджувати, що стан війни обумовлюється також і «приватними» суб'єктами – терористичними організаціями або групами? Відповідь на це аналітик пропонує шукати у сфері кардинальної зміни системи міжнародних відносин, унаслідок чого на міжнародній арені з'явилися нові суб'єкти – транснаціональні корпорації, асоціації, кримінальні картелі, неурядові організації, церкви з міжнародною мережею суспільних поглядів, глобальні товариства й т. ін.

В. Парсі намагається з'ясувати й такий важливий аспект проблеми: акт 11 вересня є свідченням прогнозованого зіткнення цивілізацій чи лише релігійною війною? Оскільки сама держава та все, пов'язане з цим інститутом, є продуктом західної цивілізації, то, на його думку, згадані терористичні акти на Америку є початком «...мілітаризації конфліктів між цивілізаціями, що змушують не стільки до стикування або до зіткнення, скільки до насильницького співіснування» [473, с. 423].

Думаємо, однак, таке підтвердження відомої прогнозної версії С. Гантінгтона не досить аргументоване, позаяк й досі ще багато чого не з'ясовано в цій трагічній справі, а численні здогади і припущення не отримали фактичного підтвердження. Тим часом, мало, скажімо, приділяється уваги таким посутнім чинникам, як різний рівень розвитку самого мусульманського світу або використання антитерористичної кампанії з метою реалізації доктринальних зовнішньополітичних засад однієї з провідних потуг світу.

Досліджуючи міжнародно-правові наслідки боротьби з тероризмом і репресій проти Афганістану, А. Конте звертає увагу на те, що «хоч інколи цілі терористів підтримуються досить широкими верствами населення, їхні методи, зазавичай, викликають огиду. Зараз багато хто підтримує боротьбу з тероризмом, однак при цьому підкреслюється, що «боротьба завжди повинна бути пропорційною та фокусуватися на власне терористах», бо не можна боротися з ними їхніми ж методами, тобто обрушувати терор і насильство на невинне громадянське населення, особливо дітей» [307]. А. Конте зазначає чітку позицію в цьому питанні Організації Об'єднаних Націй, Ради Безпеки котрої вже 13 вересня 2001 р. оперативно відреагувала на акт резолюцією 1368, у котрій осуджувався цей напад і кваліфікувався як такий, що становить загрозу міжнародному миру й безпеці. Наступною своєю резолюцією (1373) Рада Безпеки зажадала від усіх країн запобігання та заборони фінансування терористичних актів, а також співробітництва в питаннях екстрадиції й обміну інформацією про діяльність терористичних організацій. «Оскільки це рішення було прийняте відповідно до VII розділу Статуту ООН, то, за міжнародним правом, дотримання цієї резолюції є обов'язковим» [307, с. 413]. Водночас дослідник підкреслює, що зазначені документи визнають і невід'ємне право на самооборону, тобто імпліцитно передбачають можливість застосування у відповідь сили. Через те, вважає А. Конте, на ці документи «...можуть посилатися США для виправдання будь-якого застосування сили як акту відплати» [307, с. 413].

На його думку, проблема використання антитерористичних інструментів у міжнародному праві й досі не розв'язана через різні причини. По-перше, багато країн так і не ратифікували документи Ради Безпеки; по-друге, існує чимало плутанини та розбіжностей у конвенціях, спрямованих на боротьбу з терористичними злодіяннями. Позначається також і відсутність спільного підходу до визначення самих понять «тероризму» та «пропорційних заходів» спротиву його проявам. У зв'язку з подіями 11 вересня 2001 р. потребують відповідного коригування статті Міжнародного кримінального суду (Римського статуту, прийнятого 17 липня 1998 р.).

Деякі правознавці дотримуються думки, що поняття тероризму підпадає під юридичне визначення «злочини проти людяності», де зазначається й напад на цивільне населення. «Очевидно, – припускає А. Конте, – що у світлі нещодавніх нападів на США терористичні акти цілком підпадають під це визначення. Деякі країни можуть заперечити, що поняття "злочини проти людяності" поширюються лише на держави, а не на неурядові терористичні групи. Проте ООН явно дотримується іншої думки» [307, с. 414]. Жорстокість вересневого акту відчутно актуалізувала проблему репресій, однак і тут немає спільного підходу. Наприклад, Г. Кіссінджер заявив, що кожна держава, яка потурає терористам, повинна заплатити за це «непомірну ціну». К. Аннан застерігає, що дії у відповідь із боку Америки «повинні зміцнювати міжнародний мир та безпеку, а не піддавати народи новим випробуванням».

Така невизначеність у правовому полі дає можливість по-різному тлумачити як саме явище тероризму, так і застосування механізмів ефективної боротьби з ним. З огляду на це, ініціатори антитерористичної кампанії намагаються всіляко виправдати свої репресивні дії, посилаючись при цьому на згадані резолюції Ради Безпеки й загалом на антитерористичну позицію самої ООН.

Отже, можна стверджувати, що проблема міжнародного тероризму не лише стала предметом всебічного дослідження, а й, з іншого боку, обумовила проблему вироблення адекватного концептуального підходу до її розв'язання.

Акцентування уваги на самих наслідках терористичних актів чи, тим більше, спроби обґрунтування доцільності застосування силових методів для викорінення тероризму, як свідчить життя, виявляються хибними й небезпечними. Міжнародний тероризм – явище не ситуативне, воно традиційно дошкуляє цивілізаційному поступові. Не можна погодитися з тезою про те, що тероризм є проблемою № 1 сучасності: його слід розглядати в контексті взаємопов'язаних складових частин процесу глобалізації.

Отже, міжнародний тероризм є складним феноменом, що формується на перетині глобалізаційних процесів, цивілізаційних протистоянь та соціальних трансформацій. Його сучасна природа охоплює не лише насильницькі акти, але й глибоко політичні, ідеологічні та інформаційні складники. Традиційне тлумачення тероризму як суто кримінального явища є обмеженим і не враховує впливу структурної нерівності, геополітичної конкуренції та кризи цінностей. Масштабність і транснаціональність терористичних проявів свідчать про потребу переосмислення підходів до міжнародної безпеки. Комплексний міждисциплінарний аналіз дає підставу розглядати тероризм як глобальний виклик, що потребує нових парадигм реагування. Сучасний тероризм є складним і мінливим явищем, як поглиблюється на тлі соціальної нерівності, релігійного радикалізму та глобалізаційної нестабільності. Його новітні форми –інфомаційний теороризм, кібертероризм і використання зброї масового знищення – вимагають переосмислення підходів до безпеки. Ефективна боротьба з тероризмом потребує не лише силових, а й системних превентивних заходів, спрямованих на усунення першопричин.

ВИСНОВКИ ДО РОЗДІЛУ 1

Тероризм у сучасній теорії міжнародних відносин розглядають як складне, багатовимірне явище, що виходить за межі звичайного насильства. Його визначення залишається дискусійним через політичну заангажованість і широкий спектр форм прояву – від фізичних атак до інформаційного впливу.

Міжнародний тероризм є глобалізаційним викликом, що відображає глибокі цивілізаційні суперечності та нерівність у розвитку. Для ефективної протидії йому потрібна не лише силова відповідь, а й перегляд підходів до глобальної взаємодії з урахуванням культурного плюралізму й справедливості. Аналіз сучасного тероризму засвідчує його складність, багатовимірність і здатність адаптуватися до глобальних трансформацій. Попри наявні наукові дослідження, теоретичне забезпечення боротьби з терористичними загрозами поки що не відповідає реаліям. Серед головних причин тероризму дослідники виокремлюють соціальну нерівність, релігійний фанатизм, радикалізм, а також дестабілізацію, спричинену глобалізаційними процесами.

Силові методи боротьби з тероризмом виявляються обмеженими й часто контрпродуктивними. Реальна протидія можлива лише за умови усунення глибинних причин: бідності, соціального відчуження, релігійної нетерпимості та політичної дестабілізації. Отож необхідним є перехід від реактивної моделі до стратегії упередження, що передбачає широке міжнародне співробітництво й міжсекторальну координацію. Тероризм – не лише загроза безпеці, а й виклик глобальній справедливості та цивілізаційній стійкості.

Сучасний тероризм трансформувався в глобальну загрозу, яка використовує медіа, кіберпростір і соціальні мережі для досягнення політичних цілей шляхом залякування й дестабілізації. Теоретичні підходи – неореалізм, неолібералізм, конструктивізм – трактують його як інструмент впливу, виклик для інституцій або соціальний конструкт. Отже, концепт тероризму потребує комплексного осмислення та адаптації політик безпеки до нових форм загроз у глобалізованому світі. Особливу тривогу викликає поява нових форм тероризму – інформаційного, кібер- і технологічного, пов’язаного з імовірним використанням зброї масового знищення. При цьому змінюється не лише тактика, а й суб’єкти: до традиційних груп додаються транснаціональні і мережеві утворення, що функціонують у гібридному форматі. Це зумовлює потребу в переосмисленні концептів безпеки та війни,

адже тероризм дедалі більше постає як політичний інструмент у глобальних конфліктах.

Інформаційний тероризм у цифрову епоху перетворився на одну з найбільш загрозливих складових частин сучасного міжнародного тероризму. Його вплив охоплює не лише технічну інфраструктуру, а й глибоко проникає у масову свідомість, використовуючи засоби маніпуляції, кіберзлочини та цілеспрямовані інформаційно-психологічні операції. Аналіз провідних наукових підходів свідчить, що це явище проявляється в різноманітних формах – від поширення дезінформації й пропаганди до атак на критичні цифрові системи державного значення.

Особлива загроза інформаційного тероризму полягає в його латентності, високій швидкості розповсюдження та здатності підривати довіру до державних інституцій, демократичних цінностей і суспільного порядку. В умовах, коли розмежування між війною та миром дедалі більше стирається, інформаційний вплив набуває сили, зіставної з традиційною зброєю. У зв’язку з цим протидія інформаційному тероризму повинна розглядатися як один із ключових напрямів забезпечення національної та глобальної безпеки. Це потребує модернізації нормативно-правової бази, зміцнення цифрової стійкості суспільства й створення ефективної системи виявлення та нейтралізації інформаційних загроз.

У сучасних умовах гібридних конфліктів і масових інформаційних атак поняття «інформаційна стійкість» набуває ключового значення для системи міжнародної та національної безпеки. Вона постає не лише як елемент протидії дезінформаційним впливам, але й як складова частинагуманітарної, когнітивної й політичної стабільності суспільства.

РОЗДІЛ 2
ІНФОРМАЦІЙНИЙ ВИМІР ТЕРОРИЗМУ В ГЛОБАЛЬНОМУ СЕРЕДОВИЩІ БЕЗПЕКИ

2.1. Події 11 вересня 2001 р. як детермінанта цифрової трансформації тероризму

Події 11 вересня 2001 р. сколихнули світову спільноту, поставивши її перед проблемою: дати гідну відповідь викликові сучасності, що зумовило потребу нагального переосмислення традиційного концептуального підходу до явищ радикально змінюваного світу. Америка змушена була взяти на себе ініціативу підготовки такої відповіді ще й для того, щоб розвінчати сумніви, які почали дедалі частіше з'являтись у світової спільноти, щодо можливості збереження нею своєї лідируючої позиції на планеті. Склалося так, що жорсткому випробовуванню піддано зовнішньополітичні стратегічні імперативи Сполучених Штатів, ґрунтовані на ідеях американської винятковості та месіанського призначення.

Реакція адміністрації Дж. Буша-молодшого на трагедію «чорного вівторка» показала, що вона не змогла вийти за рамки традиційного рефлексування на факти, які зачіпають національні інтереси Америки. Крім того, значною мірою тут позначилось і прагнення адміністрації виокремитися на тлі діяльності своєї попередниці – адміністрації Б. Клінтона, котру так гостро критикували за надмірне переймання проблемами інших країн на шкоду своїм внутрішнім. Зокрема, закиди стосувалися ставлення Б. Клінтона до провідних європейських держав, яким він потурав у прагненні реалізувати європоцентристську ідею, та явної поблажливості до кремлівських «примх» щодо силкування реанімувати колишній імперський статус.

Тим часом, як відомо, клінтонівський зовнішньополітичний курс характеризувався виваженістю й поміркованістю. Щодо росії, наприклад, то він обумовлювався наявністю грізного військового потенціалу, який

потенційно становить загрозу світовій спільноті. До того ж треба особливо враховувати специфічний характер відносин цих країн, стратегічні доктрини котрих мали чимало спільного. Цим пояснюється, скажімо, те, що Білий дім намагався з розумінням ставитися до іміджевих проблем «скривдженої» росії, до її дій у Чечні або в Абхазії. Своєю чергою, російське керівництво не виставляло особливих претензій (хоч і на декларативному рівні не схвалювало) до американської «Бурі в пустелі», бомбардувань у Косово, антитерористичних воєн в Афганістані та Іраку. Тобто це свідчить, що загалом ці дві потуги часто знаходили спільну мову щодо підходу до вирішення різних конфліктних ситуацій у світі.

Більше того, події після 11 вересня показали, наскільки стратегічні інтереси цих країн були близькими: в антитерористичному тотальному поході проти переважно підозрюваного ворога простежувалася тенденція до узгодження дій Вашингтона й Москви. Зрозуміло, звичайно, що стратегічна мета, ресурсні можливості, тактичні засоби, а отже, і ступінь вірогідності на отримання певних політичних чи суто матеріальних дивідендів у них досить відмінні. США прагнули не просто географічно розширити свою сферу впливу, а де-факто – підтвердити претензії на світове домінування в розв’язанні міжнародних проблем, використовуючи при цьому моральний, політичний і матеріальний ресурс своїх коаліціянтів.

Якщо зважити на наявні стереотипи оцінки явища тероризму, особливо в міжнародному вимірі (хоч така дефініція досить-таки умовна), за його сутністю, формою, видом, мережею поширення, зростаючими можливостями використання досягнень сучасної техніки й т. ін., то стає очевидним загалом лінійний підхід до його сприйняття як феномену сучасного глобалізаційного процесу. Адже при цьому випускається з уваги найсуттєвіше: справжні причини виникнення; спонукальні мотиви скоєння терористичних актів; неоднозначна їх оцінка (наприклад, чому певні політичні кола та верстви громадськості підтримують такі акції); визначення його місця в процесах поступу, тобто з’ясування не лише суто деструктивного впливу на їх перебіг;

співвідношення тероризму з такими негативними суспільними явищами, як кризи, конфлікти, війни; зрештою, роль тероризму у формуванні нового світового порядку (використання як засобу для досягнення певних геополітичних амбіцій) і т. ін.

Як практично формуються стереотипи сприйняття феномену тероризму, засвідчує приклад використання Вашингтоном могутнього ресурсу сучасних медіа для доведення нагальної необхідності застосувати воєнні сили в Іраку через те, що на його території є зброя масового знищення. До речі, так само переконувалася світова громадськість у тому, що саме після 11 вересня 2001 р. тероризм став головною загрозою існування на планеті (хоча поява териризму, як відомо, сягає в глибину століть).

20 серпня 2002 р. віцепрезидент США Д. Чейні оприлюднив заяву про потребу воєнної акції, мотивуючи це тим, що в американського керівництва немає сумнівів щодо наявності на території Іраку ядерної зброї. 8 вересня того ж року журналісти газети «The New York Times» Ю. Міллер і М. Гордон опублікували статтю про вірогідність виробництва в Іраку зброї масового знищення, посилаючись при цьому на урядові джерела інформації. Визнаючи, що поки режимові С. Хусейна ще далеко до створення ядерного арсеналу, вони водночас зазначили: «… Першим димком може стати ядерний гриб». Того самого дня високопоставлені чиновники Білого дому виступили з пресрелізами, ґрунтованими на згаданій публікації. Військові експерти виявили, що журналісти зробили хибні припущення, оскільки випустили з уваги істотні факти (ідеться про можливість використання труб зі спеціального сплаву, які призначалися для запуску звичайних ракет і для корпусів бойових ракет). «Розуміння справжнього призначення цих предметів – надзвичайно складна справа», – визнав провідний військовий інспектор Д. Олбрайт. Тим часом репортер «The Washington Post» Дж. Уоррік указав на наявні розбіжності в оцінках самих військових експертів [540].

Здійснені численні інспекції не підтвердили факту наявності ядерної зброї в Іраку. Такого висновку дійшли й журналісти, які провели автономні

розслідування цього питання. Тим часом уже концентрована увага медіа до цієї актуальної теми позначилася на формуванні в читачів і слухачів схвального ставлення до намірів уряду завдати терористам адекватного удару. «Контраст між шаленим обуренням після війни та боязким меканням до початку воєнних дій виокремлює найбільш тривожну рису американської журналістики – стадний менталітет» [540].

Ідеологічна заангажованість, хоч і не такою мірою, притаманна й американським дослідникам, яким зазвичай непросто обстоювати опозиційні погляди. Крім того, потрібно враховувати також рівень патріотичності американських громадян, ступінь довіри тим, кого вони обрали у вищі державні органи для захисту своїх національних інтересів. Означене обумовлює переважно одновимірні концептуальні підходи до оцінки явищ тероризму, про що свідчить численна наукова література. Зазначається, зокрема, що хоч сучасний тероризм уможливився в контексті процесів глобалізування, однак він є його породженням. Тероризм здебільшого спричинений:

– диференціацією країн на бідні та багаті, унаслідок чого створюється підґрунтя для формування терористичного «інтернаціоналу» під зеленим прапором ісламу;

– регіональною нестабільністю, що провокує терористичні акти;

– інформаційною революцією, поширенням електронних медіа, які використовуються як інструмент маніпулювання масовою свідомістю;

– загостренням суперечностей між наявними системами цінностей – західною, яка виявляється далеко не універсальною, і системою ісламського світу, яка є як певним альтернативним варіантом.

Очевидним є факт, що вересневі терористичні акти здійснювалися з наміром завдати превентивного удару по американоцентричній концепції нового світопорядку, по однополюсному проєктові глобалізування планети. Не дивно, що теракти викликали в Америці шоковий стан: уперше за останні 150 років вона зазнала зовнішнього дошкульного нападу, який поставив під

сумнів не лише всю систему безпеки, а й систему сповідуваних цінностей. Подія сприймалася на рівні національної трагедії, що й обумовило загалом рішення уряду завдати у відповідь нищівного удару. Зачеплено амбіцію потуги, яка має колосальну військову та економічну могутність, володіє 40 % світових військових витрат, 20 % світового ВВП. Водночас треба відзначити, що таке потрясіння відіграло й позитивну роль не лише в консолідуванні нації, а й спричинило кардинальний перегляд оборонної доктрини, суттєвого коригування зовнішньополітичної парадигми в напрямі реалізації гегемоністської стратегії в контексті антитерористичної війни.

Вашингтон заявив, що «боротьба зі світовим злом» буде тривалою, важкою й потребуватиме колективних зусиль світової спільноти, однак він не збирається виробляти таку спільну стратегію, яка б передбачала докорінні зміни в глобальній економічній політиці та в самій геополітиці. Натомість Сполучені Штати виконують суто внутрішні завдання – дати належну відповідь на запити «американської вулиці», тобто показово покарати організаторів терористичних актів; у зовнішніх відносинах – продемонструвати ефективність воєнно-силового методу боротьби з тероризмом, чим підтвердити домагання на глобальне лідерство й реалізацію американського сценарію світового порядку. Мета виправдовує засіб: головне – довести спроможність «захистити демократію» в усьому світі.

Розпливчаста адресність можливої антитерористичної кампанії та явне політизування міжнародного тероризму дають підстави констатувати, що Америка здобула в цій масштабній кампанії головну стратегічну перемогу – відстояла й зміцнила своє право одноосібно розв’язувати світові проблеми. Як бачимо, традиційний концептуальний підхід до стратегії американізму залишився стрижневим, однак був ситуативно підкорегований до реалій голобалізуючого світу [29].

Тим часом світ по-різному сприймав та оцінював ці колізії, проте треба визнати, що серйозних альтернатив вашингтонському «проєктові» не простежено. Спроби протиставити як опонентів ісламський світ, Китай,

Європу або росію на тій підставі, що США втрачають позицію, оскільки дискредитовані способом утвердження демократичних цінностей, опинилися взагалі в стані глибокої рецесії, видаються лише гіпотетичними прогнозуваннями.

Глобалізаційний характер терористичних актів 11 вересня багато в чому обумовив і потребу спільної відповіді на такий злочинний акт, адже стало зрозуміло, що ефективно боротися з цим зухвалим суспільним явищем не під силу навіть такій могутній потузі, як Сполучені Штати. Тим самим спростовано легендарну безпекову невразливість Америки з її нібито суперсистемою протиповітряної оборони, найкращою структурою розвідувальної служби й ін.

Аналіз фактів і матеріалів дав підстави дослідникам констатувати: «Реально ми спостерігаємо неоголошену війну проти США, розпочату невідомим та невидимим противником, яка ведеться в зовсім невідомій досі формі і за неписаними законами. Беручи до уваги обставини, ми можемо назвати її цивілізаційною, оскільки немає жодного сумніву, що для її проведення задіяні представники Азії, Європи та іммігранти в США» [208, с. 340]. Думаємо, якраз останнє й дає привід для такого сумніву, оскільки достовірно встановлено причетність до скоєння теракту саме осіб арабського походження та, по-друге, є переконливі докази аналітиків й офіційних осіб (зокрема й американців) щодо того, що цей конфлікт не можна вважати міжцивілізаційним.

Терористичні вересневі акти спричинили нову гонку у сфері реалізації геополітичних імператив країн-лідерів, тобто знаменують новий етап трансформування системи міжнародних відносин. Так, свої дивіденди із ситуації намагається здобути росія, у військовій доктрині котрої, зокрема, зазначається: «а) останнім часом у практиці міжнародного життя намітилося затвердження політики застосування сили без санкції міжнародного співтовариства» [224], і, якщо така поведінка буде усталюватися, то «...Росія залишає за собою право діяти таким же чином». Політичний оглядач В. Шкода

з цього приводу зауважує: «Якщо США взялися по-своєму трансформувати арабський світ, не нехтуючи силовими методами, то й ми маємо право таким же чином наводити лад у просторі наших інтересів. Відмінність від минулої епохи суттєва. Тоді обидві сторони сповідували доктрину заборони, і щойно одна сторона посилювала свій вплив у якій-небудь точці планети, туди відразу вирушала й інша сторона. Тепер пропонується інший розклад – ви займаєтеся країнами, проблемними для вас, а ми будемо займатися країнами, проблемними для нас» [244]. Отже, можна говорити про серйозні резонансні наслідки воєнної відповіді США на вересневий терористичний виклик.

Військовий аналітик І. Шаблінський, досліджуючи типи моделей організації ресурсів для суспільно-політичної дії, виокремлює такі дві їхні характерні ознаки: а) ставлення до ресурсів – збереження (силова модель) та руйнування (насильницька модель); б) корисність дії цих моделей у досягненні поставленої мети. Щодо способів реагування на історичні виклики, то він вважає, що «виникнення спалахів насильства, переростання їх у масові руйнівні дії та війни, що ведуться державами і народами, – це є свідчення хибності обраних суспільних цілей, моделей організації ресурсів й, як наслідок, регресивного розвитку людських спільнот» [241].

Події 11 вересня 2001 р. та наступна антитерористична війна значною мірою прискорили процеси геополітичних трансформувань у макрорегіоні Центральної й Південної Азії. При цьому «Центральна Азія нині стикається з троїстою проблематикою, науково актуалізованою та політично артикульованою: нова пострадянська центральноазіатська геополітика наддержав і загалом геополітична трансформація регіону після 11 вересня 2001 р.; входження США до регіону Центральної Азії – Хартленд Євразії, – яке неминуче змінює статус-кво в цій частині світу; налагодження під час антитерористичної кампанії в Афганістані стратегічного партнерства США з Узбекистаном» [542]. Цим, до речі, підтверджуються прогнози американських аналітиків М. Хаунера й Д. Пайпса, котрі ще в дев’яності роки зазначали, що після розпаду Радянського Союзу в цьому регіоні розпочнеться

фундаментальна геополітична трансформація, яка позначиться на долі всього макрорегіону Центральної та Південної Азії [375].

Антитерористична кампанія формувалася за допомогою не лише активної діяльності компетентної американської дипломатії, а й завдяки використанню потужного інформаційно-технологічного чинника. Отже, Заходом продемонстровано його незаперечну перевагу, передусім, перед ісламським світом, не лише в економічній, соціальній, політичній та воєнній сферах, а й інформаційній. Унаслідок цілеспрямованої, професійно відфільтрованої пропаганди створено видимість «одностайності» Світового Співтовариства щодо проблеми покарання терористів безпосередньо в місцях їх віртуального перебування, тобто на території Афганістану. При цьому до «непокараних» Білий дім застосовував різноманітні форми психологічного тиску, погроз позбавити можливості користуватися західними інвестиціями та взагалі опинитися в цілковитій міжнародній ізоляції, що й дало певні результати. Як зазначає С. Б. Кримський, «найпоказовішим прикладом цього став розгром режиму талібів в Афганістані наприкінці 2001 р. Водночас чимало злочинних режимів існує й серед держав, що орієнтуються на Захід, тому вони фактично уникають його критики та осуду» [109, с. 661–662].

Потрібно зауважити, що навіть за такої тотальної обробки громадської думки до табору антитерористів, який формував Вашингтон, увійшло лише до трьох десятків країн, при цьому дали згоду на участь у війні лише сім. Отже, попри все, такої підтримки, на яку сподівався Білий дім у підготовці до розв’язання антитерористичної війни, він не отримав. Тим часом треба визнати, що поширена світовими медія ідея зображення тероризму як небезпеки № 1 для самого існування людства, котре, з огляду на це, мало сконсолідувати свої зусилля для знищення цього зла, стала предметом пильної уваги багатьох дослідників-суспільствознавців, передовсім, апологетів західної моделі розвитку. Щоправда, і серед них простежено неоднозначний підхід до оцінки, зокрема доцільності застосування Вашингтоном саме силових методів боротьби з тероризмом, причому останнім часом дедалі

більше зростає кількість тих, хто засуджує таку тактику американського уряду.

Рада Безпеки ООН тривалий час усебічно вивчала ситуацію, однак серйозних підстав для ухвалення санкції на ведення воєнних дій, як цього вимагала Америка, не було. Незважаючи на це, Вашингтон удався до вчинення акту, який, за нормами міжнародного права, кваліфікується як агресія. За видовою дефініцією він підпадає під означення «державний міжнародний тероризм», на відміну від традиційного – державного тероризму, тобто внутрішнього терору правлячого режиму проти власного народу.

Так що говорити про сутність антитерористичної коаліції чи, тим більше, наявність антитерористичного світу треба з великою мірою умовності: у кожному конкретному випадку ці концепти потрібно розглядати крізь призму нашарувань абстракції, за якою приховується ідеологічна заангажованість тих кіл, котрі були зацікавлені в застосуванні саме такого виду відповіді на злочинні дії терористів.

Загалом, серед дослідників превалює інтерес до всебічного аналізу правових аспектів тероризму, тобто власне до самих наслідків цього феномену. Це, безперечно, досить суттєвий аспект, тим більше, що реалії настирливо обумовлюють потребу вироблення консенсусу в чинному міжнародному праві для ефективної боротьби з цим планетарним злом. Водночас очевидно, що такий підхід можна кваліфікувати лише як паліативний: не менш (а, можливо, і більш) важливим і продуктивним є зосередження уваги на з’ясуванні та усуненні основних причин, які призводять до виникнення тероризму.

На наше переконання, при цьому доцільно виходити з оцінки цього явища – після 11 вересня стався розкол світової спільноти на тих, хто співчуває жертвам цих актів, і тих, хто підтримує злочинців. На відміну від відомих проявів націоналізму, антисемітизму та фашизму, феномен тероризму має не локальний, а загальносвітовий характер і прямо пов’язаний із різними проявами процесу глобалізації в його нинішньому вигляді.

Отже, ми вважаємо, що події 11 вересня 2001 р. стали символом початку нової епохи глобального тероризму, який виявив вразливість навіть найпотужніших держав і зумовив трансформацію міжнародної системи безпеки. Вони не лише поставили під сумнів ефективність традиційних моделей реагування, а й призвели до перегляду геополітичних стратегій, зокрема легітимізації силових дій під гаслом боротьби з терором. Водночас світова спільнота так і не досягла єдності щодо методів протидії тероризму, що засвідчує ідеологічну та інституційну фрагментованість у боротьбі з цим багатовимірним викликом.

2.2. Інформаційний тероризм у структурі сучасного міжнародного тероризму: сутність, механізми, прояви

Інформація стала стратегічним ресурсом, порівнюваним за значенням із територією, енергетикою чи людським капіталом. У зв'язку з цим поняття інформаційної безпеки набуло винятково важливого значення в структурі як міжнародної, так і національної безпеки будь-якої держави.

Міжнародна безпека – це система заходів, здійснюваних державами та міжнародними організаціями, спрямованих на запобігання воєнним конфліктам, захист територіальної цілісності, гарантування миру й стабільності у міжнародних відносинах [401]. Досить часто їх пов'язують із вивченням загрози, використанням та контролем військової сили [470]. Але сучасні дефініції значно ширші, оскільки вони включають інші види загроз, як-от: тероризм, кіберзагрози, екологічні кризи, пандемії тощо [526]. Передусім концепція «людської безпеки» – акцент не лише на державу, але й на захист окремої людини від біологічних, економічних, екологічних ризиків; розширення об'єкта безпеки – не лише держава (національна безпека), але й регіональні блоки, міжнародна спільнота (глобальна безпека) [457]; процес сек'юритизації – питання, які виводяться зі «звичайної політики» в категорію «екзистенційної загрози», щоб виправдати екстраординарні дії. Отже,

міжнародна безпека – це багаторівневе й багатовимірне явище, яке охоплює не тільки оборонні функції, але й політичні, економічні, соціальні, екологічні аспекти.

У таб. 2.1 висвітлено перелік ключових гравців, структури, які відіграють роль у забезпеченні міжнародної безпеки та їхні функції. Важливо, що інституції можуть бути формальними (офіційними міжнародними органами) або неформальними (наприклад, процеси нормотворення, звичаї).

Таблиця 2.1

Основні інституції й органи в системі міжнародної безпеки*

Рівень	Інституція / орган	Функції в міжнародній безпеці
1	2	3
Глобальний	Організація Об'єднаних Націй (ООН)	Основна платформа для підтримання миру, вирішення конфліктів, санкційної політики, миротворчих операцій
	Рада Безпеки ООН	Прийняття зобов'язуючих рішень (санкції, воєнні операції) відповідно до Статуту ООН
	Міжнародний суд / Міжнародний кримінальний суд	Судові інстанції для вирішення міжнародних спорів, покарання осіб за міжнародні злочини
	Регіональні організації безпеки	НАТО, Організація з безпеки та співробітництва в Європі (ОБСЄ), Африканський союз, АСЕАН, Ліга арабських держав тощо
	Інші механізми	Організації з контролю озброєнь (Режим Вассенар), договори про нерозповсюдження ядерної зброї (ДНЯО), конвенції з хімічної та біологічної зброї тощо

Національний рівень	Міністерства оборони, служби безпеки, розвідки	Визначення національної стратегії безпеки, оборонні спроможності, контрзаходи проти внутрішніх, зовнішніх загроз
	Законодавство та суд	Закони щодо оборони, надзвичайного стану, кібербезпеки, протидії тероризму; контроль конституційними й судами
Цивільне / неурядове середовище	Міжнародні неурядові організації (НУО)	Моніторинг дотримання прав людини в контексті безпеки, раннє попередження конфліктів, гуманітарна допомога
	Експертні центри, аналітичні інститути	Дослідження загроз, прогнози, рекомендації політикам

**Джерело: розробка здобувача.*

Нормативно-правова база міжнародної безпеки, на яку спираються інституції й заходи, складається зі Статуту ООН (Charter of the United Nations, 1945 р.) – основного документа, який установлює порядок використання сили, ролі Ради Безпеки, принципів суверенітету; Договорів із контролю над озброєннями та нерозповсюдженням (Договір про нерозповсюдження ядерної зброї (ДНЯО), Конвенції про заборону хімічної зброї, біологічної зброї; Договори про обмеження стандартних видів озброєнь, ракетних комплексів тощо); Міжнародного гуманітарного права та права людини (Женевські конвенції й протоколи, загальні міжнародні пакти прав людини, Римський статут Міжнародного кримінального суду); норм звичаєвого міжнародного права; нормативних рамок у специфічних сферах (кібербезпека: міжнародні спроби розробити інструменти правового регулювання, хоча спільного, усеохопного договору досі немає [95]), принцип «відповідальність за захист» (R2P – Responsibility to Protect), що стосується інтервенцій за гуманітарними підставами, коли держава не спроможна захистити населення від геноциду, злочинів проти людства тощо, кодекси й правила для приватних охоронних

структур, наприклад International Code of Conduct for Private Security Service Providers (ICoC).

Виокремлюємо виклики та варіанти трансформації міжнародної безпеки в сучасних умовах воєнних конфліктів і постійної інтенсифікації впливу гібридних загроз:

– зростання нелінійних / асиметричних загроз, таких як тероризм, кібер·атаки, інформаційна війна, кіберзброя;

– нерозривність між традиційною безпекою (воєнна, військова) й «новими» формами (екологія, пандемії, продовольча безпека, кліматичні зміни);

– проблема легітимності втручань під приводом гуманітарної акції – ризик «зловживань» під маскою безпеки;

– дисбаланс сил, коли великі держави мають більше ресурсів і вплив, що ставить у скрутне становище малі або слабші;

– проблеми координації між міжнародними й регіональними організаціями, конкуренція юрисдикцій;

– недостатня нормативна база в нових сферах (наприклад кібербезпека).

Отже, міжнародна безпека є системоутворювальним елементом сучасного світопорядку, оскільки саме вона забезпечує стабільність взаємодії держав, міжнародних організацій і недержавних акторів. Її головна мета – запобігання глобальним і регіональним конфліктам, підтримання миру, дотримання міжнародного права та гарантування прав людини. Однак ефективність міжнародної безпеки значною мірою залежить від того, наскільки стійкими й готовими до викликів є самі держави – основні учасники міжнародної системи.

Міжнародна безпека невіддільна від національної, адже без внутрішньої стабільності окремої держави неможливо забезпечити стабільність у глобальному масштабі. Міжнародні норми, договори й інституції створюють загальні рамки безпеки, але їх практична реалізація відбувається на рівні національних механізмів. Отже, національна безпека є фундаментом, на якому

ґрунтується міжнародна – вона визначає спроможність держави захищати свої інтереси, територіальну цілісність, громадян, політичний суверенітет і водночас робить внесок у колективні безпекові структури світу.

Національна безпека – це стан захищеності національних інтересів держави, суспільства та особи від внутрішніх і зовнішніх загроз, який гарантує сталий розвиток країни, суверенітет, територіальну цілісність і демократичний устрій. У Законі України «Про національну безпеку України» (2018 р.) прописано, що «національна безпека – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших життєво важливих національних інтересів України від реальних і потенційних загроз» [71].

Проаналізувавшм теоретичні підходи до дослідження національної безпеки, наголосимо на реалізмі, де безпека вбачається як основна функція держави у світі, де панує анархія (Т. Гоббс, Г. Морґентау, К. Уолтц), а ключовим інструментом її забезпечення є військова сила, своєю чергою, мета – виживання країни. Із погляду лібералізму, безпека можлива через співпрацю, міжнародні інститути, норми та взаємозалежність; інституції (ООН, ОБСЄ, ЄС) створюють механізми колективної безпеки; підхід орієнтований на демократичний мир і колективну відповідальність (Р. Кеохан, Дж. Най, М. Дойл). Конструктивізм убачає безпеку як соціальний конструкт, коли те, що суспільство вважає загрозою, стає нею внаслідок політичного дискурсу. Ключова концепція цього підходу полягає в сек'юритизації (Оле Вейвер, Баррі Б'юзен) – переведенні певної проблеми (міграції, дезінформації) в площину безпеки, а також пояснюється, чому різні держави по-різному визначають пріоритети безпеки. Неомарксизм розглядає безпеку крізь призму нерівності, економічної залежності, глобального капіталізму (К. Бут, Р. Кокс). Потрібне чітке переосмислення від «національної» до «глобальної» або «людської» безпеки. І нарешті – концепція людської безпеки, яка просувається ООН із 1994 р. Акцентовано передусім на захисті людини, а не лише держави, який уключає сім вимірів: економічний, продовольчий, екологічний, особистий,

політичний, громадський, здоров'я. Цей підхід інтегрує соціальні науки, розвиток і права людини. Еволюцію концепції національної безпеки відображено у табл. 2.2.

У сучасному світогляді та філософській думці застосовуються два основні підходи до розуміння поняття «національна безпека». Засновником першого – реалістичного – підходу до розуміння цієї концепції є американський політолог Г. Моргентау, який визначив національну безпеку як недоторканність території та інститутів держави, наголошуючи на воєнній, політичній безпеках, що є традиційним розумінням. Другий підхід – безпека людини, розвивався в рамках ідеалістичної теорії міжнародних відносин і характеризувався аналізом військових, політичних, економічних, соціальних, гуманітарних, екологічних проблем [451].

Щодо структури та основних компонентів національної безпеки потрібно розглянути рис. 2.1, де показано основні об'єкти й суб'єкти безпеки, загрози, механізми забезпечення та індикатори безпеки.

Таблиця 2.2

Еволюція концепції національної безпеки*

Етап	Характеристика	Домінуючий аспект
1	2	3
Класичний (до 1945 р.)	Безпека ототожнюється з військовою могутністю; головна загроза – війна між державами	Воєнно-політична
Післявоєнний (1945–1990 рр.)	Формування інститутів колективної безпеки (ООН, НАТО); поява поняття «баланс сил» і «стримування»	Геополітична, ядерна
Постбіполярний (1990–2000 рр.)	Кінець холодної війни; переосмислення: увага до політичної, економічної, інформаційної стабільності	Комплексна

Сучасний (початок XXI ст.)	Виникнення «нових» загроз – тероризм, кіберзагрози, пандемії, екологічні катастрофи, міграційні кризи	Людська, інформаційна, екологічна

***** Джерело: розробка здобувача.

Рис. 2.1. *Структура та основні компоненти національної безпеки**

* Джерело: розробка здобувача.

Дві ключові концептуальні моделі національної безпеки – трирівнева система безпеки Кеннета Волтца (індивідуальний рівень – поведінка політичних лідерів; державний рівень – внутрішня політика, економіка, ресурси; міжнародний рівень – анархічна структура міжнародної системи) та модель «всеосяжної безпеки», сформована в Японії в 1980-х рр. (безпека розглядається не лише у військових термінах, а як усеосяжна система, що включає економіку, енергетику, продовольство, екологію, кіберпростір).

Отже, національна безпека є динамічною багаторівневою системою, яка поєднує в собі державоцентричну логіку реалізму (захист суверенітету), інституційну логіку лібералізму (співпраця та норми), когнітивну логіку конструктивізму (дискурси загроз), гуманітарну логіку людської безпеки (захист особи). Таким чином, у сучасній науковій парадигмі поняття «національна безпека» виходить за межі воєнної оборони й постає як комплексна категорія, що відображає спроможність держави та суспільства адаптуватися до глобальних змін, підтримуючи стабільність, розвиток і цінності.

Сучасні процеси, що відбуваються в інформаційній сфері, суттєво впливають на прискорення руху до вищої фази розвитку людства – інформаційного суспільства, у якому інформація стає надзвичайно цінною складовою частиною національного надбання, важливим економічним, політичним і військовим ресурсом. Це своєю чергою, призвело до виникнення в умовах глобальної інформатизації та розвитку інтернету нових викликів та загроз, з’явилася можливість вирішувати міждержавні конфлікти не силовими методами, а застосовуючи сучасні інформаційні технології. Тому, як ніколи гостро, перед кожною країною сьогодні постало питання щодо забезпечення інформаційної безпеки, яке набуває стратегічного значення.

В умовах гібридних загроз, інтенсивного розвитку цифрових технологій, інформаційного тероризму та масових дезінформаційних кампаній ефективна система інформаційної безпеки стає запорукою політичної стабільності, громадянської згуртованості й державного суверенітету. Інформаційна безпека трактується як стан захищеності інформаційного простору держави, її інституцій, громадян і критичної інфраструктури від зовнішніх та внутрішніх загроз, що можуть призвести до дестабілізації, маніпулювання свідомістю, витоку стратегічної інформації чи порушення функціонування систем управління. Вона охоплює як технічну (кібербезпека, захист систем зв’язку, шифрування), так і соціально-політичну складову частину (протидія фейкам, захист від інформаційного впливу, розвиток критичного мислення).

Одним із найактуальніших викликів для держав у сучасному глобалізованому світі є інформаційна війна, що ведеться за допомогою дезінформації, пропаганди, фальсифікації фактів, кібероперацій і маніпулятивного контенту. Прикладом такого типу війни є агресія російської федерації проти України, де інформаційний фронт став одним із ключових елементів стратегії ворога: дискредитація української влади, спроби підірвати довіру до ЗСУ, розпалювання паніки, утручання у виборчі процеси, поширення фейків про «зовнішнє управління» чи «розкол суспільства».

На цьому тлі інформаційна безпека набуває не лише оборонного, а й проактивного значення – держави повинні не лише захищатися, а й розвивати національні системи стратегічних комунікацій, підтримувати незалежні медіа, формувати інформаційну культуру. Ключовими чинниками зміцнення інформаційної безпеки є:

- медіаграмотність населення, що дає змогу самостійно відрізняти правду від маніпуляцій;
- прозора державна комунікація, яка зміцнює довіру до інституцій;
- правове регулювання цифрового простору з урахуванням свободи слова та безпеки;
- координація з міжнародними партнерами, зокрема ЄС і НАТО, для обміну даними й реагування на гібридні загрози.

Отже, у сучасних умовах інформаційна безпека є не відокремленим напрямом, а структурною частиною національної безпеки, що охоплює політичну, економічну, військову та соціальну сфери. Нездатність держави забезпечити надійний захист свого інформаційного простору може призвести до серйозних криз – від утрати легітимності державних інститутів до втрати суверенітету. Саме тому ефективна державна політика у сфері інформаційної безпеки є основою для збереження незалежності, стабільності й розвитку демократичного суспільства.

Формування питання міжнародної інформаційної безпеки виокремилося в міжнародній практиці із середини 90-х рр. XX ст. Цьому сприяла низка

факторів, насамперед різноманітність негативних проявів використання інформаційно-комунікаційних технологій. Ці нові технології змогли негативно вплинути на реалізацію основних прав і свобод людини, а також на цілісність державних структур. Їх швидкий та масштабний розвиток, різноманітний вплив на суб'єктів відносин і зростаюча залежність Світового Співтовариства від належного функціонування інформаційно-комунікаційних мереж та систем посилили увагу до цих нових проблем як із практичного, так і з теоретичного погляду.

Крім того, сьогодні в кіберпросторі розгортаються численні протистояння між спецслужбами різних країн, їхніми військовими структурами, а також економічні та інформаційні битви, уключаючи економічне шпигунство й фінансові саботажі. Цей факт визначає велике значення процесів, що відбуваються в інформаційному просторі, для сучасного політичного аналізу, теорії та практики політології й визнання інформаційної безпеки як елементу системи національної безпеки. Отже, наразі існує потреба у вивченні поточних проблем забезпечення інформаційної безпеки, захисту національного інформаційного простору, з огляду на реальні та потенційні загрози, а також руйнівну пропаганду й маніпулятивні інформаційні впливи.

Це питання особливо актуальне в Україні, яка є об'єктом зовнішньої інформаційної експансії, маніпулятивних пропагандистських технологій та деструктивного вторгнення інформації. В умовах російсько-українського конфлікту існує необхідність захисту національного інформаційного простору від негативних інформаційних і психологічних впливів, а також гарантування інформаційної безпеки та інформаційного суверенітету як чинників функціонування України як суверенної й незалежної держави.

Відповідно до Закону України «Про основи національної безпеки України» (2018), серед загроз національній безпеці України в інформаційній сфері зазначено такі [429]:

– прояви обмеження свободи слова та доступу до публічної інформації;

– розповсюдження за допомогою медіа культу насильства, жорстокості, порнографії;

– комп'ютерна злочинність та комп'ютерний тероризм;

– розголошення інформації, що становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства та держави;

– спроби маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної чи упередженої інформації (Закон України) [72].

Інформаційна безпека, проблеми захисту національного інформаційного простору досліджувалися багатьма науковцями. Зокрема, відзначимо вивчення цього питання, котре відображено в працях А. І. Марущака [139; 138; 140], М. В. Маркової [135], В. А. Ліпкана [435], Б. А. Кормича [101; 103; 102] та інших експертів. Серед тем, які розглядали ці дослідники, значне місце посіли теоретичні питання з окремих аспектів міжнародно-правових відносин, питання співробітництва в рамках регіональних міжнародних організацій. Певною мірою вивчалася також роль ООН і Міжнародний союз електрозв'язку (МСЕ) у формуванні норм Інституту міжнародної інформаційної безпеки. Крім того, інноваційні зміни в сучасних формах та методах забезпечення інформаційної безпеки, окремі нюанси кібербезпеки розкриваються в дослідженнях В. Л. Бурячка [21; 22] (2011), Д. В. Дубова [338; 424; 337] (2011), Г. Почепцова [183], В. Петрика [175] (2009), М. Погорецького [179] (2009) й ін. Важливі аспекти інформаційної безпеки держави, як відомо, стосуються також специфіки бізнес-процесів. Вони розкриваються, зокрема, у працях О. Стащука (2021), Т. Шматковської (2020), М. Дзямулич [245] (2020), В. Якубіва [396] (2019).

Питаннями інформаційної та кібербезпеки займалися як вітчизняні, так і зарубіжні вчені: В. Л. Бурячок [23], Н. І. Бусленко, О. Ю. Колєсов, В. А. Ліпкан, А. М. Митко, Н. П. Карпчук, а також В. К. Конах, а особливо аналізуючи загрози й виклики національним інтересам України в

інформаційній сфері в умовах глобалізації [97] та ін. Зауважимо, що в монографії «Міжнародна інформаційна безпека: сучасні виклики та загрози» Є. А. Макаренко [129] висвітлив такі питання, як стан і тенденції розвитку міжнародної системи підтримання миру в інформаційну добу, планування й здійснення спеціальних інформаційних операцій, сутність і методи протидії маніпулятивним технологіям, прикладні аспекти інформаційної безпеки в різних сферах суспільного життя.

Теоретичною основою дослідження теми участі громадських організацій в інформаційній безпеці є праці таких вітчизняних науковців, як Я. Малика [131], Н. Зубар [75], С. Телешуна [218], О. Солдатенко [508], об'єктом дослідження яких є проблематика функціонування й захисту інформаційного простору України; роботи журналістів В. Малинки, В. Некрасова, М. Довженка, В. Кондратової; напрацювання представників громадських і волонтерських організацій – ГО «НотаЄнота» [165], ГО «Центр стратегічних комунікацій» [238], «StratCom Ukraine» [516], ГО «CAT-UA» [283], «InformNapalm» [399], «StopFake» [515], «Українські кібервійська» [231], а також телеграм-каналів BRAMA (https://t.me/brama_channel), SPRAVDI (https://t.me/spravdi), Центр протидії дезінформації (https://t.me/CenterCounteringDisinformation), Антологія брехні / VoxCheck (https://t.me/voxcheck), CyberpoliceUA (https://t.me/CyberpolUA), IT ARMY of Ukraine (https://t.me/itarmyofukraine2022), – які безпосередньо виявляють і спростовують неправдиву інформацію про Україну. Важливі результати напрацювань цілої групи дослідників на чолі з Д. Дуцик «Як функціонують та завойомують аудиторію неінституціоналізовані новинні телеграм-канали українського сегменту» [65], здійснених ГО «Український інститут медіа та комунікації» [228] в партнерстві та за фінансової підтримки німецьких колег.

Однак у працях вищезгаданих експертів інформаційна безпека вивчається переважно як невід'ємний елемент національної безпеки і її невід'ємна складова частина. Водночас учені недостатньо приділяли увагу практичним проблемам чіткого окреслення інформаційних загроз, вивчення їх

джерел, комплексного розгляду вивчення технологій інформаційно-психологічних воєн та операцій, виявлення й обґрунтування методів боротьби з інформацією та психологічних негативних впливів. Оскільки загрози інформаційній безпеці держави в сучасних умовах розвитку інформаційного суспільства є динамічними й постійно змінюються, відповідні питання наукових досліджень не втрачають своєї актуальності й донині.

Інформаційна безпека є інтегрованою складовою частиною національної безпеки та вважається пріоритетною функцією держави. Інформаційна безпека, з одного боку, надає громадянам якісну вичерпну інформацію й вільний доступ до різних джерел інформації, а з іншого – це контролювати поширення дезінформації, сприяти цілісності суспільства, зберігати інформаційний суверенітет, боротися з негативною інформацією, психологічними впливами та захищати національний інформаційний простір від маніпуляцій, інформаційних війн й операцій.

У добу інформаційного суспільства інформаційний простір будь-якої держави є організаційно впорядкованою сукупністю інформаційних ресурсів, інформаційних технологій, що реалізовують інформаційні процеси, тобто системою. Під поняттям інформаційного простору розуміють сукупність територій, охоплених медіа певної категорії (регіональними, національними, світовими) [148]. Найчастіше цей термін уживають у значенні національного інформаційного простору, який потребує законодавчого врегулювання й захисту, а його суб’єкти – державної підтримки. Інформаційний простір держави – це множина текстових, аудіо- чи відео повідомлень, які були оприлюднені чи плануються до оприлюднення на її території [171].

Інформаційний простір є ключовим для розвитку країни, оскільки дає змогу виконати багато завдань. У динамічному функціонуванні він є важелем у розв’язанні таких проблем:

– модернізації, неможливої без підтримки відповідних освітянських та інформаційних процесів;

– творенні нових еліт, оскільки саме тут він є майданчиком, де все це відбувається значно швидше, аніж у суто внутрішньому політичному полі;

– демократії й прозорості влади;

– інтелектуалізації (чи деінтелектуалізації) країни, залежно від поставлених перед нею завдань;

– творення власної ідентичності [184].

Розв'язання складної проблеми інформаційної безпеки дасть змогу захистити інтереси суспільства та держави, а також гарантувати права громадян отримувати комплексну, об'єктивну і якісну інформацію. Існує два аспекти тлумачення інформаційної безпеки в контексті національної безпеки. З одного боку, інформаційна безпека розглядається як незалежний елемент національної безпеки будь-якої країни, а з іншого – інтегрована складова частина будь-якої іншої безпеки – військової, економічної, політичної тощо.

Інформаційна безпека – це стан захисту життєво важливих інтересів особистості, суспільства та держави, який мінімізує шкоду через неповноту, своєчасність і неточність інформації, негативний вплив інформації, негативні наслідки інформаційних технологій, а також несанкціоноване розповсюдження інформації [77].

Це визначення є оптимальним і відображає всі сторони взаємодії суб'єктів інформаційних відносин. Зазначимо, що розвиток інформаційних технологій є не тільки важливою державною функцією, а й передумовою забезпечення ефективного використання інформаційних ресурсів, накопичених суспільством, для створення розвиненого та безпечного інформаційного середовища. Цією метою є організація системи інформаційної безпеки, складовими частинами якої є національні інтереси в інформаційній сфері, загрози цим інтересам, сама інформаційна безпека як інструмент створення сприятливих умов для їх реалізації, які сукупно становлять об'єкт управління державою, система забезпечення інформаційної безпеки, тобто суб'єкт управління, більше того – основні напрями політики національної безпеки в інформаційній сфері, а також внутрішнє та зовнішнє середовище.

На практиці існує кілька видів методів захисту інформації:

– однорівневі методи, які ґрунтуються на одному принципі управління інформаційною безпекою;

– багаторівневі методи, що основані на кількох принципах управління інформаційною безпекою, кожен із яких слугує для розв'язання власної проблеми. При цьому приватні технології не взаємопов'язані й спрямовані лише на конкретні фактори інформаційних загроз;

– інтегровані методи – багаторівневі технології, які об'єднані в єдину систему координаційних функцій на організаційному рівні для забезпечення інформаційної безпеки на основі аналізу набору факторів ризику, які мають смисловий зв'язок або формуються з єдиного інформаційного центру інформації;

– інтегровані високоінтелектуальні методи – багаторівневі, багатокомпонентні технології, які побудовані на основі потужних автоматизованих інтелектуальних інструментів з організаційним управлінням [122].

Дослідження інформаційної безпеки враховують той факт, що її сутність – це внутрішній зміст суб'єкта, який знаходить вираження в стійкій єдності всіх різноманітних і суперечливих форм існування. Основною характеристикою інформаційної безпеки потрібно вважати ймовірність підвищеного ризику чи загрози для окремої людини, суспільства та держави. Критерієм ефективності інформаційної безпеки є високий рівень безпеки за мінімуму відповідних витрат.

Основним елементом інформаційної безпеки є життєві інтереси суспільної системи, які співвідносяться із зовнішніми чинниками у вигляді інтересів наднаціональних чи інших національно-державних структур у межах міжнародної спільноти. У рамках національно-державного утворення його життєві інтереси перебувають у взаємодії з інтересами елементів, що становлять це утворення. Останні – це соціальні групи, еліта, організації, партії, релігійні та етнічні групи, рухи тощо. Поєднання внутрішніх і

зовнішніх інформаційних загроз створює передумови для порушення безпечного функціонування системи державного управління.

Політичні дискусії на Міжнародному семінарі з інформаційної безпеки, що відбувся в 1999 р. в Женеві під егідою Інституту досліджень роззброєння ООН (ЮНІДІР) за участі Департаменту з питань роззброєння Секретаріату організації та представників більше ніж півсотні країн світу, підтвердили актуальність проблеми й своєчасність її розгляду в рамках об'єднання. Визначаючи підходи до її розв'язання, визначили різні позиції, що відповідали стратегічним інтересам учасників дискусії. Позиція розвинених країн передбачала визнання проблеми міжнародної інформаційної безпеки, як гіпотетичне протистояння влади; перенесення концепції міжнародної інформаційної безпеки на регіональний або тематичний рівень; виокремлення таких складників, як кримінальні та терористичні міжнародні інформаційні загрози зі складної проблеми міжнародної інформаційної безпеки й створення міжнародного механізму контролю таких інформаційних злочинів.

Позиція країн, які не належать до західної моделі цивілізації, передбачала такі пропозиції: установлення міжнародно-правової норми про заборону використання засобів впливу на інформаційні ресурси та інформаційний потенціал міжнародного, регіонального й національного призначення; створення спеціального Міжнародного суду з інформаційної злочинності; спільний розвиток глобального захисту від інформаційної агресії.

У Заяві Міжнародної зустрічі проголошено затвердження Програми дій щодо запобігання інформаційним війнам та обмеження гонки інформаційних озброєнь. Женевська зустріч розкрила стратегічну проблему міжнародної інформаційної безпеки – проблему домінування в глобальній інформаційній сфері із застосуванням інформаційної зброї, тобто бажання контролювати великі території й суспільства, проблему інформаційного дисбалансу міжнародного права [18].

Однак зазначимо, що національні інтереси в інформаційній сфері випливають із таких національних цінностей, як права людини, свобода, економічний процвітання та могутність країни. Для України головним є її виживання як вільної, незалежної нації за збереження фундаментальних цінностей та інститутів безпеки. Одним із механізмів гарантування цього процесу є ефективно функціонуюча система державного управління, яка є суб'єктом й об'єктом інформаційної безпеки одночасно. І в цьому випадку зусилля багатьох країн щодо її забезпечення за рахунок інших держав викликають занепокоєння, з одного боку, а з іншого – упевненість у необхідності формування життєздатної системи інформаційної безпеки уряду. Вона є як характеристика стабільного стану системи державного управління, котра під впливом внутрішніх і зовнішніх загроз та небезпек зберігає істотні характеристики для власного існування.

У цьому аспекті ефективним механізмом забезпечення цілісності особистості, суспільства й держави як єдиного організму є державне управління національною інформаційною безпекою. Незважаючи на пріоритет і цінність інтересів конкретної особи, будь-яка розвинена країна будує власну систему через першість державного управління. Це не означає фактичного виключення конкретних громадян та громадських організацій із процесу забезпечення національної безпеки держави. Отже, життєві інтереси відображають основоположні, основні потреби держави, порушення або нездатність задовольнити які можуть призвести до її краху. Через це природно, що кожна держава має свої національні інтереси. Цей важливий момент треба враховувати під час створення систем колективної, міжнародної, глобальної інформаційної безпеки.

На початку XXI ст. держави зіткнулися з якісно новим викликом – утратою контролю над власним інформаційним простором. Те, що ще два десятиліття тому розглядалося як перевага глобалізації – відкритість комунікацій, миттєвий доступ до інформації, свобода інтернету, – нині стало потенційною вразливістю. У добу, коли геополітичні суперечності дедалі

частіше реалізовуються в цифровій площині, поняття інформаційного тероризму та цифрового суверенітету стають взаємопов'язаними ключовими категоріями політичної безпеки. Вони відображають дві сторони сучасного конфлікту: з одного боку – деструктивну силу маніпуляцій, з іншого – прагнення держави відновити контроль й автономію в мережевому світі.

Інформаційний тероризм – це системне, цілеспрямоване застосування інформаційних технологій для залякування, дестабілізації або підриву державного суверенітету, без прямого використання фізичної сили. На відміну від класичних терористичних актів, його мета – вплинути не на тіла, а на свідомість, змінити уявлення людей про реальність, делегітимізувати владу й посіяти хаос. Інформаційні атаки можуть набувати різних форм: масові кампанії дезінформації, маніпуляції в соціальних мережах, використання deepfake-технологій, кібератаки на інформаційні ресурси, підрив довіри до виборів, суду, армії чи медіа. Якщо в класичному тероризмі вирішальним чинником була фізична шкода, то в інформаційному – ефект страху й дестабілізації, досягнутий через інформаційний тиск. Отже, інформаційний тероризм стає когнітивною зброєю, яка атакує не об'єкти, а структури довіри, що підтримують політичну систему.

Глобалізація й технологічна інтеграція призвели до безпрецедентної взаємозалежності інформаційних систем. Соціальні мережі, цифрові платформи та хмарні сервіси утворили наднаціональний інформаційний простір, у якому кордони держав розмиваються. Політичний контроль над даними, потоками інформації й алгоритмами дедалі частіше зосереджений не в руках урядів, а в приватних руках транснаціональних корпорацій. Цей стан можна охарактеризувати як кризу цифрового суверенітету – спроможності держави забезпечувати контроль над власним інформаційним простором, технологічною інфраструктурою й даними громадян. Інформаційний тероризм виникає саме в цій зоні втрати контролю, де немає єдиного регулятора, немає прозорих правил і де цифрові платформи можуть використовуватися як зброя. Відомі кейси – утручання у вибори, кампанії

Cambridge Analytica, російські дезінформаційні операції в США та ЄС, атаки на енергетичні системи України – демонструють, що інформаційна зброя діє транснаціонально, а суверенітет держав стає умовним. У таких умовах інформаційний тероризм не просто порушує безпеку – він підважує саму онтологію державності, засновану на монополії контролю над інформаційними потоками.

Цифровий суверенітет – це не лише технічна категорія, а насамперед політична. У сучасній теорії міжнародних відносин він означає право держави визначати правила функціонування цифрового середовища на власній території, захищати дані громадян й інформаційні ресурси від зовнішнього втручання. Його сутність полягає у відновленні контролю над трьома взаємопов'язаними сферами: дані (data sovereignty) – національна юрисдикція над інформацією, створеною громадянами та державними інституціями; технології (technological sovereignty) – спроможність розвивати власні IT-рішення, не залежачи від іноземних платформ і хмарних сервісів; інформаційна політика (narrative sovereignty) – спроможність держави формувати й захищати власний стратегічний наратив у глобальному інформаційному середовищі. Отже, цифровий суверенітет є антиподом інформаційного тероризму: якщо тероризм руйнує єдність і контроль, то суверенітет прагне відновити порядок, визначеність та довіру.

Із політологічного погляду, інформаційний тероризм є не лише загрозою, а й симптомом структурної слабкості держави в цифровому середовищі. Він стає можливим тоді, коли інституційні механізми контролю – правові, технологічні, когнітивні – не відповідають рівню глобальної взаємозалежності. Три механізми демонструють цей зв'язок – відсутність правової юрисдикції. Інформаційні атаки часто здійснюються з-за кордону, що унеможливлює кримінальне переслідування; технологічна залежність. Використання іноземних хмарних сервісів і соціальних мереж позбавляє державу можливості контролювати інформаційні потоки; маніпуляційна вразливість. Суспільства з низьким рівнем медіаграмотності та критичного

мислення стають ідеальним середовищем для інформаційних атак. Отже, інформаційний тероризм – це прояв дефіциту цифрового суверенітету, а боротьба з ним потребує не лише кіберзахисту, а й формування власної нормативної архітектури інформаційного простору.

Тобто інформаційний тероризм і цифровий суверенітет – це взаємопов'язані концепти нової політичної реальності. Перший демонструє, наскільки вразливими стали демократичні системи в глобалізованому інформаційному середовищі; другий – прагнення держав відновити контроль і безпеку без утрати відкритості. У політологічному вимірі йдеться про переосмислення природи суверенітету: від територіального – до інформаційного та когнітивного. Для сучасної України формування цифрового суверенітету є не лише питанням технологічної незалежності, а й інструментом протидії інформаційному тероризму, відновлення довіри, легітимності й стійкості держави. Отже, у XXI ст. справжній суверенітет – це не контроль над кордонами, а контроль над смислами, які формують політичну реальність.

Отже, інформаційна безпека стала невід'ємною частиною як національної, так і міжнародної безпеки, особливо в умовах глобалізації та зростання інформаційних загроз. Для України, яка зазнає постійного інформаційного тиску, критично важливою є розбудова ефективної системи захисту інформаційного простору. Це потребує поєднання національних заходів з міжнародною співпрацею, оновлення правових інструментів і впровадження стратегій цифрової стійкості. Питання інформаційної безпеки є надзвичайно важливими для Української держави на сучасному етапі, що зумовлено насамперед необхідністю протистояти незаконним посяганням на інформаційний простір України. Ураховуючи, що європейська інтеграція є стратегічно визнаним пріоритетом зовнішньої політики України, завданням української влади має стати розвиток ефективного діалогу з ЄС щодо інформаційної безпеки. Крім того, потрібно детально вивчити практичний досвід зарубіжних країн, які вже мають організаційно-правову базу

інформаційної безпеки та максимально використовують свій досвід у національному законодавстві й впровадженні ефективних заходів у цій сфері.

2.3. Інформаційний тероризм як компонент гібридної війни

В історії людства інформаційне протистояння було присутнім у кожній війні в тій чи іншій формі. Але після Другої світової війни цей напрям набув особливого значення й досяг більш системного рівня, що зафіксовано в різних офіційних документах. У різних джерелах застосовуються різні терміни та визначення – інформаційне протистояння, інформаційна операція, психологічна операція, – а також відповідні скорочення, такі як IO, PSYOPS. Уточнимо, те, що раніше широко використовувалося в західних країнах, не завжди може бути повністю скопійовано для сучасних реалій України. Можна також сказати, що в розвинених державах світу (США і європейських країнах НАТО) спостерігаємо переосмислення інформаційної складової частини протистояння та існує тенденція до застосування більш обережного висловлювання. Відповідно, у світі з'явились й активно впроваджуються порівняно нові формулювання – «стратегії м'якої сили», «стратегічні комунікації», MISO тощо.

У XXI ст. інформаційний тероризм перетворився на одну з найнебезпечніших форм міжнародного тероризму, що дедалі активніше використовується як зброя в глобальних конфліктах. Його суть полягає в навмисному поширенні дезінформації, маніпулятивного контенту, панічних настроїв або виведенні з ладу інформаційної інфраструктури задля досягнення політичного, ідеологічного чи економічного ефекту. Від традиційних вибухів і нападів терористи перейшли до атак на свідомість – масову, миттєву й практично невидиму, що робить цю форму терору особливо небезпечною в умовах цифрової доби.

Інформаційний тероризм уключає як цілеспрямоване викривлення фактів, створення фейкових новин і конспірологічних наративів, так і кібератаки на медіа, урядові ресурси або критичну інфраструктуру. Його цілі

– не лише дезорієнтація громадськості, а й руйнування довіри до державних інституцій, провокування хаосу, підрив моральної стійкості суспільства. Особливо ефективним цей інструмент стає під час воєн, політичних криз або виборчих кампаній, коли інформаційний простір є ослабленим або надмірно поляризованим.

У цьому контексті інформаційний тероризм є не лише побічним ефектом гібридної війни – це самостійна форма терористичної діяльності, що доповнює й підсилює фізичне насильство. Нерідко за такими кампаніями стоять не тільки терористичні угруповання, а й держави, які використовують інформаційний терор як засіб зовнішньополітичного тиску або елемент асиметричних дій. Такі приклади, як кампанії дезінформації під час пандемії COVID-19, війни в Україні чи виборів у США та ЄС, демонструють його спроможність впливати на глобальні процеси.

Отже, інформаційний тероризм є невід'ємною частиною сучасного міжнародного тероризму, що потребує нових підходів до захисту інформаційного простору й зміцнення колективної стійкості суспільств. Традиційні інструменти безпеки виявляються недостатніми – натомість потрібні ефективні механізми цифрової гігієни, критичного мислення, фактчекінгу та міжнародного співробітництва. Лише усвідомлення масштабу цієї загрози дасть змогу сформувати адекватну відповідь на нову реальність терористичного тиску у сфері інформації.

Розвиток інформаційно-комунікаційних технологій дуже швидко призвів до інформаційного тероризму, використання інформаційних технологій, медіа, поширення інформації з метою цілеспрямованого впливу на обраний об'єкт, його дискредитація [17, с. 128]. Розуміння цього поняття є передумовою формування більш точних уявлень про сутність сучасного міжнародного тероризму, запобігання загрозам, які можуть зруйнувати державні інститути, основи стабільності держави й основи національної безпеки загалом. Сучасний інформаційний тероризм характеризується як сукупність інформаційних війн, спеціальних операцій із залученням

національних чи транснаціональних кримінальних структур і спеціальних служб іноземних держав.

Сутність феномену інформаційного тероризму активно досліджується в працях як зарубіжних, так і вітчизняних учених. Серед дослідників, які займаються вивченням тероризму в контексті глобалізації, розвитку інформаційно-комунікаційних технологій та зростанням ролі медіа в суспільстві, є M. Jerrold [415], C. Archetti [274], Д. Белл, Ж. Бодрійяр, Е. Гідденс, М. Кастеллс, Е. Тоффлер, Ф. Фукуяма, С. Гантінгтон, Б. Гоффман, А. Шмідт, Z. Hacsek [372], S. Atran [275], D. Cingranelli, S. Mark, M. Gibney, P. Haschke, R. Wood, D. Arnon [301] й ін. Зазначимо, що є низка робіт вітчизняних науковців, які зробили свій внесок у вивчення цієї теми. Це О. Зернецька, О. Гриценко, О. Грицун [50], В. Іванов, Є. Макаренко, М. Ожеван, Г. Почепцов, А. Чічановський, О. О. Резнікова, А. О. Місюра, С. В. Дрьомов, К. Є. Войтовський [191], К. С. Герасименко [43], О. С. Геращенко [44], М. П. Гетьманчук [45], Я. Й. Малик [131], В. М. Петрик [175], Т. П. Яцик [255], А. В. Ілляшенко, Ю. М. Кіяшко [76], О. Бойченко [16], Р. О. Банк [10], Т. Білецька [14; 120]. Соціальні мережі як засіб здійснення терористичних актів досліджували Л. І. Рудник [199], Н. Ф. Семен [205], В. Коцур [106]. Інформаційний тероризм як інструмент гібридної війни вивчали Д. Харамурза [234], О. Шевчук [243], О. Жайворонок [67].

Про важливість досліджуваної тематики свідчить кількість дисертаційних робіт у різних галузях знань. Наприклад, О. В. Саган «Протидія медіаінформаційному тероризму як питання національної безпеки України» (Національний інститут стратегічних досліджень, 21.01.01 – основи національної безпеки держави (політичні науки)) [201], О. І. Зінченко «Протидія кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону» (Харківський національний університет імені В. Н. Каразіна, 052 Політологія [80]), С. С. Здоровко «Державна політика протидії міжнародному тероризму в період світової глобалізації» (Національний університет цивільного захисту України, 281 Публічне

управління та адміністрування), С. О. Пшеничний «Тероризм як тактичний компонент сучасних війн: безпековий аспект» (Харківський національний педагогічний університет імені Г. С. Сковороди 052 Політологія), А. Д. Білюга «Залучення військових контингентів країн-членів НАТО для боротьби з міжнародним тероризмом (2001–2021 рр.» (Національний університет оборони України, 253 Військове управління), Р. В. Антонюк «Державна політика протидії тероризму в контексті сучасних викликів національній безпеці України» (Київський національний університет імені Тараса Шевченка, 281 Публічне управління та адміністрування), В. А. Ліпкан «Геостратегія України в умовах трансформації міжнародного порядку: теорія і практика» (23.00.04 «Політичні проблеми міжнародних систем та глобального розвитку»), ін.

Монографія В. Г. Воронкової й В. О. Нікітенко «Філософія цифрової людини і цифрового суспільства: теорія і практика» [41] стосується теоретико-методологічних, концептуальних і праксеологічних засад формування цифрової людини й цифрового суспільства як взаємозв'язаних феноменів, що набувають дедалі більшого значення в епоху інформаційних і технологічних трансформацій. Автори ставлять завдання дослідити те, як цифрова трансформація змінює антропологічний, соціальний, культурний, етичний аспекти буття, а також визначити можливості й ризики взаємодії людини та цифрових систем у різних сферах (освіта, комунікація, влада, інформаційний простір).

Інформаційний тероризм і його місце в структурі сучасних гібридних загроз розробляються українськими дослідниками у сфері політичної комунікації й інформаційної безпеки. Так, Н. В. Лабенко визначає інформаційний тероризм як специфічну форму психологічного насильства, що здійснюється з метою маніпулювання свідомістю громадян, підриву легітимності державних інституцій і розбалансування політичної системи. У її дослідженнях акцентовано на важливості розмежування інформаційної війни,

пропаганди та цілеспрямованих терористичних інформаційних операціях, що мають системний і стратегічний характер [116].

Л. Лабенко розглядає інформаційний тероризм як специфічну форму деструктивного впливу на індивіда, суспільство та державу, що здійснюється за допомогою різних видів інформації й окреслює низку ключових ознак цього явища [115]:

– є різновидом організованого насильства та формою психологічного терору;

– поширення здійснюється переважно через медіа;

– основним механізмом є психоемоційний тиск на великі соціальні групи;

– у тактичному вимірі спрямований на створення резонансу довкола певної проблематики;

– стратегічна мета полягає в залякуванні й деморалізації населення задля досягнення політичного чи соціального ефекту;

– застосовується ефект раптовості;

– дії мають відкритий, демонстративний характер, що й визначає публічність як ключову його рису інформаційного тероризму.

Значущими є також праці О. Рєзнікової, яка розглядає національну стійкість як ключовий елемент запобігання терористичним загрозам у гібридному середовищі. У науковій розвідці «Національна стійкість в умовах мінливого безпекового середовища» авторка наголошує на необхідності інтеграції політичних, економічних, соціальних і технологічних компонентів для створення ефективної моделі реагування на новітні загрози, уключаючи тероризм [193].

Інституційний вимір досліджень забезпечується такими аналітичними центрами, як Національний інститут стратегічних досліджень (НІСД) [155] та Центр досліджень армії, конверсії й роззброєння (ЦДАКР) [237], які регулярно публікують аналітичні матеріали щодо терористичних загроз, уключаючи з інформаційні та кіберзагрози в умовах російської гібридної агресії.

За широким визначенням, інформаційним тероризмом називають дії окремих осіб або їхніх груп щодо дезорганізації роботи автоматизованих систем і мереж зв'язку, що створюють небезпеку життю людей, спричинюють значні матеріальні збитки або інші суспільно небезпечні наслідки, а також загрозу реалізації вказаних дій, якщо вони відбуваються з метою порушення суспільної безпеки, залякування населення або здійснення впливу на прийняття рішень органами влади. З іншого боку, це використання інформаційних технологій, медіа, поширення інформації задля цілеспрямованого впливу на обраний об'єкт, його дискредитацію.

Деякі дослідники у сфері права, зокрема В. П. Ємельянов [66], розглядають інформаційний тероризм як злочин, що включає погрози, залякування окремих осіб або цілих соціальних груп і має характерні риси терористичної діяльності. Науковці підкреслюють, що використання інформаційного впливу з метою психологічного тиску та інспірації страху є формою тероризування, яка заслуговує на відповідну кримінально-правову оцінку.

Т. Яцик виокремлює інформаційний тероризм як сукупність сучасних інформаційних війн і спеціальних операцій, пов'язаних із діяльністю національних та транснаціональних кримінальних угруповань, а також спецслужб іноземних держав [255]. М. Джеррольд, своєю чергою, трактує поняття як злиття фізичного насильства з кримінальним використанням інформаційних систем, а також навмисне зловживання цифровими інформаційними системами, мережами або їх компонентами задля полегшення вчинення терористичних операцій або дій [415, с. 98]. На думку В. Коршунова, інформаційний тероризм – нова форма терористичної діяльності, яка спрямована на тимчасове або незворотне порушення функціонування інформаційної інфраструктури держави чи окремих її елементів [104]. Крім того, він уключає до цього поняття незаконне використання інформаційних ресурсів із метою створення умов, що

призводять до серйозних негативних наслідків для особистості, суспільства та держави.

На думку українського дослідника К. Герасименка, інформаційний тероризм – це механізм дестабілізації суспільства, формування атмосфери громадянської непокори й підриву довіри до влади шляхом організації спеціальних медіакампаній [43]. Він вважає, що основні загрози походять від іноземних держав, міжнародних терористичних угруповань та інших злочинних організацій, які використовують недостатню розвиненість і слабкість державних структур. У зв'язку з цим поширена думка, що сучасний інформаційний тероризм являє собою сукупність інформаційних війн та спеціальних операцій, пов'язаних із діяльністю національних і транснаціональних кримінальних угруповань, а також спецслужб інших держав.

Проаналізувавши низку трактувань та наукових підходів, робимо висновок, що поняття «інформаційний тероризм» є доктринальним у теорії інформаційної безпеки й охоплює особливі аспекти:

1) суспільно небезпечне діяння, яке є однією з форм міжнародного тероризму;

2) засіб деструктивного інформаційно-психологічного впливу на особистість, суспільство та державу;

3) небезпечні інформаційні дії, спрямовані на соціальні групи, державні органи влади й управління, що включають розповсюдження загроз, викривлення об'єктивної інформації, що провокує кризові ситуації, страх і соціальну напругу;

4) насильницький пропагандистський вплив, який позбавляє населення можливості критично осмислювати отриману інформацію;

5) нова форма терористичної діяльності, що полягає у навмисному виведенні з ладу інформаційної інфраструктури держави або її окремих елементів, а також у незаконному використанні інформаційних ресурсів для створення загрозливих умов для суспільства, особистості та держави;

6) сукупність інформаційних війн і спеціальних інформаційних операцій, які виконуються національними або транснаціональними кримінальними структурами та іноземними спецслужбами;

7) поєднання фізичного насильства зі злочинним використанням інформаційних технологій, а також умисне зловживання цифровими мережами і їх компонентами для підтримки терористичних актів;

8) ідеологічно мотивована діяльність, спрямована на залякування населення, маніпуляцію прийняттям рішень або примушування органів влади, міжнародних організацій, соціальних груп чи окремих осіб до певних дій (або бездіяльності) через використання інформаційних ресурсів та технологій.

Хронологія розвитку практики інформаційного тероризму, яка показує еволюцію від класичних форм терористичного насильства до сучасних інформаційно-психологічних операцій у цифрову добу (додаток В), із наголосом на переосмисленні подій 11 вересня 2001 р. як початку нової ери виокремлює такі основні етапи:

1. Доінформаційний етап (1960–1990-ті рр.) Традиційні форми тероризму (фізичне насильство, заручники, вибухи) спрямовувалися на досягнення медійного ефекту. Медіа виступали «посередником страху» – саме завдяки телебаченню та газетам терористичні групи здобували світову увагу. Зароджується концепція «тероризму як театру» (Б. Дженкінс, 1975 р.) [414]: ІРА, «Червоні бригади», «Бадер-Майнгоф» – використовують медіа як засіб пропаганди; захоплення літаків і заручників транслюються в прямому ефірі (1970–1980-ті рр.). Формується усвідомлення інформаційного виміру тероризму – терорист не лише вбиває, а й показує, створюючи ефект страху через медіа;

2. Етап перших інтернет-практик (1990–2001 рр.). Початок використання інтернету терористичними угрупованнями для комунікації, пропаганди, фінансування. Формуються перші сайти з маніфестами, навчальними матеріалами, зверненнями до прибічників. Кіберпростір стає паралельною ареною боротьби – терористи починають експериментувати з цифровими

каналами: «Хезболла» та «ХАМАС» створюють офіційні вебсторінки, Аль-Каїда організовує внутрішню мережу комунікацій через зашифровані листи;

3. Інформаційно-психологічний етап (11 вересня 2001 р.). Переосмислення подій, оскільки теракти 9/11 стали не лише трагедією, а й інформаційною революцією в тероризмі. Події трактуються у двох вимірах: як каталізатор наукового осмислення феномену тероризму (породжує масштабне осмислення як глобальне комунікаційне явище; з'являються нові напрями досліджень інформаційної війни, психологічної війни, медіатероризму; формуються міждисциплінарні підходи – політологічний, комунікаційний, безпековий, культурологічний; держави й міжнародні організації (ООН, НАТО, ЄС) починають розробляти нормативну базу протидії інформаційному тероризму) та як точка радикальної трансформації ролі медіа (медіа стали не лише спостерігачами, а й співучасниками поширення шоку; телевізійні трансляції перетворили трагедію на психологічний спектакль глобального масштабу; глядач став частиною «аудиторії страху»: медіа допомогли терористам досягти їхньої головної мети – масового психологічного впливу, виникнення нової форми симбіозу терористичного насильства й медіапропаганди, що забезпечувало довготривалий ефект страху (табл. 2.3).

Таблиця 2.3

Трансформація медіа після 9/11*

Аспект	До 9/11	Після 9/11
1	2	2
Роль медіа	Інформування про події	Створення «ефекту присутності»
Тип впливу	Раціональне сприйняття	Емоційно-шоковий вплив
Головна мета терориста	Символічна акція	Психологічна мобілізація
Позиція глядача	Спостерігач	Співучасник емоційної драми

* Джерело: розробка здобувача.

Події вересня 2001 р. спроєктовані як медіаподія: удари по вежах WTC – це одночасно акт фізичного насильства й глобальний медіасимвол страху, удар по США транслювався наживо – створено «ефект тотальної присутності», відтоді головною метою тероризму є інформаційно-психологічний вплив, а не просто знищення. Б. Гоффман [379] та аналітики RAND (2004 р.) [488] називають 9/11 «народженням мережевого тероризму» – коли інформаційна стратегія стає центральною у плануванні;

4. Етап цифрового розквіту тероризму (2001–2014 рр.). Терористичні групи масово освоюють інтернет як платформу впливу, з'являються нові сайти, форуми, онлайн-журнали, перші відеозвернення, формується поняття «кіберджихаду»: Аль-Каїда публікує навчальні посібники (Inspire, Jihad Recollections); зростає кількість пропагандистських відео на YouTube; інтенсифікується вербування через email та форуми, поширюються перші кібернапади на урядові сайти. Отже, формується «інформаційна інфраструктура тероризму» – від планування до психологічної мобілізації;

5. Соціально-мережевий етап (2014–2019 рр.). Терористичні організації використовують соцмережі для масового впливу, повна гібридизація, коли фізичний тероризм підсилюється інформаційним: ІДІЛ створює повноцінну медіаімперію, розповсюджуючи високоякісні відео, журнали, кампанії у Twitter та Telegram; Dabiq, Rumiyah, Amaq Agency стають ключовими інформаційними платформами ІДІЛ; масове онлайн-вербування, формування віртуальних спільнот «халіфату»; терористичні акти в Парижі, Брюсселі, Лондоні – супроводжуються цифровими кампаніями. Характерною рисою цього періоду можна виокремити той факт, що тероризм стає «мережевим брендом», коли інформація важливіша за територію;

6. Сучасний етап штучного інтелекту (ШІ) і дипфейків (2020–2024 рр.). Використання генеративного ШІ для створення фейкових відео, фото, аудіо, масове застосування інформаційно-психологічних операцій у гібридних війнах (особливо після 2022 р.), терористичні та державні актори розмивають межу між пропагандою й кібератаками: діпфейк-відео «капітуляції

Зеленського» (березень 2022 р.); спроби створення фальшивих повідомлень від лідерів НАТО; ШІ-боти у Telegram, що поширюють радикальний контент.

Отже, інформаційний тероризм входить у нову сучасну фазу автоматизації коли створення, поширення й психологічний вплив цілковито делегуються алгоритмам.

Відштовхуючись від загальної мети тероризму вплинути на рішення урядів, міжнародних організацій або громадської думки, посіяти страх і дестабілізувати суспільство, досягти політичних поступок або зміни режиму, нав'язати свою ідеологію чи систему цінностей, виокремлюємо й основні цілі інформаційного тероризму, такі як психологічна дестабілізація населення (викликати паніку, зневіру, апатію або агресію); підрив довіри до влади, армії, інституцій (створення враження безсилля держави); маніпулювання громадською думкою (вплив на вибори, суспільні настрої, ставлення до війни, партнерів, ворогів); поширення паніки під час криз (фейки про катастрофи, війну, пандемії); руйнування національної ідентичності та єдності (через наративи, дезінформацію, інформаційні атаки).

Зауважимо, що інформаційний тероризм не завжди має винятково політичну мету, а переважно політично орієнтовану, тому що вона домінує у випадках державних або ідеологічних атак (наприклад російські інформаційні кампанії проти України). З іншого боку, економічна мета полягає в маніпуляції ринками, дестабілізації банків, атакуванні бізнесів для вигоди; соціально-психологічна мета підсилює деструкцію довіри, розпалювання міжетнічної або міжрелігійної ворожнечі; гібридна мета поєднує політичні й соціально-психологічні цілі для досягнення стратегічного впливу.

Отже, будь-який інформаційний тероризм спрямований на контроль над свідомістю, поведінкою або рішеннями людей, а політична складова частина є його найчастішою, але не єдиною формою мети.

На початку 2010-х р. інформаційний тероризм поділяється на:

1) інформаційно-психологічний тероризм (контроль медіа з метою поширення дезінформації, чуток, демонстрації сили терористичних організацій задля маніпуляції думками та населенням):

2) медіатероризм (зловживання інформаційними системами, мережами і їх компонентами для терористичних дій);

3) інформаційно-технічний тероризм (пошкодження окремих елементів та всього інформаційного середовища противника в цілому: руйнування елементної бази, активне придушення ліній зв'язку, штучне перезавантаження вузлів зв'язку тощо);

4) кібертероризм (сукупність дій, які включають інформаційну атаку на комп'ютерні системи, обчислювальні системи, обладнання для передачі даних й інші складові частини інформаційної інфраструктури, учинені злочинними групами чи окремими особами) [16, с. 231].

До ключових елементів сучасного інформаційного тероризму належать:

– цілеспрямоване поширення дезінформації та фейків – маніпулятивні кампанії, спрямовані на викривлення реальності, формування недовіри до державних інституцій, розпалювання ворожнечі або паніки;
– кібератаки на інформаційну інфраструктуру – утручання в роботу вебсайтів, медіа, електронних ресурсів держави, банківських систем або стратегічно важливих об'єктів, щоб паралізувати чи дестабілізувати функціонування систем управління;
– нформаційне залякування – масове поширення загрозливих повідомлень, відео чи зображень для створення психологічного тиску або паніки серед населення;
– маніпуляція масовою свідомістю – використання соціальних мереж, ботів, алгоритмів та емоційних наративів для спрямованого впливу на думки, поведінку або політичні уподобання аудиторії;

– підрив національної ідентичності й історичної пам’яті – систематичні атаки на культурні символи, мову, історію або релігію з метою розколу суспільства та послаблення національної єдності;
– використання deepfake-технологій – створення фальшивих відео або аудіозаписів, що можуть дискредитувати лідерів, інституції або посилити конфлікти;
– зовнішнє втручання у внутрішній інформаційний простір – діяльність іноземних держав або транснаціональних акторів, які намагаються вплинути на вибори, протестні рухи або загальний політичний клімат через інформаційні інструменти.

Отже, інформаційний тероризм – це не просто частина інформаційної війни, а цілеспрямована форма насильства в інформаційному просторі, що може мати такі самі руйнівні наслідки, як і фізичний тероризм, але з менш очевидними механізмами виявлення та протидії. Ключові інструменти інформаційного тероризму – це ботоферми, фейкові акаунти в соцмережах; генератори фейкових новин і гібридних медіа; deepfake-відео та аудіо; злам платформ або витік конфіденційної інформації; розсилка загроз чи провокацій через месенджери; створення сайтів-клонів урядових ресурсів.

Одним із найнебезпечніших видів є «інформаційно-психологічний тероризм», а саме маніпуляція людьми та їхніми думками. Масова маніпуляція – прихований словесний, зображувальний вплив на суспільство, метою якого є поширення масових настроїв, формування громадської думки, її корегування. Ефективність такого впливу визначається ступенем несвідомого наслідування або відображенням саморегуляції представників різних верств населення на основі оманливих уявлень про причини та наслідки того, що відбувається. Велике значення для ефективного масового маніпулювання мають масові інфекції, які передують маніпуляції або відбуваються паралельно з нею. У сучасному світі існує багато способів маніпулювання інформацією.

Маніпуляція як вид інформаційного тероризму – це складне соціально-психологічне явище, у якому механізми свідомого викривлення інформації, емоційного впливу й психологічного тиску використовуються задля страху, дестабілізації чи примусу суспільства або окремих груп, тобто тих цілей, які властиві терористичним практикам, але реалізуються через інформаційні засоби, а не фізичне насильство.

У гуманітарних науках поняття набуло негативного відтінку й означає прихований психологічний чи інформаційний вплив, який змінює думки, почуття або поведінку людини всупереч її усвідомленим інтересам. Кембриджський словник подає визначення маніпуляції «як дії, спрямованої на вплив або контроль над іншою людиною, зазвичай прихованим або тонким чином, що сприяє досягненню особистих цілей» [438]. Психологічна маніпуляція – «це вид соціального впливу, метою якого є зміна поведінки або сприйняття інших людей за допомогою образливих, обманливих або підступних тактик» [264]. Отже, вона відбувається, коли хтось використовує оманливі, примусові або експлуататорські стратегії для контролю над думками, почуттями чи діями іншої людини. На відміну від здорового переконання, маніпуляція надає пріоритет порядку денному маніпулятора, ігноруючи благополуччя іншої сторони. Звідси – «маніпулятор прагне вплинути на переконання та бажання іншої людини, подаючи їй сумнівні або хибні підстави під виглядом переконливих і логічних аргументів, добре усвідомлюючи їх неправдивість» [510].

Основними ознаками маніпуляції є прихований характер впливу, коли людина не усвідомлює, що нею керують; емоційна спрямованість, де акцент на страх, провину, гордість, співчуття; ілюзія вибору під час створення відчуття самостійності прийняття рішень; підміна понять і цінностей у ході спотворення реальності для вигоди маніпулятора; розрахунок на стереотипи, звички, соціальні ролі.

Щодо форм та видів маніпуляції виокремлюємо такі:

– психологічна – вплив на емоції та самооцінку (компліменти, шантаж, почуття провини);

– медіаційна (інформаційна) – спотворення або відбір фактів у медіа, створення фейків, пропаганда;

– політична – використання популізму, демагогії, страху, меседжів «ми проти них»;

– економічна та комерційна – реклама, що впливає на споживача через підсвідомі мотиви;

– соціальна – конструювання образів ворога або героя, маніпуляція колективними цінностями.

Виокремлюємо ключові акценти маніпуляції, серед яких – намір (не випадковість, а цілеспрямований акт), непрозорість або маскування (маніпулятор завжди прагне приховати справжні мотиви чи методи), ціль впливу (зміна когнітивної, емоційної, поведінкової сфери цільової особи чи аудиторії), нерівність інтересів (маніпулятор використовує інструменти на свою користь, часто за рахунок цільової сторони або її автономії). З іншого боку, ознаки маніпуляції як терористичного інструменту відображено в табл. 2.4.

Інформаційна маніпуляція – це цілеспрямоване, систематичне та приховане спотворення фактів або контексту інформації з метою формування вигідного для маніпулятора сприйняття дійсності, що обмежує здатність людини до самостійного критичного вибору.

Таблиця 2.4

Ознаки маніпуляції як терористичного інструменту*

Ознака	В інформаційній маніпуляції	У межах інформаційного тероризму
1	2	3
Ціль	Зміна сприйняття, думки, поведінки	Створення паніки, дестабілізація, контроль через страх

Методи	Фейки, фреймінг, напівправда, приховані меседжі	Масові інформаційні атаки, залякування, шокові повідомлення
Емоційна домінанта	Емоційний тиск (вина, сором, страх)	Страх, безвихідь, загроза існуванню
Аудиторія	цільова група, населення	Масова аудиторія, національна або міжнародна
Рівень впливу	Індивідуальний або груповий	Суспільно-психологічний, державний

* Джерело: розробка здобувача.

Отже, маніпуляція в межах інформаційного тероризму – це засіб психологічного впливу, який ставить терористичну мету – породити страх, ненависть, безпорадність, змусити суспільство діяти певним чином.

Термін «пропаганда» спочатку мав нейтральне значення, пов’язане з поширенням віри або знань (у XVII ст. Католицька церква створила Congregatio de Propaganda Fide – «Конгрегацію поширення віри»). Згодом, особливо у XX ст., це поняття набуло переважно негативного забарвлення, асоціюючись із маніпуляцією, нав’язуванням ідеологій та політичним контролем.

Пропаганда – це свідоме й систематичне комунікаційне зусилля (організації, держави чи іншого актора), що через відбір і фреймування фактів, упереджені/оманливі повідомлення та емоційні техніки формує сприйняття, впливає на переконання й спрямовує поведінку цільових аудиторій на користь заданих політичних та/або ідеологічних цілей; у праві окремі її суспільно небезпечні форми (на кшталт пропаганди війни, тероризму чи тоталітарних режимів) прямо заборонені.

Джоветт й О’Доннелл визначають пропаганду як «свідомий, систематичний намір формувати сприйняття, маніпулювати когніціями та спрямовувати поведінку задля відповіді, що просуває інтереси пропагандиста» [418]. В енциклопедії Британіка подається її визначення як систематичного поширення фактів, аргументів, чуток, «напівправди» чи відвертої брехні для

впливу на громадську думку; відмінна риса – умисність і маніпулятивний акцент [281].

У XXI ст. пропаганда трансформувалась у цифрову форму. Соціальні мережі, алгоритмічні рекомендації, боти й «інформаційні війни» зробили її точнішою, персоналізованою та непомітною. Тепер вона діє через фабрики тролів і дезінформаційні кампанії; фейкові новини, «псевдоаналітику»; підміну наративів; створення «інформаційної бульбашки», що підсилює однобічність сприйняття.

Види пропаганди:

– за спрямуванням – політична, військова, релігійна, комерційна, соціальна;

– за формою впливу – відкрита – легітимна агітація та прихована – маніпулятивна, через медіа чи розважальний контент;

– за способом подачі – чорна – свідомо фальшива, сіра – частково правдива, але викривлена, біла – офіційна, відкрита, із відомим джерелом.

Сучасна пропаганда застосовує емоційне спрощення й повторюваність. Типові прийоми її використання в інформаційному тероризмі складаються з апеляції до страху або патріотизму, застосування символів і стереотипів, створення полюсів «друзів» і «ворогів», селекції фактів (вибіркове подання інформації), повторення меседжів (ефект «мантри»), створення псевдодоказів через маніпуляцію статистикою або експертними думками.

Під час холодної війни в контексті збройного протистояння термін «психологічні операції» (PSYOP) на Заході вживався частіше, тоді як по цей бік «залізної завіси», у Радянському Союзі та інших країнах Варшавського договору, домінував термін «ідеологічна діяльність і пропагандистська робота». У рамках класичного PSYOP також було декілька компонентів і дуже часто пропаганда розглядалася як складова частина технології психологічних операцій.

Психологічні операції (PSYOP, від англ. *Psychological Operations*) є невід’ємним елементом сучасної стратегії ведення гібридної війни та

багаторівневого інформаційного протистояння. Вони становлять сукупність заходів, спрямованих на вплив на свідомість, поведінку й мотивацію цільової аудиторії задля досягнення стратегічних, політичних або військових цілей без прямого застосування фізичного насильства. Головне завдання PSYOP полягає у формуванні або зміні переконань, установок і моделей поведінки, що відповідають інтересам суб'єкта впливу. На відміну від традиційної пропаганди, психологічні операції мають чітко визначені аудиторії, ретельно плануються з урахуванням культурних, соціальних, психологічних характеристик цільової групи й здійснюються із залученням технологій стратегічних комунікацій, соціальних мереж, мас-медіа, аудіовізуальних матеріалів і кіберпростору.

Сучасні PSYOP умовно поділяють на три основні типи, залежно від джерела інформації та ступеня її достовірності: білі психологічні операції здійснюються відкрито, від імені визнаного суб'єкта (держави, міжнародної організації тощо), і ґрунтуються на перевірених фактах. Основна мета – зміцнення довіри та легітимності дій; сірі психологічні операції реалізуються за відсутності чіткого джерела або з поданням частково правдивої інформації. Такі дії дають змогу впливати на свідомість через напівправду, сумніви або домисли. Чорні психологічні операції здійснюються анонімно або з використанням фейкових джерел, поширюють цілеспрямовану дезінформацію з метою дискредитації опонента, провокування хаосу або паніки. Інструментарій PSYOP є вкрай широким і включає дезінформаційні кампанії, маніпулятивне використання медіаконтенту (відео, зображення, тексти), створення фальшивих акаунтів і бот-мереж у соціальних мережах, поширення анонімних листівок або звернень, deepfake-технології, а також кібератаки з психологічним ефектом.

Історичні приклади застосування охоплюють широкий спектр конфліктів. Так, під час війни в Іраку (2003 р.) США проводили масовану кампанію із закликами до капітуляції серед іракських військових через листівки, радіопередачі й телеролики. У контексті сучасної війни росії проти

України (із 2014 р.) простежуємо системне використання поширення фейкових повідомлень про втрати ЗСУ, внутрішні конфлікти в українській владі, мобілізаційні паніки, створення образу «зради» тощо.

Ці кампанії мають на меті підірвати морально-психологічну стійкість українського суспільства, роз'єднати громадську думку й послабити довіру до інституцій держави. Особливо небезпечним є поєднання психологічних операцій із кібертерористичними методами, коли, наприклад, одночасно з хакерськими атаками на офіційні сайти здійснюється масоване вкидання дезінформації, яка створює атмосферу паніки або підриває віру в державну спроможність забезпечити безпеку. Отже, вони є ключовим інструментом у реалізації інформаційної агресії, що дозволяє дає змогу політичних і воєнних цілей без відкритого збройного конфлікту.

Термін «дезінформація» (від французького *désinformation*) означає навмисне поширення неправдивої або викривленої інформації з метою введення в оману. На відміну від простої помилки або неточності, дезінформація завжди має цілеспрямований, маніпулятивний і стратегічний характер. Її завдання – вплинути на свідомість, переконання чи поведінку людей в інтересах того, хто її поширює. У Кодексі практики щодо дезінформації 2022 р. це «достовірно неправдива або оманлива інформація, яка… створюється, представляється та поширюється задля економічної вигоди або навмисного введення громадськості в оману й може завдати суспільної шкоди» [522]. Руіз Карлос позначає дезінформацію як «оманливий контент, навмисно поширений із метою обману людей або отримання економічної чи політичної вигоди, що може завдати суспільної шкоди» [497].

Щоб зрозуміти дезінформацію глибше, звернемо увагу на відмінності між нею й іншими видами інформаційного спотворення такими як «містифікація», «малінформація», «фейкова новина» (табл. 2.5.)

Таблиця 2.5

Відмінності між «дезінформацією», «містифікацією», «малінформацією» та «фейковою новиною»*

Поняття	Суть	Застосування
Дезінформація	Намірно створена або поширена хибна інформація з метою обману, уведення в оману, маніпуляції	Хтось свідомо вигадує дані чи перекручує факти, щоб вплинути на аудиторію
Містифікація	Хибна або неточна інформація, поширена без наміру введення в оману, тобто без зловмисного наміру	Людина перепощує неправдивий факт, вважаючи його правдивим
Малінформація	Інформація, що ґрунтується на правдивих фактах, але використовується некоректно – виділена з контексту, перебільшена чи спотворена з метою шкоди	Справжнє фото зі скандального конфлікту використане в іншому контексті з метою очорнити особу або групу
Фейкова новина	Інформація, що виглядає як новина (формально), але є вигаданою або дуже сильно спотвореною – часто підпадає під містифікацію чи дезінформацію залежно від наміру	Сайт видає «новину», яка схожа на журналістську, але містить вигадані факти

*Складено здобувачем за [447; 448; 351].

Окрім класичних визначень, у науковій літературі з’являються більш глибокі концепції дезінформації, де показано, що це не просто «брехня», а складний інструмент інформаційної війни й маніпуляції, який функціонує в мережі пов’язаних дій. У статті «Disambiguating Disinformation: Extending Beyond the Veracity of Online Content» пропонується розглядати дезінформацію як послідовність або сітку інформаційних дій, орієнтованих на певну ціль або аудиторію, тобто фокус не лише на правдивості вмісту, а й на структурі, стратегії, контексті [332]. Оглядова праця «Frameworks, Modeling and Simulations of Misinformation and Disinformation» розкриває, що в більшості досліджень намір є ключовим для розмежування містифікації й дезінформації і що існує велика однорідність у розумінні цих термінів серед

науковців [362]. З іншого боку, стаття Леслі Д. Макінтоша, Вільяма Вайта, Синтії Хадсон Вітале «Unveiling Deception: Establishing a Taxonomic Framework for Disinformation within Scientific Discourse» розвиває таксономію різних типів дезінформації (за акторами, методами, платформами), що дає змогу класифікувати більш складні випадки [440].

Отже, дезінформація – це навмисна, цілеспрямована хибна інформація з метою обману чи маніпуляції (на відміну від містифікації, де намір може бути відсутнім). Проте сучасні дослідники наголошують, що потрібно дивитися не лише на правдивість та намір, а також й на контекст, мережеву структуру, акторів, методи поширення. У практиці боротьби з дезінформацією враховуються ідентифікація кампаній, аналіз метаданих, моделі мережевого поширення, правові підходи, етичні рамки.

На нашу думку, термін дезінформації частково перегукується з поняттям вепонізація. Виходячи з проведеного аналізу та узагальнення матеріалів, доцільно уточнити зміст і сформулювати визначення вепонізації інформації на основі результатів дослідження Чупіс А. Д., яка виокремлює її як використання будь-яких форм інформації (знань, фактів, масивів даних), а також каналів їх зберігання, обробки й передачі (цифрових або технічних) для цілеспрямованого маніпулятивного впливу, спотворення чи нецільового застосування відомостей, або обмеження доступу до них [240]. На її думку феномен вепонізації інформації має важливе значення, оскільки охоплює сам процес застосування методів пропаганди, дезінформації, інформаційно-психологічних операцій та інших когнітивних і психологічних маніпуляцій, спрямованих на досягнення визначених політичних чи військових цілей.

Отже, взаємодія вепонізації інформації з іншими сферами створює умови для трансформації їхнього змісту в негативно забарвлені медійні повідомлення, спрямовані на реалізацію прагматичних політичних чи військових інтересів, що, своєю чергою, є складовою частиною проявів інформаційної агресії – системного використання інформаційного простору як інструменту впливу, дестабілізації та підриву безпеки держави чи суспільства.

Інформаційна агресія – незаконні дії однієї зі сторін в інформаційній сфері, спрямовані на нанесення конкретної, відчутної шкоди в окремих сферах діяльності іншої сторони шляхом обмеженого й локального за своїми масштабами застосування сил [122]. У роботі Радутного О. Е. «Поняття та ознаки інформаційної агресії на законодавчому рівні» розглянуто інформаційну агресію як сукупність проявів у комунікації, які завдають шкоди, порушують права, використовують неправомірний тиск в інформаційній сфері [190]. У статті Максим Х. «Феномен інформаційної агресії в умовах повномасштабної війни росії проти України» розглянуто інформаційну агресію як форму інформаційної війни, маніпулювання інформацією, яка провокує порушення цілісності суспільства, деструкцію соціальних зв'язків, психологічний тиск [130]. У дослідженні «Інформаційна агресія російської федерації проти України» описано як «систематичну та цілеспрямовану дезінформацію, маніпуляцію й поширення пропаганди з метою впливу на українське суспільство, зміни його думок, сприяння розділу та дестабілізації країни» [214].

Ключовими характеристиками інформаційної агресії є намір / цільовість (не випадковий вплив, а цілеспрямований), шкода / агресивна дія (мета полягає в нанесенні якоїсь форми шкоди), засоби інформаційні / комунікаційні (зображення, відео, преса, інтернет, соцмережі, медіа, пропаганда, маніпуляції), системність / координованість (може бути частиною інформаційної кампанії), об'єкт агресії (суспільство, групи, інститути, окремі особи, держави).

У контексті російсько-української війни часто говорять про інформаційну агресію рф проти України, а саме видачу фейкових новин, спотворених фактів, вигаданих історій, спрямованих на дискредитацію українського уряду чи військових; маніпуляцію в соцмережах шляхом поширення «ботівських» акаунтів, які множать російські наративи, роздмухують внутрішні конфлікти, посівають недовіру до інституцій; використання новинних ресурсів як рупорів пропаганди, коли підконтрольні

медіа транслюють «офіційні версії» подій, виключаючи альтернативні думки. Ця інформаційна агресія має мету змінити сприйняття, послабити мораль підтримки населення, дискредитувати державні інститути, посіяти сумніви в безпеці.

Отже, інформаційна агресія є складовою частиною інформаційної війни або політики гібридного протистояння. А вже дезінформація та маніпуляція – це засоби, які можуть широко використовуватись у її рамках. Навіть пропаганда, яка переходить в атакувальні інструменти, виступає невід'ємною домінантою інформаційної агресії.

Наголосимо також і на інформаційному тероризмі в медіа («медіатероризм», «медіакілерство»), а саме зловживанні інформаційними системами, мережами та їх компонентами для вчинення терористичних актів й інших пов'язаних із ними дій. Цей вид тероризму характеризується як сукупність інформаційних війн та спеціальних операцій із залученням національних чи транснаціональних кримінальних структур і спеціальних служб іноземних держав. Медіатероризм (або «медіакілерство») належить до специфічного різновиду інформаційно-психологічного терору та є складовою частиною «інфраструктурного терору». Його сутність полягає в спробах шляхом організації спеціальних медіакампаній дестабілізувати суспільство, створити в ньому атмосферу громадянської непокори, недовіри суспільства до дій і намірів влади й особливо – її силових структур, покликаних захищати суспільний порядок. У випадку медіаінформаційного тероризму йдеться про різновид інформаційного тероризму, що є зловживанням інформаційними системами, мережами та їх компонентами для вживання терористичних дій і акцій. Засобами здійснення медіатероризму є друковані медіа, мережеві, ефірні й кабельні медіа, інтернет, електронна пошта, різноманітні електронні іграшки тощо.

Цифрова революція докорінно трансформує суспільство. Протягом двох останніх десятиліть мільярди людей скористались експоненціальним ростом доступу до мережі «Інтернет», швидким освоєнням інформаційних ресурсів та

комунікаційних технологій, а також економічними й соціальними можливостями, що виникли в цифровій сфері. Зворттною стороною цього процесу став такий вид інформаційного територзму як кібертероризм; використання комп'ютерних і телекомунікаційних технологій (особливо інтернету) для терористичних цілей.

Законодавство України визначає кібертероризм як «терористичну діяльність, що здійснюється в кіберпросторі або з її використанням». Це вбивча атака, спрямована на залякування для досягнення політичних результатів або пошкодження комп'ютерних мереж, особливо персональних комп'ютерів, підключених до інтернету, із використанням таких засобів, як комп'ютерні віруси. До кібертероризму відносять також деструктивні дії щодо інформаційних систем, які створюють умови для проведення актів тероризму [317].

Кібертероризм спрямований на проникнення в інформаційно-телекомунікаційну систему, перехоплення контролю, гальмування засобів мережевого обміну інформацією й здійснення інших руйнівних дій. Небезпека цього виду інформаційного тероризму полягає в тому, що він не має національних кордонів, і проблема виявлення терориста в інформаційному просторі є життєво важливою, оскільки хакери здійснюють терористичну діяльність через свої пристрої, що ускладнює його ідентифікацію та місцезнаходження [16]. Сьогодні кібертероризм – один із найнебезпечніших видів злочинів. Кібератаки можуть завдати значної шкоди на місцевому, державному і навіть міжнародному рівнях. Адже зовнішні кібератаки можуть переслідувати більш серйозні цілі, ніж пасивний збір даних, а об'єктами кібертероризму можуть бути грошова та секретна інформація, управління обладнанням космічних пристроїв, атомних електростанцій, військових комплексів, основних комп'ютерних вузлів тощо.

У зв'язку з цим особливого значення набуває розвиток систем стратегічних комунікацій, медіаосвіти, цифрової безпеки та інформаційної

гігієни, що мають стати основою державної політики протидії психологічному впливу та інформаційно-психологічним операціям у XXI ст.

Стратегічні комунікації – це навмисна, узгоджена та довгострокова система планування, реалізації й оцінювання комунікаційних заходів (внутрішніх і зовнішніх), спрямована на досягнення визначених цілей організації (або державного актора). Передбачають чітке визначення аудиторій, ключових повідомлень, вибір оптимальних каналів, координацію всіх комунікаційних елементів і корекцію на основі зворотного зв'язку.

Виокремлення ключових характеристик стратегічних комунікацій стартує саме зі стратегічності, тобто працює не фрагментарне, а системне мислення, далі розглядаємо координацію, де всі комунікації суб'єкта мають бути погоджені, наступна орієнтація на результат буде ефективна, коли відбувається зміна сприйняття, поведінки, іміджу, потім – іде адаптивність, цілковита здатність реагувати на зміни в середовищі, коригувати її і, нарешті, вимірюваність, коли відбувається оцінка ефектів і зворотний зв'язок.

Таблиця 2.6

Аналіз ключових компонентів стратегічних комунікацій*

Компонент	Значення	Приклад
1	2	3
Намір / ціль	Комунікація має бути цілеспрямованою задля досягнення певного ефекту (зміна сприйняття, поведінки, іміджу і т.д.)	Організація ставить за мету покращити свою репутацію серед ключових стейкхолдерів
Аудиторія / сегментація	Ідентифікація груп, на які спрямовано повідомлення; розуміння їхніх потреб, ментальних моделей, каналів сприйняття	Для внутрішньої комунікації – співробітники різних підрозділів із різними інформаційними стилями
Повідомлення / наратив / меседж	Формулювання змісту, що враховує цінності, культурні коди, рамки мислення аудиторій	Державна стратегія «Україна – країна свободи й боротьби за демократію»

Канали / носії	Вибір оптимальних засобів передачі (медіа, соцмережі, офіційні виступи, публічні заходи й ін.)	Використання YouTube, пресрелізів, сторінок у соцмережах, інтерв'ю
Координація / узгодженість	Усі комунікації (внутрішні й зовнішні) мають бути узгоджені між собою та із загальною стратегією	Не допускати суперечливих заяв із різних підрозділів
Планування / тактика / етапи	стратегія розбивається на етапи, окремі проєкти, активності, строки	Попереднє дослідження, створення меседжів, тестування, масштабування, моніторинг
Оцінка / зворотний зв'язок / корекція	Вимірювання ефектів (кількісні, якісні), унесення коректив	Проведення опитувань, аналіз охоплення, дослідження зміни ставлення
Контекст / зовнішні чинники	Успіх комунікації залежить не тільки від внутрішньообраної стратегії, але й від політичного, соціального, інформаційного середовища	в умовах інформаційної війни державний комунікаційний підхід має враховувати ворожу дезінформацію
Ціннісна основа / наративна рамка	Комунікація часто ґрунтується на певних цінностях, ідеях, що транслюються через ключові меседжі	«Демократія», «свобода», «національна гідність»

* Джерело: розробка здобувача.

У табл. 2.6 є структурною моделлю стратегічних комунікацій, у якій представлено дев'ять ключових компонентів ефективної комунікаційної системи – від задуму (цілі) до контексту та ціннісної рамки. Вона демонструє логіку побудови цілісної, керованої й вимірюваної комунікації. У роботі систематизовано елементи стратегічної комунікації у форматі «компонент – зміст – приклад», що дає змогу бачити структуру процесу комунікаційного менеджменту, виявити послідовність і взаємозалежність кроків (від цілі до оцінки результатів), інтегрувати теоретичні засади з практичними

прикладами, адаптувати цю модель для державних, корпоративних чи громадських комунікацій. Таким чином, таблиця відображає системний підхід до комунікації як управлінського процесу, а не як спорадичного обміну повідомленнями.

Рис. 2.2. ***Механізми реалізації стратегічних комунікацій****

* Джерело: розробка здобувача.

На рис. 2.1 відображено п’ять механізмів реалізації стратегічних комунікацій, а саме: превентивну комунікацію (пояснення ризиків до того, як з’являться фейки), антикризові інформаційні центри (моніторинг, перевірка, швидке реагування), наративи інформаційної стійкості («ми сильні», «правда на нашому боці»), мережу довірених джерел (створення інституцій, яким вірять – StratCom Ukraine, CAT-UA, Detector Media), партнерство з медіа та технологічними платформами (обмеження розповсюдження шкідливого контенту).

Таблиця 2.7

Функціональна модель протидії інформаційному тероризму*

Рівень	Завдання стратегічних комунікацій
1	2
Оперативний	Швидке реагування на фейки, кризові меседжі, виправлення інформаційних атак
Тактичний	Координація між держорганами, медіа, громадськими структурами; єдність меседжів
Стратегічний	Формування довгострокових наративів стійкості (resilience), національної ідентичності, позитивного образу держави

* Джерело: розробка здобувача.

У табл. 2.7 продемонстровано три рівні функціонування стратегічних комунікацій, які утворюють цілісну ієрархічну систему реагування та планування в інформаційному просторі: перший – оперативний – «реагує», другий – тактичний – «узгоджує», третій – стратегічний – «творить ідентичність». Отже, це модель багаторівневої інформаційної оборони, де стратегічна комунікація є не лише інструментом, а й щитом і дороговказом у боротьбі з інформаційною агресією.

В. Ліпкан визначає структуру системи стратегічних комунікацій як сукупність взаємопов'язаних компонентів, серед яких:

– інтеракціоністський компонент – охоплює публічну дипломатію, участь ключових лідерів, взаємодію з медіа, державними органами, громадськістю, а також внутрішні комунікації;

– інформаційно-психологічний компонент – уключає проведення інформаційних, психологічних і спеціальних операцій, спрямованих на вплив на цільові аудиторії;

– технічний компонент – забезпечує кібернетичну безпеку та протидію в електромагнітному просторі;

– військовий компонент – охоплює військове й цивільно-військове співробітництво, фіксацію та документування подій, забезпечення безпеки операцій і здійснення заходів активного впливу [125].

Отже, стратегічні комунікації – це не просто передавання інформації, а цілеспрямований, узгоджений і керований процес, який поєднує планування, реалізацію, координацію й оцінювання комунікаційних дій задля досягнення визначених цілей держави чи організації. Їх ефективність ґрунтується на системному підході, що включає стратегічність мислення, координацію всіх учасників, орієнтацію на результат, адаптивність до змін інформаційного середовища та вимірюваність ефектів.

Модель стратегічних комунікацій демонструє послідовність етапів – від формування наміру й визначення аудиторій до вибору каналів, координації дій, оцінки впливу та корекції повідомлень. Вона є інструментом не лише управління іміджем і репутацією, а й протидії інформаційним загрозам.

Отже, стратегічні комунікації є інтегрованим механізмом інформаційної оборони та впливу, що поєднує дипломатичні, інформаційно-психологічні, технічні й військові інструменти в єдину систему забезпечення державної безпеки й стійкості суспільства.

У XXI ст. інформаційний тероризм став системним інструментом гібридної війни: від «тероризму як театру» доби мас-медіа він еволюціонував до мережево-алгоритмічної моделі, де дезінформація, маніпуляція та PSYOP поєднуються з кібератаками, ботмережами й технологіями deepfake. Його ціль – не стільки фізичне знищення, скільки деморалізація, дестабілізація та контроль над сприйняттям, що підриває довіру до інституцій і розмиває національну єдність. У цій логіці інформаційний тероризм функціонує як ядро інформаційної агресії й органічно взаємодіє з іншими доменами гібридного впливу – політичним, економічним, військовим.

Концепт вепонізації інформації окреслює ширший процес перетворення знань, даних і каналів комунікації на зброю, що живить інформаційний тероризм методами пропаганди, дезінформації та психологічного тиску.

Соціальні мережі й рекомендаційні алгоритми роблять ці атаки точнішими, персоналізованішими й менш помітними, а участь державних і парадержавних акторів посилює стратегічний масштаб загрози – від виборчих циклів та криз до повномасштабної війни.

Український і міжнародний науковий дискурс збігається в ключовому: інформаційний тероризм – суспільно небезпечна, ідеологічно мотивована діяльність, що може включати як інформаційно-психологічні операції, так і навмисні технічні ураження інформаційної інфраструктури. Він проявляється в кампаніях дезінформації, інфраструктурних інцидентах, масовому інформаційному залякуванні та підриві історичної пам'яті, тобто в практиках, де зміст і носії інформації використовуються для досягнення політичних і воєнних цілей.

Звідси випливають наслідки для державної політики й безпекової архітектури: стратегічні комунікації як каркас багаторівневої відповіді (оперативний – швидке спростування та антикризові центри; тактичний – координація акторів і єдність наративів; стратегічний – формування ідентичності та resilience); інституційна стійкість: розбудова спроможностей кіберзахисту, моніторингу інформаційних операцій і правового реагування на інформаційну агресію; суспільна стійкість: медіаосвіта, розвиток критичного мислення й фактчекінгу, мережі довіри та партнерства з платформами; технологічна відповідь: виявлення ботмереж і синтетичного контенту, прозорість алгоритмів, використання ШІ для детекції й атрибуції атак.

У сучасних умовах гібридних конфліктів і масових інформаційних атак поняття інформаційна стійкість набуває ключового значення для системи міжнародної та національної безпеки. Вона постає не лише як елемент протидії дезінформаційним впливам, але і як складова частина гуманітарної, когнітивної й політичної стабільності суспільства. З огляду на це, розроблення категоріально-понятійного апарату та системи вимірювання інформаційної стійкості є необхідним кроком для формування аналітичних інструментів політики безпеки.

Під інформаційною стійкістю треба розуміти комплексну здатність особи, суспільства й держави підтримувати функціональну рівновагу та достовірність інформаційного середовища в умовах деструктивних впливів. Вона передбачає не лише технічну або кібернетичну захищеність, а й когнітивну, етичну, соціальну та інституційну спроможність протистояти інформаційному тероризму, маніпуляціям, панічним наративам і підривним операціям. Інформаційна стійкість є результатом інтеграції трьох взаємопов'язаних вимірів – когнітивного (свідомість та критичне мислення), інституційного (ефективність медіа, освіти, державних комунікацій) і системного (нормативно-правова та політична здатність держави реагувати на гібридні загрози).

У цьому контексті інформаційна стійкість є антиподом інформаційного тероризму, який ґрунтується на руйнуванні довіри, викривленні реальності та формуванні емоційно-кризового стану суспільства. Якщо інформаційний тероризм прагне дестабілізації, то інформаційна стійкість – це механізм відновлення балансу, психологічної цілісності та соціальної солідарності. Відтак поняття стійкості може розглядатися як інтегральний критерій рівня інформаційної безпеки держави.

Отже, інформаційний тероризм є однією з найнебезпечніших форм сучасного міжнародного тероризму, що діє через дезінформацію, маніпуляцію свідомістю, пропаганду й ін. Його загроза полягає в підриві довіри до держави, дестабілізації суспільства та руйнуванні інформаційної безпеки. Ефективна протидія потребує міжнародної співпраці, правового врегулювання та зміцнення інформаційної стійкості. У сфері політичних, філософських, правових, естетичних, релігійних й інших поглядів та ідей, тобто в духовній сфері, інформаційний тероризм здійснюється там, де відбувається боротьба ідей. Деякі експерти пов'язують це з високотехнологічним застосуванням традиційного тероризму, а інші стверджують, що інформаційний тероризм спрямований не на суспільство, а на окремих людей у повсякденному житті, що не має нічого спільного з політикою та міжнародними відносинами. Однак

усі експерти об’єднані в одне: інформаційний тероризм – це насамперед негативний вплив на людину, суспільство й стан усіх наявних видів. Інформаційний тероризм – невід’ємна, інтегрована складова частина гібридної війни, а не її побічний продукт. Його ефективність зумовлена симбіозом пропаганди, маніпуляції, дезінформації й кіберінструментів у рамках інформаційної агресії. Адекватна протидія можлива лише як цілісна політика інформаційної безпеки та національної стійкості, що поєднує правові, інституційні, технологічні та комунікаційні рішення з довгостроковою роботою над суспільною довірою і єдністю.

ВИСНОВКИ ДО РОЗДІЛУ 2

Події 11 вересня 2001 р. стали рубіжним моментом у розвитку міжнародного тероризму, започаткувавши якісно нову фазу його еволюції, що охоплює інформаційно-комунікаційний, ідеологічний та геополітичний виміри. Терористична атака на Сполучені Штати не лише поставила під сумнів ефективність традиційної архітектури глобальної безпеки, а й засвідчила вразливість навіть найбільш технологічно розвинених держав перед новими асиметричними загрозами. У відповідь США реалізували стратегію жорсткої воєнної та інформаційної протидії, що легітимізувала застосування сили в межах глобальної «антитерористичної» парадигми, водночас започаткувавши процес політизації поняття тероризму і його використання в стратегічних інтересах. Глобальний резонанс подій «чорного вівторка» активізував переосмислення концептуальних підходів до тероризму, виявивши потребу в міждисциплінарному аналізі феномену, у якому тероризм є не лише загрозою, але й індикатором глибших цивілізаційних зрушень і дисбалансів. Отже, 11 вересня стало символом переходу від класичних форм насильства до гібридних, інформаційно-технологічно обумовлених форм терористичної активності, що докорінно трансформували безпекове мислення початку XXI ст.

Інформаційна безпека постає як стратегічно важлива складова частина національної й міжнародної безпеки, що охоплює широкий спектр політичних, правових, технологічних і соціальних аспектів. У сучасному глобалізованому та цифровізованому середовищі вона є ключовим чинником захисту державного суверенітету, стабільності демократичних інституцій і забезпечення сталого розвитку. Для України, яка зазнає масштабних гібридних атак, зокрема в інформаційній сфері, питання інформаційної безпеки набуло екзистенційного виміру, вимагаючи комплексного підходу – від кіберзахисту до формування критичного мислення громадян. В умовах триваючої агресії з боку російської федерації держава повинна не лише реагувати на інформаційні загрози, а й проактивно вибудовувати ефективну систему стратегічних комунікацій, взаємодіяти з міжнародними партнерами й упроваджувати адаптивну нормативно-правову базу. Забезпечення інформаційної безпеки є не просто оборонною функцією, а фундаментом національної стійкості, демократичного розвитку та інтеграції України в європейський безпековий простір.

РОЗДІЛ 3
ІНФОРМАЦІЙНА ВІЙНА ЯК ФОРМА ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОТИСТОЯННЯ

3.1. Інформаційний тероризм у системі інформаційних війн: взаємозв'язки та інституціональні характеристики

У контексті трансформації міжнародного безпекового середовища війна вже давно перестала бути лише збройним протистоянням регулярних армій на полі бою. Сучасні конфлікти набувають дедалі складніших форм, у яких стирається межа між військовими й невійськовими засобами впливу, між державними та недержавними суб'єктами агресії, а також між фізичними й інформаційно-психологічними методами ведення війни. Такі трансформації спричинили появу нових підходів до класифікації конфліктів, зокрема концепції «війни четвертого покоління» (Fourth generation warfare – 4GW), яка сформульована американським військовим теоретиком Вільямом Ліндом у 1989 р., пропонує аналітичну модель нових форм агресії, що ґрунтується на децентралізації насильства, ерозії державної монополії на війну й посиленні ролі недержавних суб'єктів конфлікту [434]; передбачає також децентралізацію насильства, партизанські тактики, підривну діяльність, психологічний та інформаційний тиск.

Війна четвертого покоління – конфлікт, який характеризується стиранням відмінностей між безпосередньою війною й політикою, між залученими в неї військовими та цивільним населенням [183]. На Заході прийнято таку класифікацію поколінь війн: перше покоління характеризується лінійною тактикою часів застосування холодної зброї й мушкетів; друге – упровадженням тактики «вогню та маневру» часів Першої світової війни й безпосередньо перед нею; третьому поколінню властива тактика широких маневрів, оточень супротивника та прорив його ліній оборони на велику глибину з використанням великих танкових з'єднань й авіації. Ідея «війни

четвертого покоління» зародилася в часи Холодної війни, коли наддержавам у ході боротьби за свою присутність у різних точках світу стало зрозуміло, що широкомасштабне застосування танків, авіації та ракет у цих умовах малоефективне, проте роль партизанських і різних політичних, економічних, фінансових, інформаційних та психологічних підривних операцій кардинально зросла. Концепцію 4GW уперше висунуто в 1989 р. американським військовим експертом У. Ліндом, який вважав, що для четвертого покоління війни властиві децентралізація й зникнення державної монополії на війну. Саме це дає змогу повернутися до війни культур, а імміграція та мультикультуралізм створюють передумови для війни ідентичностей [433].

Такий тип війни вважається ефективним щодо «витрат–здобутків»: не вкладати величезні кошти в широкомасштабну війну, а застосовувати різні новітні підривні тактичні прийоми, щоб змусити країну-жертву агресії постійно виснажувати свої військові, фінансові ресурси в ході безперервної й постійно підживлюваної ззовні партизанської війни та терористичної діяльності. Паралельно з цим цілеспрямовано ініціюють наростання соціально-економічного хаосу в країні, посилюють психологічний та інформаційний тиск на народ і керівництво до такого моменту, коли небажана влада об’єкта агресії буде готова здатися й піти.

Водночас з цим на міжнародній арені активізуються так звані проксі-війни – збройні конфлікти, які розгортаються за ініціативою чи за підтримки зовнішніх держав-акторів, але ведуться чужими руками на території третіх країн. Цей тип конфлікту, за класифікацією К. Дойча [327], поєднує в собі елементи внутрішнього протистояння та зовнішнього впливу, що дає змогу державам-ініціаторам уникати прямої відповідальності за військову ескалацію. У XXI ст. проксі-війни стають особливо привабливим інструментом для глобальних і регіональних акторів, оскільки уможливлюють мінімізацію витрат, зберігаючи при цьому високий рівень стратегічного контролю.

Посередницька війна, опосередкована війна, війна «чужими руками», проксі-війна має два виміри: 1) війна, у якій дві держави воюють не безпосередньо, а використовуючи як сторони в конфлікті треті країни: своїх союзників (сателітів), надаючи рішучу допомогу фінансами, технікою, військовими кадрами (радниками) тощо; 2) міжнародний конфлікт між двома державами, які намагаються досягти власних цілей із допомогою воєнних дій, що розгортаються на території та з використанням ресурсів третьої сторони, під прикриттям розв'язання внутрішнього конфлікту в цій третій державі (К. Дойч, 1964 р.) [269]. За своєю суттю проксі-війна – це громадянська війна, яка спровокована іноземною державою – третьою стороною конфлікту – чи ведеться за її активної ресурсної, політичної й військової підтримки. Прохі-війна може бути не лише між країнами, але й між ТНК і національною державою, що провокує серйозні виклики не лише для держави, але й для міжнародного права, бо не зрозуміло, хто є воєнним агресором [87].

У XXI ст. роль війн «чужими руками» зростає через низку чинників [180]:

1. Поєднання ефективності й дешевизни: такі війни зменшують як фінансові витрати, так і політичні ризики, порівняно з прямим воєнним утручанням; дають змогу підтримувати конфлікт тривалий час за незначні кошти з високою ефективністю;

2. Обмеження воєнних витрат: у результаті системної фінансово-економічної кризи більшість глобальних акторів намагаються скоротити свої військові витрати й не схильні брати безпосередню участь у великий війнах, особливо у формі прямих регулярних дій. Натомість глобальні актори активно використовують місцеві збройні сили, які є дешевою альтернативою дорогим регулярним арміям. Це, своєю чергою, дає змогу не ризикувати життям власних військових;

3. Громадська думка: із кожним роком зростає чутливість громадської думки до людських утрат і до значних витрат на військові сили, утягнуті в збройні конфлікти; громадськість (особливо країн Заходу) не бажає зазнавати

будь-яких утрат, пов’язаних із війнами. У цьому контексті війна «чужими руками» стає прийнятною [453].

Важливим і «перспективним» напрямом проксі-війн є створення й функціонування приватних воєнних компаній, які володіють такими перевагами, порівняно з регулярною армією: 1) їх використання є дешевшим, оскільки потрібна менша інфраструктура й не треба грошей на пенсії та сім’ям загиблих; 2) похорони таких контрактників не привертають увагу населення й медіа, опозиція не може звинуватити уряд у їх смерті [489].

У цифрову епоху особливого значення набуває феномен інформаційної війни (iWar), де поле бою зміщується у віртуальний простір – до цифрових платформ, мережевих сервісів та соціальних медіа. Тут вирішальними стають не ракети й танки, а алгоритми, контент, фейки, кібератаки та психологічна маніпуляція. Інформаційна війна дедалі частіше доповнюється медіавійною, у якій медіа застосовуються як знаряддя для впливу на сприйняття реальності, формування ворожого образу та створення атмосфери страху, недовіри чи ненависті. Згідно з доктриною НАТО, iWar є принципово новою формою агресії, що поєднує методи інформаційного впливу, кібератак, маніпулятивного контенту та дезінформації в режимі реального часу [458]. Цей тип війни істотно відрізняється від традиційної кібервійни, оскільки її головною ціллю є не інфраструктура, а «готова» до впливу аудиторія – інформаційно вразливе населення.

iWar – термін, що застосовується НАТО для опису форми війни в інтернеті; стосується нападів, здійснених через інтернет, які орієнтовані на споживача інфраструктури інтернету, наприклад вебсайти, які надають доступ до онлайн-послуг інтернет-банкінгу. У цьому сенсі iWar відрізняється від кібервійни, кібертероризму, інформаційної війни чи інформаційної боротьби, які належать до використання комп’ютерів, інтернету й інших засобів зберігання чи поширення інформації для здійснення атак на інформаційні системи противника, використовуючи для цього телеінформаційні системи та мережі; мають стосунок до контролю зв’язку, доступу до військової та

критичної інфраструктури, електронного шпигунства, а також командування й управління полем битви, а їхнім полем бою є мережі зв'язку та супутникова розвідка [25].

Дослідники [498] виокремимо п'ять характеристик iWar, які вказують на те, що він може революціонізувати конфлікт: потенціал для розширення наступальних дій; географічне охоплення; важкість викриття (розпізнавання); легкість поширення; вплив на «готові» цілі. Ці якості свідчать про те, що прихід iWar може означати нову військову революцію нарівні з винаходом пороху або атомної бомби.

Як зазначає Ж. Еллюль, інформаційний вплив за допомогою медіа може бути ефективнішим за пряме насильство, оскільки формує сприйняття реальності, політичні вподобання та емоційний фон громадської думки [339]. Медіавійна стає тригером радикалізації, делегітимізації урядів, дестабілізації суспільств – особливо в умовах поляризованого або кризового інформаційного простору. Медіавійна розглядають у двох аспектах: 1) явище формування негативного ставлення в аудиторії медіа до ворога (суб'єкта міжнародних відносин, або учасника політичного процесу всередині країни); 2) широке використання медіа як фактора впливу на супротивника для досягнення необхідних політичних або воєнних переваг, спонукання до прийняття сприятливих для сторони-ініціатора інформаційного впливу рішень, а також впливу на свідомість людини, унаслідок якого вона виконує необхідні дії [474].

Медіавійна – це форма війни, яка продовжується неофіційно навіть у явно мирних умовах. Кожна країна намагається максимально використовувати масмедіа для досягнення своїх політичних цілей. Головними «солдатами» медіавійни є публіцисти, міжнародні експерти з пропаганди та медіаагенти. Медіавійна потребує тіснішої співпраці й координації з боку військових, а також політичних, інформаційних, безпекових, медіа та рекламних секторів країни [87].

Основна мета медіавійни – створення хаосу, коли стає незрозуміло, хто друг, хто ворог, хто виграв у війні й хто програв. Типовими прийомами є приховування реальних подій, реального стану справ; виривання фраз із контексту з наступним акцентуванням уваги саме на них; ототожнювання негативних аспектів певного явища із самим явищем і його сутністю; навішування ярликів; дифамація – образа чи висміювання особи, народу; акцентування на особистих рисах опонента; розповсюдження пліток, чуток тощо; утягування в ситуацію осіб, абсолютно до неї не причетних; навіювання опонентові відчуття тривоги, депресії, іноді з доведенням до повного відчаю й самогубства [127].

Причинами медіавійни часто є нерозв'язаність внутрішньодержавних проблем і бажання об'єднати населення країни проти зовнішнього ворога, тим самим відволікаючи увагу від внутрішніх проблем. Цей тип війни впливає на ментальність і поведінку людей, стимулює радикальні настрої в суспільстві.

Основними засобами медіавійни є радіо, телебачення, вебсайти, преса, міжнародні інформаційні агентства, соціальні мережі.

Крім того, сучасні конфлікти нерідко мають асиметричний характер, коли слабший супротивник компенсує нестачу ресурсів використанням нестандартних стратегій, несиметричних дій та атак на вразливі місця сильнішого [436]. У підсумку це спричиняє появу гібридних загроз – багатокомпонентного явища, що об'єднує військові, економічні, інформаційні, дипломатичні, правові та кібертехнологічні засоби задля дестабілізації держав-жертв без формального оголошення війни.

Асиметрична війна має два визначення: 1) вид війни, що характеризується істотною різницею у військовій силі або можливостях використання стратегій і тактик сторонами-учасниками; 2) конфлікт, у якому ресурси двох сторін суттєво відрізняються й під час боротьби суперники намагаються використовувати характерні недоліки один одного [518]. У 2001 р. Інститут стратегічних досліджень США визначає «асиметрію» як стратегічну концепцію у військовій сфері та сфері національної безпеки –

уміння діяти, організовувати свою діяльність і мислити відмінним від опонентів способом із метою максимізації власних переваг та використання вразливих місць опонента, захоплення ініціативи чи забезпечення простору для маневрування.

Уперше термін «асиметрична війна» з'явився в 1975 р. в статті Ендрю Макка «Чому великі нації програють малі війни» в журналі «World politics» [436], у якій словом «асиметричний» просто пояснювали значну різницю в силі між різними сторонами конфлікту («сила» в цьому сенсі означала матеріальну силу: велика армія, новітня зброя, розвинена економіка й ін.).

У традиційній війні беруть участь принаймні дві професійні армії, які мають приблизно однаковий досвід, ресурси та технології. Єдина реальна відмінність полягає в тому, як вони реалізовують свої стратегії. Таку війну називають симетричною, оскільки обидві сторони, по суті, виглядають однаково. Наприклад, коли союзники боролися з країнами Вісі Зла, це був конфлікт між професійними, національними арміями, які були переважно схожими [417].

Нарешті, усі зазначені форми конфлікту узагальнено в концепції гібридної війни та гібридних загроз, що була інституалізована в рамках НАТО [460] і Європейського Союзу. Гібридна війна включає поєднання військових та невійськових засобів – дипломатичних, економічних, інформаційних, кібертехнологічних – що застосовуються в спосіб, який унеможливлює формальне оголошення війни, але дає змогу досягати політичних цілей через дестабілізацію противника. Яскравим прикладом гібридного впливу є агресія російської федерації проти України, яка супроводжується поєднанням проксі-угруповань, кібероперацій, інформаційних кампаній, юридичного тиску та економічної дестабілізації.

Як відомо, гібридна війна не має жодних правил, її тактика відзначається гнучкістю й планується не під стратегію фронтальної війни, а під стратегію інформаційної війни, де відбувається побудова альтернативної реальності, усередині якої можливе перетворення супротивника на ворога. Головною та

керівною складовою частиною гібридної війни є інформаційна, яка сьогодні набуває нової, модифікованої форми й постає у вигляді мережево-центричної війни.

Під поняттям «мережево-інформаційна війна» розуміють війну нового покоління, у якій моделювання та програмування необхідних процесів у державі противника відбувається засобами інформаційного впливу [62]. Об'єктом мережево-інформаційної війни є масова й індивідуальна свідомість. Інформаційний вплив може здійснюватися як на тлі інформаційного шуму, так і в умовах інформаційного вакууму. Інформаційно-мережева війна будується за тими самими принципами, що й будь-яка рекламна кампанія, але її завдання – продати ідею гібридного агресора. Атака спрямована не на тіла, а на душі супротивника, адже найсильніші конфлікти в історії людства, як відомо, мали у своїй основі релігійний характер. Тому інформаційна війна є головною й дуже сильною складовою частиною гібридної війни. Засобами ведення інформаційної війни є будь-які засоби передачі інформації – від медіа до пошти та пліток [62].

Гібридні загрози – загрози, що створюються противником із наміром і можливістю одночасно застосовувати традиційні та нетрадиційні засоби боротьби й впливу, залежно від нагальної потреби досягнення цілей ворогом (згідно зі Стратегічною концепцією НАТО 2010 р.) [310]. Це сконцентроване, повністю контрольоване та спрямоване на підрив і дестабілізацію опонента, підтримку партизанських рухів, приховане вторгнення шляхом застосування різноманітних (не обов'язково обмежується однією формою) відкритих і таємних тактик, що впроваджуються примусовими військовими та невійськовими засобами (пропаганда, дезінформація, саботаж, зрив комунікацій, постачання електроенергії, диверсії й т. ін.), через інформаційний та економічний тиск, кінцева мета якого – не лише досягнення повного політичного впливу, а й цілковитого домінування над об'єктом – країною-жертвою [284]. У Європі гібридні загрози розглядають як поєднання примусової й підривної діяльності традиційних і нетрадиційних методів

(дипломатичних, військових, економічних, технологічних), які скоординовано можуть використати держави чи недержавні суб'єкти для досягнення конкретних цілей, залишаючись на рівні, нижчому від порога формально оголошеної війни.

«Родоначальником» гібридної війни, а також сучасних гібридних загроз вважається російська федерація, особливо її протиправні дії стосовно України, а також модернізовані операції ІДІЛ, які використовують величезну кількість гібридних способів і засобів проти ослабленої, навіть слабкої держави. Види й сфери виникнення гібридних загроз – тероризм, пропаганда, організована злочинність, кібербезпека, морські пірати, дефіцит ресурсів, космос, агентурні мережі, політичні рухи, спекуляція та маніпуляція історичними фактами, юридичні війни, збурювання міжнаціональних і міжетнічних конфліктів, дезінформація, фейкові новини. Гібридні загрози на сьогодні є дієвим та ефективним інструментом для зміни сучасного світопорядку, регіональних і глобальних лідерів, що призводить до значного тиску на міжнародній арені [386]. Спільна стратегія боротьби з гібридними загрозами, прийнята Європейською комісією у 2016 р., передбачала 22 оперативні дії для підвищення рівня інформованості про гібридні виклики, підвищення стійкості стратегічних секторів, реагування на кризу та відновлення системи. Створено аналітичну структуру – Hybrid Fusion Cell, що відповідає за єдину базу гібридних загроз. Європейський центр із протидії гібридним загрозам (EuropeanCentre of Excellence for Countering Hybrid Threats, Фінляндія 2017 р.) спрямований на виконання таких завдань [346]:

− налагодження на стратегічному рівні діалогу й консультацій поміж учасниками центру, ЄС, НАТО [461];

− проведення досліджень та аналізу сучасних гібридних загроз і методів ефективної протидії;

− розробка доктрини, проведення навчань та тренувань, спрямованих на покращення індивідуальних і спільних можливостей протистояння гібридним загрозам;

– залучення до діалогу урядових та неурядових експертів.

Можливі заходи запобігання гібриднии загрозам і їх подолання: покращення та посилення обізнаності громадян про можливі сучасні загрози, інформаційне забезпечення стійкості структур, захист даних у мережі «Інтернет», інтенсифікація міжнародного співробітництва в цій сфері, розробка 56 відповідних документів/нормативно-правових актів для швидкого реагування й запобігання таким кризам, постійна та детальна співпраця держав із ЄС і НАТО, оскільки гібридні загрози не обмежуються внутрішніми кордонами, а спрямовані на транскордонні мережі або інфраструктуру. Виокремлюють чітку необхідність розвитку гібридного мислення, що зосереджується на таких психічних характеристиках, як розуміння стратегічного контексту, цілісне бачення та підхід до операції, зосередження уваги на потенційних можливостях, охоплення природної складності операційного середовища [31].

На початку XXI ст. глобальна інформаційна екосистема стала ключовим чинником політичної стабільності, безпеки й розвитку. Проте зростання цифрової взаємозалежності супроводжується появою нових форм насильства – інформаційного тероризму, який підриває демократичні системи не шляхом збройної агресії, а через маніпуляції смислами, алгоритмами, довірою. Паралельно в політичній науці формується тріада процесів – глобалізація, глокалізація та фрагментація, – що відображає суперечливу динаміку сучасного світопорядку. Вони є не просто фоном для розвитку інформаційних загроз, а середовищем, у якому тероризм еволюціонує від фізичного до когнітивного виміру.

Глобалізація в класичному визначенні – це процес зростання взаємозалежності держав, суспільств й економік, що охоплює політичну, культурну та інформаційну сфери. На початку 2000-х глобалізацію розглядали як рушія поширення демократії, знань і комунікаційних технологій. Однак у добу цифрових мереж вона стала також інфраструктурою вразливості. Інформаційний тероризм – це феномен, який використовує саме механізми

глобалізації: інтернет-комунікації без кордонів, глобальні соціальні платформи, інфраструктуру даних, анонімність і швидкість поширення контенту. Якщо у XX ст. тероризм був локальним або ідеологічним, то сьогодні він набуває транснаціонального й мережевого характеру. Глобальні медіа стали не лише ареною публічного дискурсу, а й інструментом політичного насильства: атаки на інформаційну довіру, маніпуляції виборами, дестабілізація держав через укидання фейкових наративів перетворюють інформаційний простір на поле бою. Отже, глобалізація створила передумови для дематеріалізації тероризму, коли інформація стала головною зброєю.

Поняття глокалізації (від *global* + *local*) указує на процеси адаптації глобальних явищ до місцевих контекстів. У політичному вимірі це означає, що глобальні ідеї, технології або рухи модифікуються відповідно до локальних культурних, етнічних або ідентичнісних реалій. Інформаційний тероризм саме через глокалізаційні механізми здобуває ефективність. Терористичні або пропагандистські наративи, створені на глобальному рівні, локалізуються в національних контекстах – через мову, історичну пам’ять, релігію, травматичний досвід. Так, глобальний антизахідний чи антидемократичний дискурс у різних країнах адаптується у вигляді локальних теорій змови, історичних ревізій чи псевдопатріотичних рухів. Цей процес можна описати як «фракталізацію» насильства: єдині за суттю меседжі проявляються в множинних локальних формах, що робить боротьбу з ними значно складнішою. Із погляду політичної комунікації, глокалізація створює асиметрію сприйняття: одна й та сама інформаційна кампанія може викликати полярно протилежні реакції в різних суспільствах. Для держави це означає, що політика інформаційної стійкості має бути не лише технічною (кіберзахист), а й культурно-адаптивною, ураховувати локальні ідентичності та особливості наративного простору.

Фрагментація – це політичний і соціальний процес розпаду єдиного комунікаційного простору на множину паралельних, замкнених інформаційних світів. Її причинами стають алгоритмічні бульбашки,

поляризація, утрата довіри до інституцій і домінування емоційних комунікацій. Із погляду політології, фрагментація є не просто інформаційним феноменом, а кризою модерності – коли суспільство втрачає спільну картину реальності. Інформаційний тероризм активно експлуатує ці умови. Його ефективність зростає саме у фрагментованому середовищі, де різні групи мають власні джерела «правди», інтерпретації подій і майже не взаємодіють між собою. Фрагментація інформаційного простору створює передумови для когнітивних атак, адже руйнується саме поняття спільного суспільного дискурсу – основи демократії. Отже, фрагментація є не лише наслідком інформаційного тероризму, а й його мультиплікатором, що підсилює ефект інформаційної зброї через відсутність єдиної системи фактів і довіри.

У політологічному аспекті ці три явища – глобалізація, глокалізація та фрагментація – формують єдиний контур трансформації міжнародних систем у добу цифрової гібридності (табл. 3.1).

Таблиця 3.1

Контур трансформації міжнародних систем у добу цифрової гібридності*

Процес	**Вплив на політичну систему**	**Зв'язок з інформаційним тероризмом**
1	2	3
Глобалізація	Інтеграція економік, спільний інформаційний простір, послаблення державних кордонів	Створює глобальну інфраструктуру для поширення терористичних наративів і кібератак
Глокалізація	Локальна адаптація глобальних трендів, зростання культурної чутливості	Дозволяє терористичним акторам модифікувати свої меседжі під локальний контекст
Фрагментація	Руйнування комунікативної єдності, поляризація суспільства	Поглиблює сприйняття страху, хаосу, недовіри – ключових цілей інформаційного тероризму

* Джерело: розробка здобувача.

Інформаційний тероризм стає інструментом політичного управління хаосом, який поєднує ефекти глобалізації (швидкість, масштаб), глокалізації (культурна релевантність) і фрагментації (когнітивний розпад). У результаті утворюється новий тип війни – когнітивно-гібридна, де основною ціллю є не територія, а свідомість.

Із позицій політичної теорії, така ситуація ставить держави перед дилемою – як зберегти відкритість глобальної комунікації, не втрачаючи контролю над інформаційною безпекою? Відповіддю має стати формування інформаційної стійкості як нової категорії національної політики, що інтегрує три виміри:

1) інституційний – створення системи реагування на когнітивні атаки (центр фактчекінгу, кризові комунікації, законодавство);

2) технологічний – стандарти кіберзахисту, алгоритмічна прозорість, детекція маніпуляцій;

3) соціальний – підвищення медіаграмотності, розвиток критичного мислення, громадська участь у забезпеченні достовірності інформації.

Отже, політична стійкість у XXI ст. прямо залежить від інформаційної зрілості держави, її спроможності протистояти гібридним формам насильства в мережевому світі. Інформаційний тероризм, глобалізація, глокалізація та фрагментація – це не окремі явища, а взаємопов’язані аспекти трансформації політичного простору сучасності. Глобалізація створює умови для розгортання інформаційного тероризму, глокалізація робить його наративи ефективними на локальному рівні, а фрагментація забезпечує довготривалі наслідки у вигляді руйнування комунікативної єдності суспільства. У політологічному сенсі це означає, що сучасна демократія мусить не лише захищати свої інституції, а й оновити парадигму безпеки, визнати інформацію новим простором політичної боротьби. Саме формування інформаційної стійкості – інституційної, технологічної та когнітивної – стає ключовою умовою виживання держав у глобальному світі, де війни ведуться не за території, а за інтерпретації.

Отже, розгляд основних типів сучасних конфліктів – від війни четвертого покоління до медіа- та гібридної війни – є необхідним для розуміння нових реалій глобальної безпеки, а також для формування ефективної стратегії протидії комплексним викликам у сфері національної й міжнародної безпеки. Сучасні війни дедалі частіше відбуваються в нестандартних формах – гібридній, інформаційній, асиметричній чи проксі, де основна мета полягає в підриві внутрішньої стійкості держави без прямої агресії. Такі конфлікти ускладнюють міжнародне реагування та ставлять під сумнів ефективність традиційної системи безпеки. Отож зростає потреба в нових стратегіях захисту, що поєднують військові, інформаційні, правові та дипломатичні інструменти.

3.2. Інформаційна війна та інформаційна зброя: функції, цілі, інструменти впливу

Інформаційна війна – це форма ведення інформаційного протистояння між різними суб'єктами (державами, неурядовими, економічними та іншими структурами), що передбачає проведення комплексу для завдання шкоди інформаційній сфері конкуруючої сторони й захисту власної інформаційної сфери, а також дії, розпочаті для досягнення інформаційної переваги шляхом через заподіяння шкоди інформаційним процесам, що ґрунтуються на інформації та інформаційних системах супротивника за одночасного захисту власної інформації [388]. Основні її методи – блокування або спотворення інформаційних потоків і процесів прийняття рішень супротивника [249].

Уперше термін «інформаційна війна» застосовував воєнний діяч Китаю Сунь-Цзи у 1985 р. Він спробував узагальнити досвід інформаційного впливу на противника. Увів його в науковий обіг американський дослідник М. Маклюен. До головних завдань інформаціної війни відносимо [387]:

– формування атмосфери негативного ставлення до культури та історичної спадщини в суспільстві конкурента чи ворога;

– маніпулювання громадською думкою й політичною орієнтацією населення держави задля створення політичного напруження та стану;

– дестабілізація політичних відносин між партіями, об’єднаннями й рухами задля розпалення конфліктів, стимулювання недовіри, підозри, загострення ворожнечі, боротьби за владу;

– провокування соціальних, політичних, національноетнічних і релігійних зіткнень;

– провокування, застосування репресивних дій із боку влади щодо опозиції;

– зниження рівня інформаційного забезпечення органів влади та управління;

– уведення населення в оману щодо роботи державних органів влади, підрив їхнього авторитету, дискредитація їхніх дій;

– ініціювання страйків, масових заворушень, інших акцій протесту й непокори;

– підрив міжнародного авторитету держави, її співпраці з іншими державами;

– створення чи посилення опозиційних угруповань чи рухів;

– дискредитація фактів історичної, національної самобутності народу;

– формування передумов економічної, духовної чи воєнної поразки, утрати волі до боротьби та перемоги;

– підрив морального духу населення, зниження обороноздатності й бойового потенціалу країни;

– спричинення шкоди інформаційно-технічній інфраструктурі.

Основні об’єкти інформаційної війни – ідеологічно-психологічне середовище суспільства, пов’язане з використанням інформації, інформаційних ресурсів та інформаційної інфраструктури для здійснення впливу на психіку й поведінку людей; ресурси, які розкривають духовні, культурні, історичні, національні цінності, традиції, надбання держави, нації в різних сферах життя суспільства; інформаційна інфраструктура, тобто всі

проміжні ланки між інформацією та людиною; система формування суспільної свідомості; система формування громадської думки; система розроблення й прийняття політичних рішень; свідомість і поведінка людини.

Сучасні процеси глобалізації якісно змінили зміст та форми ведення інформаційних воєн. Глобалізація подвійно вплинула на характер сучасних конфліктів і війн: по-перше, спричинила ерозію державної влади та соціальну вразливість, по-друге – створила нові можливості й економічні заохочення, що виникають під час громадянської війни [52, с. 140].

Розглядаючи тенденції глобального інформаційного суспільства, мусимо наголосити на міжнародному кібертероризмі, який за допомогою сучасних телекомунікацій продукує «терористичну свідомість», надає можливість терористичним групам, завдяки медіа, маніпулювати масовою свідомістю.

Кібертероризм є високодинамічним: сайти швидко з'являються та зникають, змінюють свої назви, доменні імена, однак залишають зміст посилань і статей на сторінках кібервидань. Їхня мета – вплинути на думки, поведінку, свідомість або посіяти страх, паніку, деморалізувати суспільство; викликати почуття провини за дії своєї влади, спричинити громадянське протистояння, розв'язати дискусії на тему тероризму [225, с.190].

Найпоширенішим явищем є кіберзлочинність та хактивізм [90]. Останній застосовуються шляхом використання комп'ютерних мереж у політичних цілях [560]. Прикладом є блокування роботи сайтів урядів Тунісу і Єгипту організацією хактивістів «Anonymous» у січні 2011 р. на знак підтримки народних рухів проти чинних політичних режимів [90].

Більшість розвинутих країн володіє потужним інформаційним потенціалом (додаток Д), який за певних умов забезпечить будь-якій із них досягнення політичних цілей. До того ж на сьогодні відсутні міжнародні юридичні норми ведення інформаційної боротьби. Моніторинг публікацій у медіа переконливо засвідчує, що головна тенденція інформаційної боротьби полягає в підвищенні її ролі у виконанні зовнішньополітичних завдань.

Удосконалення нетрадиційних засобів на сучасному етапі науково-технічної революції призвело до виникнення зброї глобального ураження, системне застосування якої спроможне знищити середовище існування людства.

Використання інформаційних засобів і систем збільшує можливості державного впливу. Водночас зростає вразливість систем управління від цілеспрямованого впливу в інформаційній сфері. Ці тенденції об'єктивно приводять до розширення арсеналу методів і засобів боротьби, посилення її впливу на хід і результат воєнних дій, зростання кількості застосовуваних у ній сил та засобів. На початку XXI ст. значно зросла кількість держав, стосовно яких здійснено кібератаки [57].

На сучасному етапі домінування штучного інтелекту та дипфейків до повномасштабного вторнення рф в Україну превалює тенденція розв'язання зовнішньополітичних конфліктів без збройного насильства. Інформаційна війна перестала бути другорядним чинником, доповненням до «основних» подій. Вона перетворилася на один із найважливіших механізмів ведення активних дій, про який говорять нарівні з використанням збройних сил і техніки, а також стала легітимним засобом політичної боротьби [166, с. 7].

Незважаючи на те, що значна частина суспільства усвідомлює процес цілеспрямованої інформаційної атаки на противника та допускає можливість застосування «брудних» технологій, вона все одно піддається маніпулюванню з боку медіа. У результаті, у комунікативному протистоянні перемагає не той, хто говорить правду, а той, кому вдалося показати глядачам більш захопливий «інформаційний серіал» і гранично чітко обґрунтувати свою позицію. Тобто, чим більшими інформаційними можливостями володітиме країна, тим імовірніша можливість досягнення стратегічних переваг у майбутній системі міжнародних відносин [236, с.71].

Інформаційні війни стали аксіомою сучасних міжнародних відносин і дають змогу досить ефективно, із залученням незначних фінансових та людських ресурсів досягати потрібних цілей: усе залежить від ступеня професіоналізму реалізаторів інформаційних операцій. Відстоювати свої

позиції в інформаційному протиборстві буде легше тим країнам, які матимуть гармонійно розвинуте й тому захищене інформаційне суспільство [5, с. 10].

Види інформаційної війни – психологічна війна; кібервійна; мережева війна; ідеологічна війна; радіоелектронна боротьба, яка може проявитися такими способами, як телебачення й радіомовлення, можуть бути подавлені; ресурси телебачення та радіомовлення можуть бути захоплені для здійснення дезінформації; мережі комунікацій можуть бути заблоковані або недоступні; операції фондової біржі можуть саботуватись електронним утручанням, створюючи витік інформації або поширюючи дезінформацію [136].

Інформаційна війна харкктеризується використанням інформаційної зброї – це різновид зброї, головними елементами якої є інформація, інформаційні технології (зокрема технології інформаційного впливу), інформаційні процеси та технічні засоби, що застосовуються в інформаційному протиборстві[175]. Під інформаційною зброєю потрібно розуміти сукупність організаційних й організаційно-технічних впливів на інформаційні системи, системи автоматизованого та автоматичного керування, системи й мережі зв’язку тощо, здійснених із використанням систем і засобів знищення, викривлення, розкриття, крадіжки, створення хибної інформації; систем та засобів подолання систем захисту; засобів обмеження або розширення доступу до інформації й ресурсів законних користувачів; систем і засобів протидії та дезорганізації роботи технічних засобів, комп’ютерних систем; систем і засобів управління ресурсами інформаційних систем [48].

Швидка передача великої кількості інформації стає найважливішим завданням під час створення сучасних систем управління, рішення якого позв’язується з розвитком космічних систем зв’язку й широким використанням волоконно-оптичних ліній. При цьому подібні елементи інформаційної інфраструктури стають найбільш уразливими з погляду інформаційної наступальної операції.

Інформація стала не лише ресурсом, а й знаряддям впливу та контролю. Інформаційна зброя – це не метафора, а реальний інструмент ведення сучасних війн, який дедалі частіше застосовується державами, терористичними угрупованнями, корпораціями та навіть окремими особами. На відміну від традиційної зброї, вона не знищує фізично, але руйнує ментально – підриває довіру, дестабілізує суспільства, провокує хаос, маніпулює свідомістю, звідси – класифікацію її технологій виведено окремо в табл. 3.2.

Таблиця 3.2

Класифікація технологій інформаційної зброї*

Тип технології	Приклади застосування	Цільовий ефект
1	2	3
Кібератаки	DDoS, злам урядових систем, шкідливе ПЗ (віруси, трояни, ransomware)	Порушення комунікацій, дестабілізація інфраструктури, саботаж
Дезінформація	Фейкові новини, deepfakes, бот-мережі, фабрики тролів	Формування хибної реальності, втрата довіри до влади, поляризація суспільства
Психологічні операції (PSYOPS)	Деморалізуючі меседжі, відео зі сценами насильства, погрози, викривлення фактів	Страх, паніка, демотивація, зниження бойового духу, моральне виснаження
Соціальна інженерія	Фішинг, інженерні атаки на персонал, маніпуляція лідерами думок	Отримання конфіденційної інформації, зниження опору, проникнення в закриті системи
Меметична зброя	Політизовані меми, візуальні жарти, вірусні образи	Викривлення смислів, нормалізація екстремізму, емоційна маніпуляція
Інформаційні блокади	Блокування медіа, заборона соціальних мереж, контроль інтернет-трафіку	Ізоляція від альтернативної інформації, посилення контролю над населенням

Аудіовізуальна маніпуляція	Deepfakes, синтетичний голос, змінені відео	Імітація заяв лідерів, фальсифікація подій, компрометація
Алгоритмічне маніпулювання	Маніпуляції соцмережевими стрічками, підбір контенту через AI-алгоритми	Радикалізація, формування «інформаційної бульбашки», спотворення реальності
Мікротаргетинг (цільова пропаганда)	Політична реклама в соцмережах із точним націлюванням на аудиторії	Вплив на виборчу поведінку, мобілізація / демобілізація електорату, маніпуляція емоціями
Насичення інформаційного простору	Потік хаотичних новин, дезорієнтуюча інформаційна «піна»	Утома від новин, апатія, небажання перевіряти інформацію
Інформаційне маркування (labeling)	Навішування ярликів: «фашист», «ворог народу», «зрадник», «іноагент»	Делегітимація опонентів, створення негативного іміджу
Фінансована пропаганда через медіа	Запуск лояльних телеканалів, YouTube-каналів, Telegram-мереж	Поширення ідеології, виправдання агресії, нормалізація авторитаризму

* Джерело: розробка здобувача.

Цілеспрямована організація подібних ситуацій і є пріоритетним завданням під час застосування інформаційної зброї в ході ведення наступальної інформаційної війни й досягнення інформаційної переваги над противником. Ефективна протидія такого виду діям противника визначає мету оборонної інформаційної війни [207, с. 5].

Основними способами й методами застосування інформаційної зброї як загрози безпеці можуть бути:

– завдання збитків фізичним елементам інформаційної інфраструктури (руйнування мереж електроживлення, створення перешкод, використання спеціальних програм, які стимулюють виведення з ладу апаратних засобів, а також біологічних і хімічних засобів руйнування елементної бази);

– знищення чи пошкодження інформаційних, програмних і технічних ресурсів противника, подолання систем захисту, упровадження вірусів, програмних закладень і логічних бомб;

– вплив на програмне забезпечення та бази даних інформаційних систем і систем управління задля їх спотворення чи модифікації;

– загроза або здійснення терористичних актів в інформаційному просторі (розкриття та загроза оприлюднення чи оприлюднення конфіденційної інформації про елементи національної інформаційної інфраструктури, суспільно значущі й військові коди шифрування, принципи роботи систем шифрування, успішний досвід ведення інформаційного тероризму тощо);

– захоплення каналів медіа з метою поширення дезінформації, чуток, демонстрації сили та доведення до відома своїх вимог;

– знищення й придушення ліній зв'язку, штучне перевантаження вузлів комутації;

– вплив на операторів інформаційних і телекомунікаційних систем із використанням мультимедійних та програмних засобів для введення інформації в підсвідомість або погіршення здоров'я людини;

– вплив на комп'ютерне устаткування бойової техніки й озброєння, щоб вивести їх із ладу [233, с. 149].

Формування єдиного глобального інформаційного простору, що є природним результатом розвитку світової науково-технічної думки та вдосконалення комп'ютерних й інформаційних технологій, створює передумови для розроблення та застосування інформаційної зброї. Володіння нею й засобами захисту стає однією з головних умов забезпечення національної безпеки держав у XXI ст. Перегляд пріоритетів та акцентів в інтерпретації проблем національної безпеки поставив науку та практику перед необхідністю розробки абсолютно нового аспекту – безпеки психологічної. Нині створено багато нових засобів впливу на психіку людей й управління їхньою поведінкою (рис. 3.1). У медіа періодично з'являється інформація про

американські програми «МК-ультра», «Артишок», а також аналогічні напрацювання Франції, Німеччини, Ізраїлю, Японії тощо. В останні десятиліття можливості впливу на психіку людини різко зросли. Однією з головних причин цього є значні досягнення у сфері психотроніки, парапсихології, біоенергетики, інших психофізіологічних феноменів [41].

Рис 3.1. *Інформаційні впливи на населення держав* *

*Побудовано здобувачем за [48].

Пошук нових форм і методів впливу на психіку особи, великих мас людей розгорнутий у більшості провідних країн світу. Лідером у цій справі є США, які мають у своєму розпорядженні найбільш розгалужену мережу інститутів, центрів, лабораторій, підприємств для проведення відповідних теоретичних досліджень і виконання завдань військово-прикладного характеру. Великий інтерес до подібних розробок проявляють військові відомства США.

Аналіз найвідоміших міжнародних військових, політичних та економічних конфліктів кінця XX – початку XXI ст. показав, що інформаційно-психологічна зброя як один із засобів гібридної війни має бути прирівняна до зброї масового знищення. Не вбиваючи фізично,

психотехнології стають причиною групових, а також масових психічних розладів, що призводять до соціальних конфліктів.

В інформаційній війні об'єктом впливу стають комп'ютери та інформаційні системи. В інформаційно-психологічній війні до інформаційного напряму приєднується психологічний – об'єктом впливу стають індивідуальна й масова свідомість [137]. У форматі використання усього спектра інформаційно-психологічних операцій соціальні онлайн-мережі мають можливість забезпечувати координацію протестних та терористичних рухів; поширення контенту, що належить до інформаційної зброї; збирання важливої інформації, що становить інтерес для агресора; відстеження суспільних настроїв; локалізацію джерел інформації, яка становить небезпеку [113].

Інформаційна зброя включає широкий спектр технологій: кібератаки, глибинні фейки (deepfakes), бот-мережі, нейромережеві генератори текстів, алгоритми соціальних медіа, а також технології Big Data, – що дають змогу точно націлювати пропагандистські повідомлення на вразливі аудиторії. Найнебезпечнішим є поєднання цих інструментів у межах інформаційно-психологічних операцій (ІПсО), спрямованих на зміну поведінки цілих соціальних груп.

Особливу увагу привертають штучний інтелект та аналітика соціальних мереж, які дають змогу автоматизувати створення й поширення дезінформації в реальному часі. Наприклад, за допомогою AI можна створити десятки «персоналізованих» новин для різних демографічних груп, які маніпулюватимуть саме тими страхами або уявленнями, що притаманні цільовій аудиторії. Водночас інформаційна зброя є складною в регулюванні. На відміну від традиційних видів озброєння, вона часто ґрунтується на легітимних інструментах: медіа, соціальних платформах, рекламі, навіть освітніх чи наукових ресурсах. Саме це розмиває межу між свободою слова та ворожим впливом.

Для демократичних держав основною дилемою залишається пошук балансу між забезпеченням інформаційної безпеки й захистом прав людини. Розробка нормативних рамок для виявлення та протидії інформаційним атакам, посилення цифрової грамотності громадян, розвиток стратегічних комунікацій і міжнародне співробітництво у сфері кібербезпеки – це ключові напрями протидії використанню інформаційної зброї. Отже, технології інформаційної зброї – це не загроза майбутнього, а реальність сьогодення. Їх ефективність і доступність роблять їх привабливими для широкого кола акторів, а їх невидимість – особливо небезпечними. Протидія цим загрозам потребує не лише технологічної, а й інтелектуальної мобілізації суспільств, спроможних критично мислити та розпізнавати маніпуляції в цифровому просторі.

Фейкова інформація (англ. *fake* – фальшивий, сфабрикований) може трактуватися як: 1) шахрайство, повністю або частково вигадана інформація про суспільні події, справжніх людей або про речі, явища, що подаються в мас-медіа під виглядом справжніх журналістських матеріалів; 2) спеціально спотворена новина, подія чи журналістський матеріал, який містить неправдиву або перекручену інформацію, що дискримінує певну людину або групу осіб в очах аудиторії [88]. Як синонім до поняття вживається термін «журналістська качка» чи латинське словосполучення «non testatur», чи його скорочення NT, що в перекладі означає «не перевірено», але німецькою мовою звучить як «качки». У сучасних українських соціальних медіа фейкова інформація спрямована на дезінформацію, уведення в оману аудиторії, що, у результаті, викликає негативні емоції. Д. Кулеба в книзі «Війна за реальність: як перемагати у світі фейків, правд і спільнот» зазначає, що «фейк – це сконструйована фальшива новина і маніпуляції так, щоб у споживачів складалося чітке переконання: це і є важлива для мене правда, яку всі приховують від мене, тому що в умовах комунікативної війни емоції загострюються, а критичне мислення притуплюється» [111].

Фейками можуть бути фотографії, зроблені в програмі Photoshop; відеоролики, що не несуть правдивого контенту; написані або вигадані неправдиві новини, які важко відрізнити від правдивих; фальшиві акаунти в соціальних мережах тощо. Мета поширення фейків дуже різна – від поширення новин заради грошей до шахрайства, особливо для fishing-атак (вид шахрайства, мета якого – виманювання в довірливих чи неуважних користувачів мережі персональних даних клієнтів онлайн-аукціонів, сервісів із переказу або обміну валюти, інтернет-магазинів). Основне завдання фейкових повідомлень зводиться до передавання недостовірної інформації й прагнення переконати аудиторію в її правдивості.

За методом поширення фейки класифікують на медійні, які створюють спеціально для медіа й через них поширюються; мережні чутки, що поширюють чиюсь вигадку через соціальні мережі. За формою розрізнюють фотофейк – найбільш поширений і водночас найлегший для спростування; відеофейк та фейковий журналістський матеріал [88]. Також фейки можна систематизувати як навмисно створені; вигадки, що сприймаються як правда; масштабні містифікації; умисне однобічне висвітлення подій; історії, у яких «правда» є суперечливою.

Британська телерадіомовна корпорація (BBC) пропонує таку класифікацію фейків: неправдиві новини, поширені навмисно; новини, які містять правдиву інформацію, але не є цілковито точними (може виникнути, якщо журналісти чи блогери не перевірили факти, перш ніж опублікувати матеріал, або перебільшили деякі з них) [380]. Потрібно виокремити три типи неправдивих повідомлень, характерних для українського інформаційного простору: спеціально створені й розповсюджені, аби завдати шкоду; створені без наміру завдати шкоди; створені на основі конкретних подій чи інформації та поширені для того, щоб завдати шкоду.

Найбільш доступні канали для поширення фейків – інтернет-платформи, соцмережі та месенджери. Неперевірену інформацію, поширену через ці канали, можуть підхопити як «класичні» медіа, так і інші сайти. Можливість

фейкам швидко поширюватися надають соціальні мережі. Вони створюють відчуття реальної причетності до соціально-політичних процесів не лише на рівні спілкування, а й конкретних дій, участі в розв'язанні конкретних суспільних проблем. З огляду на такі властивості, як доступність, анонімність, оперативність, високий рівень довіри, сегментація за інтересами, соціальні мережі, є найзручнішими для поширення фейків.

Серед детермінант, що сприяють використанню соціальних мереж, виокремимо такі: дешевизна й мобільність поширення інформації; можливість приховати реальні джерела, поширювати фейки в кількох мережевих ресурсах; безкарність, анонімність; технічні можливості інтернету дають змогу не лише створювати мережі та впливати на споживачів інформації, але й проводити моніторинг мереж, визначаючи можливі мережі й адреси поширювачів тієї чи іншої інформації.

Завдяки розширеному доступу до інформації та її продукування, полегшенню взаємодії людей, розділених територіально, та можливості утворення спільнот однодумців відкриваються нові можливості для використання соціальних мереж для поширення фейків.

У цифровому столітті реальність і вигадка дедалі частіше зливаються в одне ціле. Технологія *deepfake* – глибокої підробки на основі штучного інтелекту – стала одним із найяскравіших прикладів цієї тенденції. Вона дає змогу створювати надреалістичні відео або аудіо, де люди говорять або роблять те, чого насправді ніколи не відбувалося. І хоча спочатку deepfake-технології застосовувалися для розваг або творчих експериментів, сьогодні вони дедалі частіше стають інструментом інформаційної війни, пропаганди, шантажу та маніпуляцій. Deepfake – це продукт поєднання нейромережевого машинного навчання (особливо генеративно-змагальних мереж – GAN) і великих обсягів даних. Алгоритми аналізують тисячі зображень чи звукових зразків конкретної людини, щоб «навчитись» імітувати її міміку, голос, інтонацію, рухи. Результат майже не відрізнити від справжнього відео. І хоча

експерти можуть виявити підробку, для пересічного користувача deepfake видається абсолютно достовірним.

Небезпека технології deepfake полягає в її руйнівному потенціалі – дезінформації та фальсифікації подій. Виготовлення фейкових відео з політичними лідерами, які «оголошують війну», «визнають поразку» чи «роблять компрометуючі заяви», може спричинити паніку, провокації або зруйнувати репутацію; шантаж і репутаційні атаки. Політики, бізнесмени чи активісти можуть стати мішенню фейкових відео з компрометуючим змістом –зокрема порнографічного або кримінального характеру; підрив довіри до інформації загалом. Навіть реальні відео можуть бути поставлені під сумнів у суспільстві, що вже стикалося з deepfake-маніпуляціями. Це породжує ефект «реальності після правди», коли люди не вірять нічому; військово-політичні провокації. Deepfake може бути використаний як тригер в умовах гібридного конфлікту – для дестабілізації громадської думки, зриву переговорів або провокації міждержавної ескалації.

У зв’язку з цим постає питання захисту. На міжнародному рівні лише починають формуватися правові механізми для регулювання застосування deepfake-технологій. У США, ЄС, Китаї розробляють законопроєкти, що вимагають маркування фейкових матеріалів. Водночас ключовими напрямами захисту залишаються цифрова медіаграмотність населення, технології виявлення deepfake-контенту, жорсткі санкції за використання deepfakes із метою шкоди, міжнародна кооперація у сфері цифрової етики й штучного інтелекту.

Отже, deepfakes – це не лише технологічний прорив, але й етичний виклик. Дипфейки знецінюють довіру до фактів, ставлять під загрозу інформаційну безпеку, а в умовах геополітичної напруги можуть перетворитися на справжню інформаційну зброю. Людство мусить навчитися не лише створювати нові інструменти, а й відповідально ними користуватися.

На сьогодні інтернет, а особливо соціальні мережі, є невід’ємним атрибутом життя сучасної людини. Підтвердження цього – велика кількість

користувачів. Аудиторія соціальної мережі «Facebook» становить понад 1 млрд користувачів, «Twitter», «Google +», «LinkedIn» – понад 300 млн.

Яскравим прикладом інформаційно-психологічного впливу в сучасних умовах є соціальні мережі. Попри те, що вони забезпечують спілкування між людьми, надають широкий спектр медіа-можливостей, існує великий ризик інформаційного впливу на свідомість користувачів мереж. Зазначимо, що існує повна довіра всій інформації, яка публікується в соціальній мережі. Користувач переважно не перевіряє отриману інформацію й приймає її за достовірну. Серед основних моделей ведення інформаційних війн у соціальних медіа виокремлюють такі, як модель мережевих атак, модель із залученням користувачів-волонтерів, модель тотального блокування.

Для того щоб запобігти поширенню фейкових новин, deepfake у соцмережах, видання The Huffington Post склало перелік правил, як їх розпізнавати [383]:

1. Читати більше ніж назву. Якщо проглянути новину до кінця, можна виявити, що назва ніяк не пов’язана з текстом новини або ж у ній немає жодних даних, які підтверджують її правдивість;

2. Оцінити надійність джерела повідомлення – незнайомі сайти, заповнені оголошеннями й назвами, написаними капслоком, повинні викликати скепсис. Перевіряти через пошукові системи тексти, які були опубліковані раніше (це дасть уявлення про те, чи є джерело надійним), а також URL сторінок, які видаються підозрілими, аби переконатися в тому, що це не фальшивка, яка маскується під надійне джерело;

3. Звертати увагу на дату публікації й час. Поширений елемент фейкових новин – видавати старі публікації за нові. Якщо в новині є посилання на інші джерела, проглянути їх, звертаючи увагу на те, коли вони опубліковані та як у них описується подія, особливо коли йдеться про час;

4. Хто автор? Ознайомитися з попередніми публікаціями автора – його бекграунд дасть змогу зрозуміти, чи справді автор є журналістом, чи не писав він дезінформуючих статей до цього;

5. Ознайомитися з джерелами, на які посилається новина. Відсутність посилань або джерел, із яких узято ті чи інші заяви, є очевидним сигналом того, що пост, імовірно, є фейком. Будь-які заяви або цитати посадовців повинні бути підкріплені надійними джерелами;

6. Звертати увагу на сумнівні цитати й фотографії. Скептично ставитися до шокуючих або підозрілих цитат та опублікованих фотографій із місця подій;

7. Не варто поширювати новини лише тому, що поділяєте думку автора або ж приймаєте одну із сторін конфлікту;

8. З'ясувати, що інші видання пишуть із цього приводу. Якщо жодне інше надійне джерело не повідомляє про зазанчені події, то, очевидно, новина є рейковою;

9. Замислитися, перш ніж робити перепублікацію. Новинні сайти, які поширюють дезінформацію, працюють із розрахунком на те, що читачі поширюватимуть їхні новини.

Соціальна інженерія – це використання соціальних медіа для атаки на репутацію певної особи чи компанії. Наприклад, компанії зі сторінками в соціальних мережах стикаються з уразливістю того, що їхні сторінки або зламують, або люди надсилають інформацію, неприйнятну для клієнтів. Наприклад, порнографічні матеріали, розміщені в акаунті в соціальних мережах. Це також може відштовхнути клієнтів. Порушення бази даних відбувається, коли компанія не може легко отримати доступ до інформації зі своєї бази даних через її порушення. Зазвичай хакери порушують і змінюють паролі під час доступу до обсягів даних.

Наприклад, коли американське ФБР було зламано, а відеозапис убивства американських військових з гелікоптера випущений незаконно. Такі порушення часто мають серйозні наслідки, оскільки вони розкривають конфіденційну інформацію та секрети, які є ключовими для компанії. Погане управління ідентичністю та доступом також може призвести до інформаційного тероризму, оскільки інформація, яка не повинна перебувати в

руках терористів, опиняється в їх руках, що впливає на діяльність компанії. Прикладом може слугувати обмін із друзями паролями доступу, що, урешті, призведе до інформаційного тероризму. Цю проблему буде дуже важко усунути, оскільки вона залежить від прогресу технологічного розвитку, що охопив Африку, особливо з появою волоконно-оптичної мережі.

Відомий факт, що «соціальні медіа стрімко й широко вбудовуються» в наше суспільство та змінюють спосіб нашого життя, навчання та роботи. Вони потребують незначної технічної експертизи чи взагалі не визначають її ролі у видавничій галузі, що дає змогу авторам здійснювати прямий контакт із читачами й взаємодіяти з ними. Робочі процеси цифрового видавництва сприяють «підвищенню редакційної точності, вищим стандартам виробництва та більшій економії витрат і часу», але водночас вони розширили обов'язки редакторів і збільшили ризик професійної ізоляції.

Для того щоб висвітлити питання ефективності роботи соцмедіа у видавничій галузі, треба звернути увагу, власне, на соціальні медіа як вид медіа й низку онлайн-технологій на принципах Веб 2.0, завдяки яким споживачі контенту через власні дописи стають його співавторами і можуть співпрацювати, ділитись інформацією, спілкуватися, або брати участь у будь-якій інший соціальній активності з іншими користувачами певного сервісу [503]. Хоча рівень участі в соціальних медіа може відрізнятися, чітке розуміння можливостей їх інструментів є важливим для професіоналів, які займаються редагуванням, особливо тому, що вони працюють у галузі, яка цілковито керується виробництвом контенту.

Незалежно від того, говоримо ми про друковану чи цифрову видавничу діяльність, соціальні медіа – це гнучкий інструмент, який дає змогу видавцям охопити будь-який тип читачів і поширити свій вплив. Кожен допис або твіт, яким можна поділитися, стає відразу видимим для групи нових, потенційних читачів. Активність, завдяки публікації цікавого контенту, посилань та промороликів – це лише частина стратегії соціальних мереж, яка включає також участь у дискусіях, написанні коментарів, спостереженні, уподобанні й обміні

інформацією. Однак побудова десятків каналів соціальних мереж не є ні ефективною, ні необхідною. Краще витратити час на створення однієї-двох платформ. Ключем до їх вибору повинен стати аналіз цільової групи. Соціальні медіа – це прямий спосіб зв'язку з нинішніми та потенційними читачами. Ці платформи дають змогу полегшити зв'язок з іншими користувачами або клієнтами, які можуть бути безкомпромісними у своїх коментарях і думках. Дописувачі отримують миттєвий зворотний зв'язок у формі «подобається», «поділитися» або «смайлик».

Медіаплатформи відображають природну поведінку людей у багатьох сферах. Це чудовий приклад того, як працює маркетинг рекомендацій в інтернеті – є більша ймовірність, що рейтинг журналу підніметься. Людям потрібно поділитися власним досвідом та направити думки інших на цифровому рівні. Тож природно створювати спільноти, подібні до груп Facebook. Соціальні медіа відіграють роль сповіщення в режимі реального часу. Однією з головних причин того, чому видавці й деякі бренди присутні на цих платформах, є потреба інформувати своїх «фоловерів» (і навпаки – послідовники хочуть бути в курсі подій), завантажуючи менеджер обміну ПК [194]. Це правило стосується, передусім, новинних порталів та сайтів, які роблять крок уперед в інтернет-маркетингу й повідомляють своїх читачів про найновіший уміст через мобільний додаток. Швидкий перегляд соціальних мереж дає змогу дізнатися про поточні події, переглянути останній номер журналу чи нову книгу. Крім того, багато каналів пропонують пряму трансляцію й, завдяки цій функції, можна показувати людям події, конференції, вечірки, присвячені випуску книг; або інтерв'ю, яке вони не могли бачити в прямому ефірі.

Реклама в соціальних мережах може стати чудовим доповненням до стратегії монетизації вмісту. Сила цього рішення полягає у використанні інформації про користувачів із метою розповсюдження найбільш релевантних оголошень: зростання продажу й збільшення кількості фанатів; використання

вмісту, створеного клієнтами для реклами; краще націлювання на нових клієнтів; A / B тест із застосуванням аналітики платформи [235].

Соціальні медіа відіграють важливу роль у професійному житті незалежних авторів: це стає основною лінією просування власних публікацій, підвищує незалежність у прийнятті рішень, забезпечує нагляд за цілковитим процесом просування книг самостійно, без участі видавництва.

Отже, можливість використовувати платформи соціальних медіа для розповсюдження контенту дає їм фантастичну можливість охопити набагато ширшу аудиторію. Однак зростаюча залежність від соціальних платформ виявляє необхідність повернення влади та захоплення читачів у власних доменах видавця. І саме тут взастосування важливих соціальних медіа для посилення редакційних статей відіграє надзвичайну роль. Починаючи від журналістів, політиків, бізнесменів, лідерів громадських організацій і закінчуючи пересічним користувачем, усі публікують свої спостереження, переконання та думки в соціальних мережах. Соцмережі інтегрують усе більше різноманітних функцій у повсякденне життя, а також повністю охоплюватимуть усі аспекти життя людини, причому як онлайн, так і офлайн, – завдяки подальшому розвитку геолокації.

Більшість сучасних людей, зокрема молодь, поглинає інформацію з популярних соціальних мереж (Facebook, Instagram, TikTok, Twitter і т.ін.), де не раз можна стати свідком конфліктів користувачів у коментарях, що призводить переважно до деструктивного діалогу. Досить часто таке трапляється в ході президентської чи парламентської передвиборчих кампаній. Велика кількість людей переконує інших в ефективності роботи того чи іншого політичного лідера, якого вони підтримують, а інші ж виступають за свого кандидата.

Спостерігаючи за перебігом «переписки», чи взаємного звинувачення, можемо звернути увагу, що один і той самий користувач / дописувач з’являється з однаковими образливими чи хвалебними коментарями під різними повідомленнями й постами. Із цього можна зробити висновок, що

реагує бот. Бот – це програмне забезпечення, створене людиною, яка працює за принципом робота, тобто виконує одноманітні та механічні дії, що закладені в систему [134]. Це може бути рандомна реєстрація на сайтах, або спам-розсилка; більшість комп'ютерних вірусів працюють за подібною схемою.

Ефективно використовують можливості соціальних мереж боти й тролі. Боти – як певна технологія, яка за допомогою спеціальних програм здійснює комунікацію в соціальних мережах. Тролі – це особи, які за матеріальну вигоду підбурюють у соцмережах і провокують. Замовний тролінг полягає в навмисному розміщенні повідомлення провокативного, принизливого змісту, аби спровокувати суперечку, довести опонентів до нестями від роздратування, обурення. Розміщення «вірусних» матеріалів на ресурсах відео- та фотохостингу у соціальних мережах дає змогу ефективно поширювати потрібний контент.

Чим знаковіша подія, чим більша аудиторія впливу, тим очевидніша кількість ботів, що спрацьовують на відповідно закладені вирази, вислови, словосполучення для реклами, поширення посту, підвищення зацікавленості, а також і непоодинокі випадки для негативного піару чи образливого контенту. Звідси випливає таке поняття, як «ботоферма». Ботоферма – це спеціальне офісне приміщення з невеликою кількістю людей, які працюють із декількома фейковими сторінками / акаунтами задля пропаганди, агітації, поширення дезінформації тощо. Ботоферми – це, передусім, хороший спосіб заробітку, а з іншого боку – удалий інструмент різноманітного впливу для політиків, бізнесменів, відомих публічних людей та ін.

З огляду на вищезгадане, звертаємо особливу увагу на те, що в ботів є спеціально визначені прийоми, щоб здаватися реальними людьми:

– продукування діалогів між різними фейковими акаунтами, де особливу увагу акцентують на перевагах конкретного політика;

– управне маніпулювання думками дописувачів шляхом підведення до думки, що саме за визначеного кандидата потрібно голосувати на виборах.

Алгоритм же створення фейкових сторінок досить простий і надзвичайно шкідливий, коли співробітники ботоферми беруть фотографії реальних людей із соціальних мереж, що на сьогодні заборонено на території України («Вконтакте», «Одноклассники» тощо), завантажують їх на порожні, щойно стоворені фейкові сторінки у Facebook із вигаданими іменами та прізвищами.

Основним завданням політичних ботів є маніпуляція громадською думкою, реалізується вого через різноманітні функції: атаки на опонентів політика; створення негативного образу; привернення уваги до конкретної події чи допису; термінове «розганяння» інформації; відволікання уваги від скандалу або неприємної ситуації.

Досить часто інструментами політичних ботоферм є написання коментарів (по 20–30 коментарів на підтримку посту, щоб він почав розкручуватися в групах соціальної мережі), а реальні люди / учасники починають залучатися лише в тому випадку, коли вже є якась активність. Щоб усі коментарі були з необхідним наголосом чи акцентом, ботам зазвичай скидають «методички», де завдання оформлене у вигляді 5–6 ключових тез, виразів, словосполучень і вказано майданчики, де треба активно працювати (зазвичай це або персональні сторінки політиків, або популярні сторінки з політичними новинами).

Звернемо увагу, що неабияку загрозу інформаційній безпеці також можуть становити так звані веброботи, або інтернет-боти, – спеціально розроблені програми, що виконують повторювальні завдання в інтернеті автоматично [20]. Вони створені спершу для того, аби спростити рутинне життя людини – каталогізувати інформацію з різних вебсайтів і виділити основне. Не всі з них корисні, оскільки шкідливі боти, які використовуються кіберзлочинцями – це програми, призначені для таємного встановлення на незахищений пристрій. Здійснюється це через розповсюдження спаму. У цьому випадку пристрій заражається й стає частиною бот-мережі (винайдена на відстані кіберзлочинцем мережа для реалізації власних незаконних дій). На

думку експертів, цей вид мережі є одним із найнебезпечніших в інтернеті, адже пропускна спроможність пристрою й системні ресурси автоматично здаються в оренду, аби забезпечити допомогу нападу на інших користувачів організації.

Подібне зараження комп'ютера можливе у випадку перегляду вебсторінок, коли програмне забезпечення в системі є застарілим, а також надсилаються підозрілі листи спамерами на електронну пошту.

Превентивними заходами можуть бути відповідальне ставлення до вибору антивірусної системи; слідкування за оновленням програмного забезпечення, адже застарілі програми створюють усі умови для «інфікування»; обережне ставлення до вкладення власної електронної пошти; повне ігнорування підозрілих вікон та вебоголошеннь.

Отже, ботоферми можуть становити загрозу інформаційній безпеці не лише окремо взятої держави, але й світу загалом, оскільки вона значно більша за класичну пропаганду. Це таргетоване промислове виробництво фейків, які влучно потрапляють на ґрунт незнання та влучно застосовують теорію до сучасних умов і вимог соцмереж.

Отже, сучасна інформаційна зброя – це комплексна система гібридного впливу, де об'єднуються кіберзасоби, психологічні методи й алгоритмічна інженерія. На відміну від традиційної війни, вона діє не відкрито, а приховано, впливаючи на уми, а не на тіла. Тому держави, особливо в умовах глобального конфлікту (як-от війна рф проти України), повинні формувати власні інформаційні щити: розвивати стратегічні комунікації, інвестувати в медіаграмотність, підтримувати технічну кібербезпеку, формувати національну інформаційну стійкість.

3.3. Формування інформаційної стійкості як напряму протидії інформаційному тероризму

Інформаційний тероризм є однією із найнебезпечніших загроз сучасному демократичному устрою, оскільки спроможний підривати довіру до ключових політичних інституцій, делегітимізувати владу, викликати громадянське невдоволення та створювати умови для дестабілізації. Атаки на електоральні процеси, інформаційне маніпулювання громадською думкою, розповсюдження фейків і підрив моральної довіри до держави є типовими інструментами, які застосовуються для розбалансування політичної системи. У контексті гібридної війни це набуває особливої актуальності, адже інформаційний тероризм часто реалізується в комплексі з іншими формами впливу – економічним тиском, кібератаками, дипломатичними провокаціями.

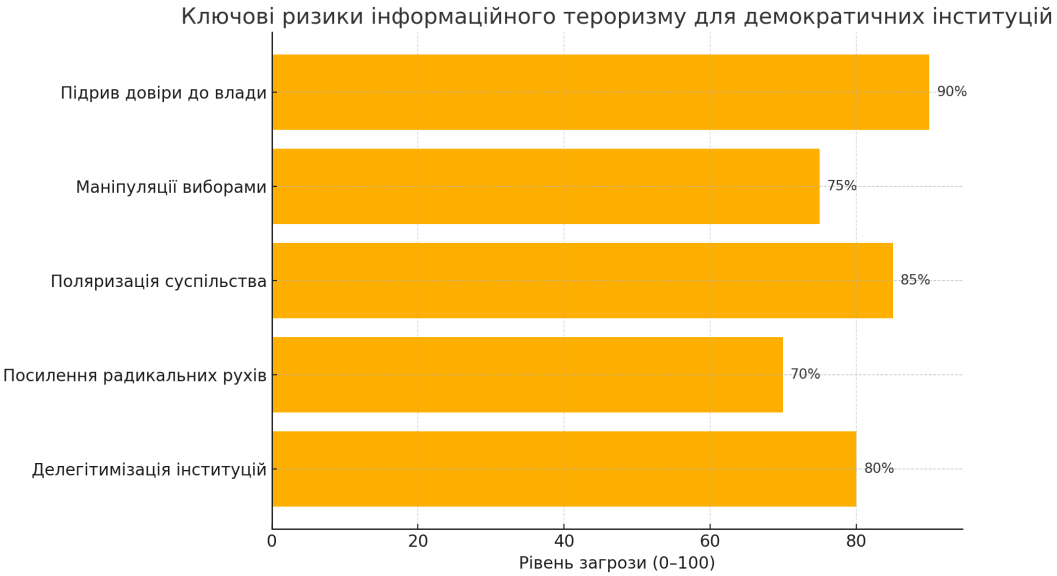


Рис 3.2. Вразливість національних інформаційних інфраструктур [363].

* Джерело: розробка здобувача.

Ключовими ризиками для демократій є поляризації суспільства, посилення радикальних рухів, зниження участі громадян у виборах через утрату віри в їх чесність, а також зростання впливу антидемократичних сил, які використовують інформаційний хаос для просування авторитарних

наративів (рис. 3.2). Особливо вразливими до такого впливу є країни з молодими демократіями, слабкою інформаційною гігієною й недостатнім рівнем цифрової медіаграмотності населення.

Ефективна протидія цим ризикам потребує комплексних підходів, що поєднують безпекові інструменти з розвитком стратегічних комунікацій, інституційної прозорості та підвищення інформаційної стійкості суспільства.Національні інформаційні інфраструктури (НІІ) охоплюють критичні цифрові платформи, мережі зв'язку, дата-центри, урядові інформаційні системи, банківські мережі, медіа, телекомунікаційні сервіси, системи електронного управління й інші канали обробки та передачі інформації. Їх уразливість стала однією з ключових загроз в епоху цифрової трансформації й гібридних конфліктів.

Основними чинниками вразливості є застаріла ІТ-інфраструктура в критичних секторах, зокрема в державному управлінні; відсутність належного аудиту кіберзагроз і неузгодженість стандартів безпеки між секторами; низький рівень підготовки персоналу, що працює з інформаційними системами, зокрема в муніципалітетах та органах місцевого самоврядування; критична залежність від закордонного програмного забезпечення й хмарних сервісів; відсутність законодавчо унормованої системи управління інформаційною безпекою, а також міжвідомчої координації.

Згідно з аналізом Європейського агентства з кібербезпеки (ENISA), 77 % держав-членів ЄС визнали свою критичну інфраструктуру недостатньо стійкою до інформаційних атак (2022 р.). Своєю чергою, звіти CERT-UA (2023 р.) засвідчують постійне зростання інцидентів, спрямованих проти енергетичних, фінансових і телекомунікаційних систем в Україні. Ці інциденти часто мають комплексний характер – поєднують кіберзлочинність, фішинг, вірусні атаки та цілеспрямовані інформаційно-психологічні операції. Уразливість НІІ робить державу мішенню як для державних акторів (наприклад російської федерації, яка активно здійснює кібердиверсії в Україні

з 2014 р.), так і для недержавних суб'єктів – кіберугруповань, що працюють в інтересах третіх країн або з ідеологічних міркувань.

Отже, захист національних інформаційних інфраструктур потребує цілісної політики цифрової стійкості, що ґрунтується на законодавчому забезпеченні, міжнародній співпраці, регулярних аудиторських перевірках, інвестиціях у кіберграмотність та адаптації найкращих практик з кіберзахисту (наприклад NIST, ISO/IEC 27001). Без цього будь-яка стратегія протидії інформаційному тероризму залишатиметься незавершеною.

Окремо треба відзначити концептуальну вагомість праці «Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз: національна доповідь» [154] для розвитку наукового дискурсу у сфері національної стійкості в межах політичних наук. У цьому дослідженні представлено оригінальне бачення проблематики, яке акцентує увагу на необхідності стратегічного підходу до формування національної стійкості в умовах глобалізації, постійного зовнішнього тиску й внутрішніх дестабілізаційних чинників. Важливо, що автори не обмежуються констатацією наявних загроз, а прагнуть виробити конкретні практичні рекомендації для зміцнення інституційної спроможності держави. Концептуальна цінність цього документа полягає в критичному переосмисленні традиційних моделей забезпечення стійкості та напрацюванні нових стратегічних підходів до реагування на актуальні виклики сучасного політичного середовища. Особливу увагу приділено аналізу так званих гібридних загроз, які вже стали системною складовою частиною поточної геополітичної реальності. Ідеться про складне поєднання класичних і нетрадиційних форм впливу – від інформаційних операцій і кібератак до економічного тиску й підриву суспільної стабільності. У цьому контексті формування науково обґрунтованих стратегій запобігання та ефективного реагування на зазначені загрози набуває ключового значення для зміцнення національної безпеки [430].

Потрібно також відзначити фундаментальну вагу дослідження О. Рєзнікової «Національна стійкість в умовах мінливого безпекового середовища» [193], яке зробило суттєвий внесок у формування сучасного уявлення про національну стійкість і її роль у забезпеченні безпеки України. У цій роботі авторка пропонує цілісний, багатовимірний підхід до осмислення та конструювання стратегій, що дають змогу державі адекватно реагувати на нові виклики безпекового середовища, зокрема гібридні загрози й трансформації міжнародного політичного ландшафту.

Рєзнікова аргументовано наголошує на необхідності інтеграції політичних, економічних, соціальних і технологічних компонентів стійкості як передумови для забезпечення життєздатності державних інститутів та адаптації до умов невизначеності. Такий підхід дає змогу формувати стійку модель державного розвитку, спроможну не лише реагувати на ризики, але й ефективно функціонувати в умовах тривалого тиску й багатофакторних загроз.

У сучасних умовах гібридної війни та інформаційної конфронтації дедалі більшого значення набуває концепт інформаційної стійкості, який розглядається як ключова складова частина національної безпеки й соціальної згуртованості. Під інформаційною стійкістю зазвичай розуміють спроможність держави, інституцій і громадянського суспільства протистояти зовнішнім та внутрішнім інформаційним загрозам, уключаючи дезінформацію, маніпуляції, пропаганду й інші форми інформаційного впливу, що мають на меті дестабілізувати політичне, соціальне або культурне середовище.

Інформаційна стійкість є комплексним міждисциплінарним феноменом, який уключає технічні, організаційні, нормативно-правові, освітні та психологічні складники. Зокрема, вона охоплює такі аспекти, як:

– інституційна спроможність держави забезпечувати кібербезпеку й контроль за інформаційним середовищем;

– рівень медіаграмотності населення та його здатність до критичного мислення;

– ефективність стратегічних комунікацій, спрямованих на посилення довіри до демократичних інституцій;

– інклюзивна державна політика щодо інформаційної безпеки, спрямована на захист прав людини й свободи слова.

Особливе значення інформаційна стійкість має в контексті протидії інформаційним операціям іноземних держав, що можуть впливати на демократичні процеси, створювати соціальну напругу, підривати легітимність влади та дезорієнтувати громадянське суспільство. Отже, вона є важливою передумовою національного суверенітету в умовах цифрової епохи.

У науковому дискурсі інформаційну стійкість також розглядають у зв'язку з такими поняттями, як інформаційна безпека, стратегічні комунікації, національна стійкість і громадська довіра, що дає змогу комплексно оцінювати ефективність державної політики у сфері інформаційного захисту. Методи боротьби з інформацією в електронних медіа основані на комплексному підході, поєднуючи технічні, організаційні, правові, політико-дипломатичні, економічні й гуманітарні методи протидії, уключаючи побудову єдиної загальнодержавної системи протидії кіберзлочинності, що повинна забезпечити захист критичної інфраструктури.

Ефективна протидія інформаційному тероризму та стабільної інформаціної стійкості потребує узгоджених дій на трьох взаємопов'язаних рівнях – державної інформаційної політики, підвищення рівня громадянської обізнаності та забезпечення технологічної стійкості. У цьому процесі визначальну роль відіграють стратегічні комунікації, розвиток медіаграмотності й цифрова безпека, які разом формують основу національної та міжнародної інформаційної стійкості.

Концепція стратегічних комунікацій набуває особливої значущості в контексті міжнародної безпеки, де її розглядають як інструмент впливу на інших суб'єктів стратегічної взаємодії через застосування комплексу інформаційних операцій, таких як радіоелектронна боротьба, кібервпливи, операції з дезінформації та військове введення в оману із метою досягнення

стратегічної переваги. В умовах динамічної трансформації світового безпекового середовища стратегічні комунікації відіграють ключову роль у формуванні чіткої стратегічної візії міжнародного актора, підвищенні його спроможності впливати на конфігурацію міжнародних мереж взаємодії, а також у реалізації національних інтересів через удосконалення наявних і створення нових каналів стратегічного партнерства [506].

Автори монографії [215] «Стратегічні комунікації ЄС: протидія деструктивним впливам» трактують стратегічні комунікації як скоординовану діяльність державних інституцій, спрямовану на формування й донесення цілісного, достовірного та переконливого наративу до цільових аудиторій. В умовах війни чи кризи вони забезпечують інформування, мобілізацію, згуртування суспільства й нівелювання паніки. Український досвід (наприклад кампанії «Армія. Мова. Віра», «Доброго вечора, ми з України», спростування фейків через Центр стратегічних комунікацій при МКІП) доводить ефективність державних наративів у протидії дезінформації.

У «Заключному звіті Оперативної групи Оборонної наукової ради зі стратегічних комунікацій» (Defense Science Board Task Force on Strategic Communication, 2004 р.), підготовленому за ініціативою Міністерства оборони США, стратегічні комунікації визначаються, як «фокусовані на політиці дії, пов’язані з інформаційною діяльністю, які повинні просувати інтереси країни шляхом обізнаного та координованого використання всіх доступних інформаційних ресурсів держави – дипломатичних, військових, економічних й інформаційних» [64]. Згідно з цим звітом, стратегічні комунікації охоплюють не лише публічну дипломатію, а й інформаційні операції, військову інформаційну підтримку, психологічні операції, внутрішню комунікацію в структурах оборони та координацію меседжів на міжвідомчому рівні. Їхня мета – забезпечити узгоджене формування й трансляцію наративів, що сприяють досягненню національних стратегічних цілей, впливають на ставлення та поведінку зовнішніх аудиторій і підтримують міжнародну легітимність дій держави. Цей підхід засвідчив перехід від фрагментованих

інформаційних кампаній до інтегрованої, стратегічно орієнтованої комунікаційної політики, яка розглядається як елемент національної безпеки.

Стратегічні комунікації активно застосовуються не лише державними акторами, а й радикальними та терористичними угрупованнями, які ефективно використовують їх для досягнення власних цілей в інформаційному просторі. Явище радикалізації, що призводить до проявів екстремізму й тероризму, хоча і не є новим, сьогодні набуває безпрецедентного розмаху в межах Європейського Союзу. Країни-члени ЄС стикаються з уніфікованими загрозами, зокрема пов'язаними з активним використанням інтернету та соціальних мереж терористичними структурами для пропаганди, вербування, дестабілізації суспільної злагоди й підриву засадничих демократичних цінностей [89].

У доповіді Високої групи експертів з питань радикалізації (2017 р.) наголошено, що терористична організація ІДІЛ систематично використовувала цифрові платформи для поширення інструкцій щодо здійснення терактів, їх героїзації, а також для навчання, ідеологічної обробки й залучення нових членів. Подібну тактику застосовують й інші терористичні та екстремістські групи, зокрема «Аль-Каїда», «Боко Харам» і різні представники праворадикального спектра, демонструючи високий рівень обізнаності з цифровими інструментами та комунікаційними технологіями [376].

21 березня 2022 р. Рада Європейського Союзу схвалила Стратегічний компас для безпеки та оборони, що визначає основні пріоритети й орієнтири зміцнення обороноздатності ЄС до 2030 р. [260]. Цей документ є відповіддю на нові виклики у сфері міжнародної безпеки та передбачає трансформацію Європейського Союзу в більш стійкого, автономного й спроможного діяти актора. У Стратегічному компасі виокремлено низку актуальних загроз, що дедалі більше ускладнюють європейське безпекове середовище:

– гібридна агресія з боку державних і недержавних суб'єктів**,** що включає кібератаки, кампанії з дезінформації, утручання у виборчі процеси,

економічний тиск та інструменталізацію міграційних потоків для досягнення політичних цілей;

– правова інструменталізація – свідоме викривлення норм міжнародного права задля реалізації політичних, економічних або військових інтересів, що викликає серйозне занепокоєння серед країн-членів ЄС;

– використання новітніх руйнівних технологій конкурентами ЄС як засобу посилення ефективності гібридних операцій і здобуття стратегічних переваг у міжнародному протистоянні;

– експлуатація інформаційного вакууму, що виник у період пандемії COVID-19, із метою поширення дезінформаційних і шкідливих наративів, спрямованих на підрив суспільної довіри та демократичних інституцій;

– зростання стратегічної конкуренції у сфері кібербезпеки, що супроводжується посиленням залежності від цифрових технологій, перетворює кіберпростір на арену глобального геополітичного суперництва;

– ускладнення характеру кібератак, яким усе частіше піддається інфраструктура Європейського Союзу, свідчить про потребу в підвищенні рівня кіберзахисту та розбудові цифрової стійкості як ключового елементу безпекової політики ЄС.

Отже, Стратегічний компас фіксує усвідомлення Європейським Союзом системної трансформації загроз і визначає курс на посилення власної спроможності протистояти гібридному тиску та забезпечувати стабільність на регіональному й глобальному рівнях.

Медіаосвіта та медіаграмотність – це фундамент для довготривалої інформаційної безпеки й високої інформаційної стійкості. Вони дають громадянам інструменти розпізнавання фейків, критичного мислення та оцінки джерел інформації. У країнах Балтії, Скандинавії й Україні запроваджено шкільні та університетські програми медіаграмотності, що довели свою ефективність під час хвиль інформаційних атак. Згідно з дослідженням IREX (2022 р.), учні з високим рівнем медіаграмотності на 60 % рідше вірять фейковим новинам [143].

Медіаграмотність, що охоплює спроможність критично осмислювати, інтерпретувати й раціонально використовувати інформацію, є однією з ключових компетентностей у сучасну добу інформаційної надмірності. Вона виявляється у вмінні відрізняти надійні джерела від маніпулятивних, розуміти контекст поданої інформації, цільові аудиторії медійних повідомлень, а також у здатності до усвідомленої комунікації в цифровому середовищі. Центральним компонентом медіаграмотності є критичне мислення – уміння системно аналізувати інформаційний контент, оцінювати його об’єктивність, точність і логічну послідовність, а також розпізнавати можливі викривлення, маніпуляції або навмисне емоційне забарвлення. Завдяки критичному мисленню користувачі спроможні відокремлювати факти від суб’єктивних суджень, розуміти приховані смисли й виявляти потенційні інформаційні впливи [144].

Із поширенням цифрових технологій поняття медіаграмотності значно розширилося та нині включає елементи цифрової грамотності. Це означає володіння навичками використання цифрових інструментів і платформ, а також спроможність розпізнавати й уникати кіберзагроз, таких як онлайн-шахрайство, фішинг, шкідливе програмне забезпечення чи інформаційні атаки. Отже, сучасна медіаграмотність передбачає не лише розуміння традиційних медіа, а й активну участь у безпечному та усвідомленому функціонуванні в цифровому комунікаційному просторі.

А. Шуляк і Н. Шуляк у монографії «Стратегічні комунікації та інформаційна гігієна: національна безпека в умовах глобальних викликів»[248] зазначають, що медіаграмотність є показником рівня освіченості й інформаційної зрілості суспільства. Особи, які володіють цією компетентністю, спроможні не лише брати активну участь у суспільному житті, а й критично осмислювати політичні, соціальні та економічні процеси, сприймати різноманітність поглядів й ухвалювати аргументовані, зважені рішення. Вона сприяє формуванню суспільства з розвиненим критичним мисленням, де громадяни можуть визначати власні ціннісні орієнтири та

підтримувати відкритий, толерантний діалог. Крім того, медіаграмотність має важливий вплив на психоемоційний стан особистості. Розуміння механізмів впливу медіа на емоції, світогляд і поведінку дає змогу споживачам інформації бути більш свідомими, стійкими до психологічного тиску та маніпуляцій. Спроможність ність розпізнавати маніпулятивні повідомлення й інтерпретувати їх з урахуванням контексту сприяє формуванню більш об'єктивного ставлення до дійсності та зменшує вразливість до стереотипів і спрощених інтерпретацій. У такий спосіб медіаграмотність виконує не лише освітню, а й соціальну та психологічну функції, зміцнюючи як індивідуальну, так і колективну інформаційну стійкість.

У 2022–2023 рр. у сферу медіаграмотності інтегровано новий важливий чинник – технології штучного інтелекту (ШІ), які істотно трансформують як виробництво, так і споживання інформації. У відповідь на ці виклики Європейська комісія представила перший у світі проєкт комплексної нормативно-правової бази щодо регулювання ШІ, який покликаний охопити потенційні ризики, пов'язані з його використанням, і закріпити лідерську позицію ЄС у цій сфері. Запропоноване у квітні 2021 р. законодавство про штучний інтелект (AI Act) передбачає запровадження чітких вимог і зобов'язань для розробників, операторів та користувачів систем ШІ з урахуванням ступеня ризику, пов'язаного з конкретним застосуванням технології. Він уключає положення про людський нагляд, прозорість, відповідальність і захист користувачів у випадках взаємодії з алгоритмами [188].

Паралельно з розвитком нормативного поля ЄС приділяє увагу просвітницькій та інформаційно-освітній діяльності. Зокрема, у 2024 р. за підтримки Європейського Союзу запущено спеціальний проєкт у межах «Всеохопної інформаційно-просвітницької кампанії з протидії дезінформації» [192], що передбачає аналіз досвіду найбільш медіаграмотних країн Європи. За підсумками проєкту, уже сьомий рік поспіль Фінляндію визнано (ще з 1990-х рр.) лідером за рівнем медіаграмотності, оскільки вона системно реалізовує

державну політику у сфері медіаосвіти) [209]. Її успіх зумовлений упровадженням медіаграмотності в шкільну освіту, міжсекторальною співпрацею держави, освітніх установ і медіа, а також широкою підтримкою критичного мислення як складової частини громадянської компетентності. Отже, взаємозв'язок між регулюванням цифрових технологій і розвитком медіаграмотності в політиці ЄС формує комплексну відповідь на нові виклики, пов'язані з інформаційною безпекою й етикою в епоху штучного інтелекту.

Також у концепцію поняття інформаційної стійкості входить визначення інформаційної гігієни – взаємодія між людьми та інформаційними технологіями, а також методи й засоби гарантування безпеки, збереження та оптимізації роботи з інформацією в цифровому середовищі, запобігання негативним наслідкам від користування інформаційними технологіями, зокрема захистом від шкідливих впливів інформаційного середовища на здоров'я людини, психологічним комфортом, забезпеченням конфіденційності та безпеки особистих даних в інтернеті, збереженням інформаційної етики тощо [247].

Цифрова безпека включає набір інституційних і технологічних заходів, які захищають індивідуальні, корпоративні та державні інформаційні системи і є важливою складовою частиною інформаційної стійкості. Ідеться про впровадження протоколів шифрування, систем багатофакторної аутентифікації, резервного копіювання, кібергігієни, реагування на інциденти. У 2023 р. понад 90 % атак на українські ІТ-системи відбито завдяки зусиллям CERT-UA і міжнародного обміну даними про загрози (зокрема з країнами НАТО).

З огляду на зростання складності сучасних гібридних загроз, Європейський Союз активно розширює й удосконалює арсенал інструментів протидії, спрямованих на забезпечення ефективної реакції, стійкості та солідарності в межах об'днання. Зокрема, до ключових елементів цієї стратегії належать:

1. Гібридний інструментарій ЄС (EU Hybrid Toolbox) – комплекс заходів, що забезпечує скоординовану відповідь на гібридні кампанії, спрямовані проти ЄС і його держав-членів. Уключає превентивні, стабілізаційні, обмежувальні та відновлювальні механізми, а також сприяє підвищенню рівня солідарності й взаємодопомоги між країнами-членами. Ефективне застосування цього інструментарію передбачає посилення спроможності ЄС до виявлення, ідентифікації та аналізу джерел і форм гібридної агресії;

2. Гібридні команди швидкого реагування ЄС (EU Hybrid Rapid Response Teams) – спеціалізовані багатосекторальні формування, які мобілізують національний, цивільний і військовий досвід для підтримки держав-членів, місій Спільної політики безпеки й оборони (CSDP), а також країн-партнерів у протидії гібридним загрозам;

3. Інструменти кібердипломатії ЄС (EU Cyber Diplomacy Toolbox) – нормативно-політичний механізм, який передбачає превентивні заходи, політичну реакцію та санкції проти зовнішніх суб'єктів, відповідальних за зловмисну кібердіяльність, що загрожує безпеці Союзу і його держав-членів;

4. Інструментарій ЄС для протидії зовнішньому інформаційному впливу та втручанню (EU Toolbox to Address and Counter Foreign Information Manipulation and Interference) – комплекс заходів, спрямованих на виявлення, аналіз і нейтралізацію кампаній з дезінформації, зокрема з боку російської федерації в контексті її збройної агресії проти України. Особливу увагу приділено встановленню відповідальності за інформаційні маніпуляції, покладанню витрат на винуватців та посиленню суспільної стійкості шляхом забезпечення доступу до достовірної інформації, підтримки вільних і незалежних медіа в усьому ЄС.

Усі зазначені вище інструменти відображають прагнення Європейського Союзу до формування цілісної й багатовимірної відповіді на гібридні виклики сучасності з урахуванням їх міжгалузевого та транснаціонального характеру [260].

Синергія трьох напрямів формує систему превентивної протидії інформаційному тероризму, де громадяни, держава та технічна інфраструктура виступають єдиним фронтом у боротьбі за безпечне інформаційне середовище. Їх розвиток є не лише національним, а й глобальним пріоритетом у XXI ст.

Для протистояння загрозам кібертероризму виокремлюють низку основних напрямів боротьби, як-от: уніфікація та гармонізація національного законодавства й міжнародних актів; проведення наукових розробок у сфері формування сучасних технологій виявлення та запобігання кримінальним і терористичним впливам на інформаційні ресурси; створення спеціалізованих підрозділів у сфері боротьби з комп'ютерними злочинами й комп'ютерним тероризмом; удосконалення міжнародної організаційно-правової взаємодії з питань протидії комп'ютерній злочинності та комп'ютерному тероризму; удосконалення багаторівневої системи підготовки кадрів у сфері інформаційної безпеки.

Інститут інформаційного омбудсмена відіграє суттєву роль у формуванні й підтримці інформаційної стійкості держави. Як гарант дотримання інформаційних прав громадян, омбудсмен сприяє зміцненню довіри суспільства до державних інституцій, забезпечуючи прозорість, підзвітність і захист від інформаційних зловживань. Саме через моніторинг порушень інформаційних прав, розгляд скарг, ініціювання нормативних змін та інформування населення про безпечну поведінку в цифровому середовищі омбудсмен формує основу для підвищення критичного мислення та інформаційної грамотності громадян. Своєю чергою, це підвищує спроможність суспільства протистояти дезінформації, кіберзагрозам й іншим інструментам інформаційної агресії. Отже, інформаційний омбудсмен є інституційною ланкою, що поєднує захист цифрових прав із розвитком колективного імунітету до інформаційних впливів, тобто сприяє посиленню національної інформаційної стійкості.

Інформаційний омбудсмен – посадова особа, на яку покладаються функції контролю за дотриманням законних прав та інтересів громадян на доступ до інформації. Уперше таку посаду заснував риксдаг Швеції 1809 р., відповідно до прийнятої того року конституції. Довгий час вона не була поширена в інших правових системах, окрім шведської. Проте з часом такий пост за шведським зразком запровадили в інших країнах Північної Європи – у Фінляндії (1919 р.), Норвегії (1952 р.), Данії (1953 р.). Першою неєвропейською державою, яка запровадила посаду омбутсмена, стала Нова Зеландія (1962 р.). Ідея заснування інституту уповноваженого з прав людини знайшла своє втілення вже в понад 120 країнах світу.

Інформаційний комісар має набір мінімальних повноважень: право видавати обов'язкові приписи для запобігання або усунень порушень права на доступ, отримувати доступ до інформації, у тому числі з обмеженим доступом, тощо. Інституція Інформаційного комісара нині існує в багатьох державах. У таких країнах, як Великобританія, Португалія, Угорщина, Туреччина, Словенія, успішно діють комісари або комісії з питань інформації. Головне їхнє завдання – розгляд скарг та реагування на них. Причому в більшості країн рішення інформаційного комісара є обов'язковими для виконання [217]. Щоб забезпечити реалізацію закону про доступ до інформації та створити дієвий, оперативний і незалежний механізм оскарження відмов у наданні інформації, у Бельгії, Ісландії, Польщі, Таїланді, Естонії, Японії та деяких інших країнах на підставі законів, що визначають порядок доступу до інформації, у рамках виконавчої влади створено спеціальний орган контролю за забезпеченням права на доступ до інформації [156].

Форми діяльності інформаційного омбудсмена – це або спеціальний орган контролю за забезпеченням права на доступ до інформації в рамках виконавчої влади, або посада спеціалізованого омбудсмана з питань інформації, або колегіальний орган, що здійснюватиме незалежний парламентський контроль за охороною й захистом права на доступ до інформації, або спеціальний представник зі здійснення контролю за забезпеченням конституційного права

на інформацію в межах апарату уповноваженого з прав людини, або орган контролю, який формально створюється при уряді, парламенті, але до його складу входять представники законодавчої, виконавчої, судової гілок влади, представники від громадськості та місцевого самоврядування.

До повноважень інформаційного омбудсмена входять: 1) розгляд скарг; 2) нагляд за реалізацією Закону про доступ до інформації та інших законів про обробку інформації; 3) унесення пропозицій, що сприяють реалізації права на доступ до суспільно значущої інформації; 4) пропозиція органам влади низки заходів, спрямованих на покращення їхньої роботи у сфері доступу до інформації; 5) проведення моніторингів щодо додержання Закону; 6) забезпечення ведення Реєстру із захисту інформації; 7) розробка щорічних доповідей про стан додержання й захисту права на доступ до інформації та права на приватність; 8) здійснення нагляду за дотриманням органами державної влади закону під час визначення режиму доступу до інформації; 9) проведення для держслужбовців семінарів, тренінгів, інших заходів із метою правильного тлумачення й застосування останніми законів, що регулюють доступ до інформації [147]. Його рішення повинні мати обов'язковий характер, але можуть бути оскаржені до Вищого адміністративного суду. Спеціалізований уповноважений із питань інформації обирається парламентом із рекомендованих громадськими організаціями кандидатів.

У контексті введення інституту інформаційного комісара, інформаційна безпека розглядається, як мінімізація шкоди через неповноту, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації [202].

У контексті забезпечення права на доступ до публічної інформації в Україні дедалі актуальнішою стає ідея створення спеціалізованого органу – інформаційного комісара, який би виконував функції незалежного арбітра в справах порушення інформаційних прав громадян. Така ініціатива відповідає рекомендаціям Ради Європи щодо формування інституційної моделі,

спроможної забезпечити оперативний, неупереджений і позасудовий розгляд скарг, що стосуються порушення права на доступ до інформації. В Україні термін «інформаційний омбудсмен» офіційно не вживається як окремий посадовець чи інститут. Наразі ці функції в Україні виконує Уповноважений Верховної Ради з прав людини. Це і є найближчий аналог ролі омбудсмана з питань інформації. Однак обмеженість його повноважень і ресурсів унеможливлює ефективне реагування на велику кількість звернень (до 11 000 на рік), що ставить під сумнів дієвість наявної моделі. Особливого значення набуває дискусія про перспективу розширення повноважень омбудсмана з метою тимчасового виконання ним функцій інформаційного комісара, зокрема через запровадження механізмів примусового виконання приписів, делегування повноважень із фіксації правопорушень та активної участі у формуванні нормативно-правової бази у сфері доступу до інформації. Передбачено також посилення відповідальності розпорядників інформації за порушення законодавства, як за неправомірну відмову, так і за надання недостовірної чи неповної інформації.

Інформаційний омбудсмен повинен визначати орієнтири інформаційної демократії й контролювати їх, займатися формуванням інформаційної політики держави з певного питання, бути самостійною фігурою в уряді. У нього не може бути власної політичної ніші, щоб не доводилося конкурувати за владу та сфери впливу з іншими вищими посадовими особами.

Інформаційний комісар – це окрема незалежна інституція, яка займатиметься захистом прав громадян, журналістів і громадських активістів у справах із доступу до інформації. Він виконуватиме дві важливі функції: забезпечення реалізації прав на доступ до публічної інформації та захист персональних даних. Під час подання запиту на отримання публічної інформації чи відмови розпорядника її надавати (порушуючи таким чином ЗУ «Про доступ до публічної інформації») саме до інформаційного комісара потрібно звертатися. Працівники Секретаріату проводять детальне розслідування, установлюють, чи правомірно розпорядник відмовив у наданні

інформації, якщо ні – складають щодо порушника адміністративний протокол, який дасть змогу притягнути до суду чиновника, котрий порушив закон, а скаржникові надсилають детальну відповідь із роз'ясненням по суті [82].

Запровадження інформаційного комісара як незалежного органу сприятиме інституційному зміцненню інформаційної стійкості держави, оскільки ефективний доступ до публічної інформації є ключовим чинником формування прозорого управління, підзвітності влади й суспільної довіри. В умовах гібридної війни це також є важливим елементом протидії інформаційним загрозам, зокрема дезінформації, маніпуляціям та спробам делегітимізації демократичних інституцій. Формалізація такого органу на рівні Конституції потребує значних політико-правових зусиль, однак є вагомим кроком у напрямі адаптації українського інформаційного законодавства до європейських стандартів, зміцнення інформаційної безпеки й посилення спроможності держави протистояти викликам цифрової доби [81].

Захист даних – одне з основних прав, захищених європейським законодавством і закріплених у ст. 8 Хартії основних прав Європейського Союзу, що ґрунтується на захисті та пропагуванні конфіденційності приватних осіб і захисті даних у повсякденній роботі. Правила захисту даних (Регламент (ЄС) 2018/1725), що застосовуються до установ, органів й агенцій ЄС (EUI), відповідають положенням Загального регламенту захисту даних (Регламент (ЄС) 2016/679) [11], що застосовується до всіх держав-членів Союзу. Європейський інспектор із захисту даних (European Data Protection Supervisor, EDPS) [348] – незалежний орган Європейського Союзу із захисту даних. Посаду запровадили 2001 р. в межах Договору про заснування Європейської спільноти. Він повинен забезпечувати право громадян на таємницю приватних даних, якими оперують інституції й установи ЄС.

Інспектора із захисту даних ЄС і його заступника призначають Європейський парламент і Рада ЄС строком на п'ять років із можливістю продовження мандата. Основна мета їхньої діяльності полягає в гарантуванні

захисту персональних даних і забезпеченні конфіденційності під час обробки особистої інформації установами та органами Європейського Союзу.

До ключових функцій Інспектора належать:

– моніторинг і контроль дотримання стандартів захисту персональних даних під час їх обробки в структурах ЄС;

– надання консультативної допомоги інституціям ЄС – як на запит, так і з власної ініціативи – із питань, пов'язаних із персональними даними, уключаючи з оцінку законодавчих ініціатив, міжнародних договорів, а також імплементаційних і делегованих актів;

– аналіз впливу новітніх технологій на сферу захисту особистої інформації;

– участь у процесах Суду ЄС у ролі експерта для надання фахових висновків щодо тлумачення правових норм про захист даних;

– співпраця з національними органами нагляду за дотриманням законодавства про захист персональних даних із метою уніфікації практик на європейському рівні.

Ці функції здійснюються на основі принципів, закладених у Конвенції Ради Європи № 108 від 28 січня 1981 р., яка стала першою міжнародною угодою, що встановлює стандарти захисту персональних даних, а також Директиви 95/46/ЄС Європейського парламенту і Ради від 24 жовтня 1995 р. [566]. Згідно з цими документами, обробка персональних даних повинна відповідати таким вимогам:

– дані повинні збиратися й оброблятися чесно та законно;

– вони повинні зберігатися для чітко визначених і легітимних цілей та не використовуватись у спосіб, несумісний із цими цілями;

– обсяг оброблюваних даних повинен бути адекватним, релевантним і не надмірним щодо мети, для якої їх зібрано [308].

Актуальна правова база у сфері захисту персональних даних закріплена в Регламенті (ЄС) 2018/1725 Європейського парламенту і Ради від 23 жовтня 2018 р. Він регулює обробку персональних даних інституціями, органами,

службами й агентствами ЄС і встановлює правові рамки для вільного переміщення таких даних. Документ набув чинності 11 грудня 2018 р. після офіційної публікації в Офіційному віснику ЄС.

Рішення Бюро Європейського парламенту від 17 червня 2019 р. встановлює порядок реалізації положень Регламенту (ЄС) 2018/1725, який замінив попередні акти – Регламент (ЄС) № 45/2001 і Рішення № 1247/2002/ЄС [99]. Цей Регламент визначає загальні принципи захисту персональних даних, які обробляються інституціями, органами, службами й агентствами ЄС, а також регламентує вільний обіг таких даних у межах Союзу.

Європейський наглядовий орган із захисту даних (EDPS) функціонує на підставі Регламенту 2018/1725 [566], який, своєю чергою, ґрунтується на статті 16 Договору про функціонування Європейського Союзу (TFEU). Його основні завдання викладено в статті 57, а повноваження – у статті 58 зазначеного Регламенту. Документ окреслює правила, обов'язки та інституційну незалежність наглядового органу, передбачені в розділі VI. За порушення вимог Регламенту може бути накладено штраф у розмірі до 10 млн євро або до 2 % річного світового обороту підприємства, залежно від того, яка сума є більшою.

Із метою мінімізації ризиків компанії зобов'язані впроваджувати превентивні заходи, що забезпечують дотримання норм регулювання обробки персональних даних.

На сьогодні в європейському правовому полі діє понад 100 міжнародних документів (конвенцій, протоколів, директив, рекомендацій), які безпосередньо або опосередковано стосуються правового регулювання у сфері захисту персональних даних. Водночас низка системних проблем залишається невирішеною як у нормативному, так і в практичному аспектах:

– більшість баз персональних даних функціонують без автономності, що суперечить міжнародним стандартам;

– відсутній ефективний механізм організаційно-правового забезпечення транскордонної передачі даних;

– персональні дані активно використовуються в бізнесі як ресурс у цифровому середовищі;

– незаконна торгівля персональними даними (у тому числі через CD-носії) є поширеною практикою на ринках;

– функціонує нелегальна інфраструктура збирання й продажу адресних баз даних.

У цьому контексті EDPS є незалежним і впливовим регуляторним органом, діяльність якого забезпечується головою (Supervisor) та секретаріатом, що складається з висококваліфікованих юристів, фахівців з IT й адміністративного персоналу. Орган відіграє ключову роль у забезпеченні законності, прозорості та захищеності обробки персональної інформації в межах Європейського Союзу.

Згідно з чинними правилами захисту даних, EUI несуть повну відповідальність за спосіб обробки персональних даних, тому обов'язкова вимога – щоб усі EUI призначили Уповноваженого із захисту персональних даних Європейського парламенту (DPO) [324], який відповідає за моніторинг застосування Регламенту в інституції, незалежно забезпечує правильне застосування Комісією закону про захист персональних даних фізичних осіб і веде публічний реєстр усіх операцій, що здійснюються Комісією з персональними даними. Будь-яка служба, інституція зобов'язана повідомляти DPO про всі операції, під час яких обробляються персональні дані (збір, консультації, пересилання, організація тощо). Його завдання полягає в тому, щоб незалежно забезпечити дотримання установою законодавства про захист даних і прав, свобод особи/громадянина. Він призначається Європейським наглядовим органом із захисту даних. Застосовуючи відповідні правила захисту даних, EDPS затвердив своє Рішення про внутрішні правила щодо обмежень певних прав суб'єктів даних стосовно обробки персональних даних у межах діяльності, яку виконує EDPS, а також імплементаційні правила щодо Уповноваженого із захисту даних (Рішення EDPS від 11 грудня 2018 р.) [74].

Система вимірювання інформаційної стійкості повинна спиратися на міждисциплінарний підхід, що поєднує політичну науку, соціальну психологію, комунікативістику та кібербезпеку.

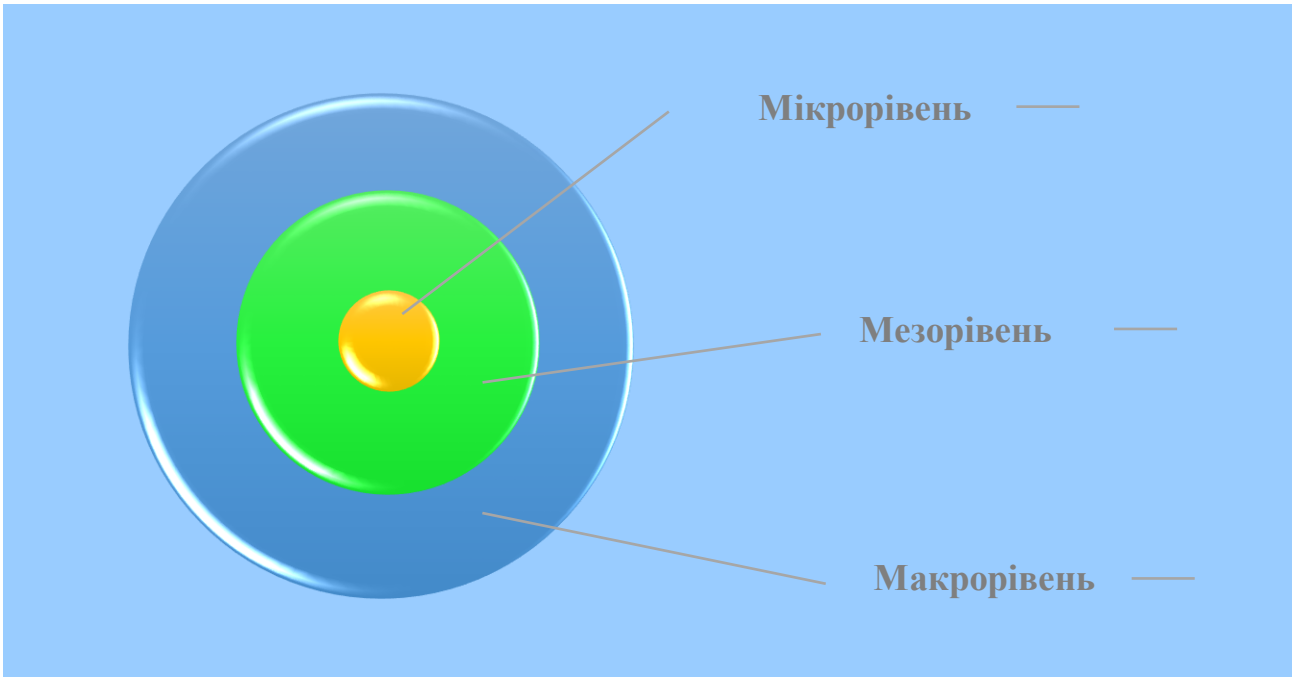


Рис. 3.3. *Триєдина модель вимірювання інформаційної стійкості**

* Джерело: розробка здобувача.

В основі – триєдина модель, яка охоплює (рис. 3.3, табл. 3.3):

мікрорівень – індивідуальні когнітивні та поведінкові реакції громадян (медіаграмотність, спроможність критично сприймати інформацію, емоційна саморегуляція);

мезорівень – діяльність інституцій, медіа, громадських організацій та освітніх закладів у сфері протидії дезінформації, розвитку цифрової компетентності та медіаосвіти;

макрорівень – політична, правова й стратегічна спроможність держави забезпечувати стабільність інформаційного простору, нейтралізувати зовнішні інформаційні атаки та підтримувати суспільну довіру до інституцій.

Така модель дає змогу не лише описати, а й кількісно оцінити рівень інформаційної стійкості суспільства, визначивши її динаміку під впливом

зовнішніх і внутрішніх чинників. Зокрема, можна застосовувати порівняльний метод для аналізу відмінностей у рівнях стійкості різних країн, що зазнають інформаційної агресії.

Таблиця 3.3

Триєдина модель інформаційної стійкості*

Рівень	Опис	Об'єкт вимірювання
1	2	3
Мікрорівень (індивідуальний)	Критичне мислення, медіаграмотність, цифрова компетентність громадян	Людина як споживач і творець інформації
Мезорівень (інституційний)	Ефективність медіа, освітніх, наукових, громадських інституцій у формуванні медіаосвіти та цифрової культури	Організації, громади, освітні заклади
Макрорівень (державний / системний)	Здатність держави забезпечувати інформаційну безпеку, протидію дезінформації та підтримку довіри до інституцій.	Національний інформаційний простір

* Джерело: розробка здобувача.

Для побудови операційної системи оцінювання інформаційної стійкості запропоновано комплекс кількісних і якісних індикаторів, згрупованих за чотирма основними категоріями (табл. 3.4):

1. Когнітивна стійкість (КС) – рівень медіаграмотності, уміння розпізнавати маніпуляції, розвиток критичного мислення. Індикатори: частка громадян, спроможних самостійно ідентифікувати фейкові повідомлення; середній бал критичного аналізу новин; частота довіри до перевірених джерел;

2. Цифрова компетентність (ЦК) – технічна спроможність користувачів забезпечувати власну кібербезпеку, знання основ кібергігієни, навички роботи з цифровими платформами. Індикатори – кількість

користувачів, що застосовують двофакторну автентифікацію; рівень дотримання правил кіберзахисту; індекс цифрової культури;

3. Інституційна довіра (ІД) – оцінка рівня суспільної довіри до національних ЗМІ, органів влади, експертного середовища та міжнародних партнерів. Індикатори – показник довіри до офіційних каналів комунікації; ступінь прозорості державних повідомлень; активність інституцій у протидії дезінформації;

4. Інформаційна стабільність (ІС) – спроможність держави та суспільства знижувати вплив деструктивних інформаційних кампаній і швидко відновлювати баланс після криз. Індикатори – тривалість та інтенсивність інформаційних криз; кількість нейтралізованих фейкових кампаній; швидкість відновлення довіри до джерел після інформаційних атак.

Таблиця 3.4

Система індикаторів інформаційної стійкості держави*

Категорія	Індикатор	Метод оцінювання	Шкала
1	2	3	4
Когнітивна стійкість (КС)	Рівень медіаграмотності, критичне мислення	Соціологічні опитування, тестування	0–1
Цифрова компетентність (ЦК)	Навички кібергігієни, виявлення фейків	Практичні завдання, аудит безпеки	0–1
Інституційна довіра (ІД)	Довіра до держави, медіа, експертного середовища	опитування, аналіз комунікацій	0–1
Інформаційна стабільність (ІС)	Тривалість криз, здатність до відновлення	OSINT-моніторинг, аналіз інцидентів	0–1

* Джерело: розробка здобувача.

Кожен індикатор може бути оцінений за стандартизованою шкалою (від 0 до 1), що дає змогу формувати композитний індекс інформаційної стійкості (ІСІС). Методологічно застосовано трирівневу модель (мікро/мезо/макро) та чотири категорії індикаторів: когнітивна стійкість, цифрова компетентність,

інституційна довіра, інформаційна стабільність. Композитний індекс ІСІС обчислюється як середнє цих чотирьох компонентів (нормування 0-1).

Для інтегрального вимірювання рівня інформаційної стійкості пропонується формула:

$$ІСІС=0.25КС+0.25ЦК+0.25ІД+0.25ІС,$$

де:

КС – когнітивна стійкість;

ЦК – цифрова компетентність;

ІД – інституційна довіра;

ІС – інформаційна стабільність.

Отримані результати можуть бути інтерпретовані за чотирибальною шкалою:

0,8–1,0 – висока інформаційна стійкість (стратегічна стабільність);

0,6–0,79 – середня (керована стабільність);

0,4–0,59 – низька (зона ризику);

нижче 0,4 – критично вразливий стан (загроза деструктивного впливу).

Отже, ІСІС може бути використаний як аналітичний інструмент державного моніторингу у сфері інформаційної безпеки, а також як порівняльний показник під час аналізу інформаційної стійкості різних країн у межах систем колективної безпеки (ЄС, НАТО, ООН).

Запропонована система оцінювання інформаційної стійкості має прикладне значення для формування державної політики протидії інформаційному тероризму. Вона дає змогу визначати слабкі місця в структурі національного інформаційного простору, прогнозувати потенційні загрози та коригувати стратегії стратегічних комунікацій. Для України така модель є особливо актуальною в контексті триваючої російської гібридної агресії, коли інформаційні атаки поєднуються з воєнними, економічними та дипломатичними впливами.

Вимірювання інформаційної стійкості стає також важливим чинником у розробленні концепції інформаційної безпеки ЄС і НАТО, де поняття

«resilience» є фундаментальною складовою частиною колективної оборони. Саме порівняльний аналіз рівня стійкості різних країн дає змогу оцінити ефективність міждержавних механізмів протидії дезінформації, інформаційному тероризму й гібридним загрозам.

Отже, інформаційна стійкість є системним показником зрілості держави у сфері інформаційної безпеки. Її вимірювання уможливлює поєднання когнітивного, інституційного й політичного рівнів аналізу, забезпечуючи наукове підґрунтя для розроблення ефективних стратегій захисту від інформаційного тероризму. Формування національної моделі вимірювання інформаційної стійкості, адаптованої до українського безпекового контексту, має стати одним із ключових напрямів сучасних досліджень у галузі політичної науки та міжнародних відносин. Розуміючи важливість права на доступ до інформації в демократичному суспільстві й ураховуючи євроінтеграційний курс України, що передбачає імплементацію міжнародних стандартів, зокрема у сфері прав людини, убачаємо за доцільне створити окремий інститут Інформаційного комісара. Створення інституту Інформаційного комісара, який би максимально відповідав міжнародним стандартам, потребує закріплення його статусу на конституційному рівні, оскільки для ефективного здійснення контролю за вказаним правом такий орган повинен бути незалежним від гілок влади.

ВИСНОВКИ ДО РОЗДІЛУ 3

У контексті трансформації сучасного безпекового середовища війна перестала бути лише збройним протистоянням між регулярними арміями. Вона набула комплексного, багатовимірного характеру, що інтегрує воєнні дії з політичними, інформаційними, кібернетичними та психологічними засобами впливу.

Концепція війни четвертого покоління (4GW), сформульована В. Ліндом, окреслює децентралізацію насильства, залучення недержавних

акторів і стирання меж між військовими та цивільними сферами. Паралельно феномен проксі-війни слугує інструментом для досягнення геополітичних цілей через делеговані конфлікти, мінімізуючи пряме залучення держав. Інформаційна війна (iWar), згідно з підходом НАТО, становить нову якість агресії, де головним об'єктом є не фізична інфраструктура, а людська свідомість. У цьому контексті медіавійна функціонує як підсистема iWar, що спрямована на формування викривленої реальності, делегітимацію інституцій та дестабілізацію суспільства.

Асиметричні конфлікти, які виникають за умов значної диспропорції сил, ґрунтуються на використанні тероризму, саботажу й інформаційного впливу. Усі ці форми війни синтезуються в гібридну модель, у якій інформаційна компонента відіграє ключову роль. Агресія російської федерації проти України є показовим прикладом гібридного сценарію із залученням проксі-структур, кібероперацій і масованих кампаній дезінформації.

Отже, війни нового покоління репрезентують зсув від фізичного протиборства до боротьби за когнітивне домінування. Це потребує нових стратегічних підходів до забезпечення національної та міжнародної безпеки, заснованих на поєднанні воєнних, інформаційних, кібернетичних і дипломатичних інструментів. Інформаційна зброя в умовах гібридної війни стала одним із головних засобів впливу, що потребує цілісної політики протидії, розвитку інформаційної стійкості й стратегічних комунікацій.

Противагою інформаційній зброї може стати інформаційна стійкість – це ключ до протидії інформаційному тероризму, що підриває довіру до держави, провокує розкол у суспільстві та дестабілізує демократію. Ефективна відповідь потребує поєднання стратегічних комунікацій, кіберзахисту, медіаграмотності й правових механізмів. Особливу роль відіграють незалежні інституції, зокрема інформаційний комісар, який сприяє захисту інформаційних прав. Успішні приклади ЄС засвідчують, що тільки комплексний підхід забезпечує спроможність держави та суспільства чинити опір сучасним гібридним загрозам.

РОЗДІЛ 4
ПОРІВНЯЛЬНИЙ АНАЛІЗ НАЦІОНАЛЬНИХ СТРАТЕГІЙ ПРОТИДІЇ ІНФОРМАЦІЙНОМУ ТЕРОРИЗМУ

4.1. Нормативно-інституційні засади забезпечення інформаційної безпеки та кіберстійкості в США і ЄС

XXI століття – ера інформаційних технологій. Свобода доступу до інформації та швидкість її поширення, підвищення конкурентоспроможності економіки й розширення можливостей інтеграції у світову систему господарства, підвищення ефективності державного керування – усі ці переваги надає нам користування інформаційно-комунікативними технологіями. Світ стає більш залежним від сучасних технологій. Соціальні медіа та транзакції через інтернет відіграють ключову роль у тому, як більшість організацій ведуть бізнес і спілкуються з потенційними клієнтами сьогодні. Утім, зі всіма перевагами глобалізація у сфері інформаційних технологій підвищує ризик зловживань, крадіжок та шахрайства. Світ стає вразливішим до кібератак. Ефективність інформаційної безпеки будь-якої держави насамперед залежить від досконалості нормативно-правового регулювання діяльності інформаційної системи державних і громадських органів.

Початкові стратегії кібербезпеки з’явилися на початку минулого десятиліття. Однією з перших держав, які прийняли кібербезпеку як проблему державного рівня, були Сполучені Штати, де Стратегія національної безпеки в кіберпросторі була опублікована ще у 2003 р. Після цього такі документи й плани безпеки у віртуальному просторі поширилися по всій Європі. Наприклад, у 2005 р. Німеччина прийняла Державний план захисту інформаційної інфраструктури; у 2006 р. у Швеції розроблено стратегію посилення безпеки інтернету; 2008 р. Естонія опублікувала широку державну стратегію з кібербезпеки. Тоді ж подібні стратегії створюються у Фінляндії та

Словаччині. Перелік усіх національних стратегій кібербезпеки Європейського Союзу та деяких інших країн, що не є членами, опублікований Європейським агентством безпеки мережі та інформації. Задля розробки нової стратегії об'єднання щодо кіберзлочинності в лютому 2013 р. Європейська комісія запропонувала директиву про заходи щодо забезпечення високого рівня мережевої та інформаційної безпеки (NIS) у всьому Союзі. Через взаємозв'язок мереж й інформаційних систем значні збої в одній державі можуть торкнутись інших держав-членів та ЄС загалом.

Події 11 вересня 2001 р. в США спричинили трансформацію уявлень як про національну безпеку в цілому, так і про інформаційну безпеку як її ключову складову частину. Зокрема, відбулося формування нової парадигми національної безпеки США, яка ґрунтується на усвідомленні повної залежності національної інфраструктури від інформаційних систем та мереж країни. При цьому під кібернетичним тероризмом у штатах сьогодні розуміють «навмисне руйнування, переривання чи перекручування даних у цифровій формі або потоків інформації, що має широкомасштабні негативні політичні, релігійні чи ідеологічні наслідки» [428].

Законодавство США у сфері зовнішньої інформаційної безпеки включає сукупність федеральних законів, законів штатів і нормативних актів, які разом становлять правову основу для утворення й здійснення державної політики у сфері інформаційної безпеки. Законодавство штатів різниться одне від одного, оскільки нормативні акти окремих штатів є досить відмінними. Розглядаючи положення законодавства США в інформаційній сфері, зазначимо, що вони, з одного боку, спрямовані на забезпечення права громадян на інформацію та конфіденційність їхнього приватного життя, а з іншого – на зовнішню інформаційну безпеку. Це свідчить про збалансованість у законодавствах інтересів особи, суспільства й держави.

У лютому 2003 р. в Сполучених Штатах Америки розроблено «Національну стратегію захисту кіберпростору» [535], у якій визначено комплексний підхід до захисту життєво важливих комунікаційних технологій

американської нації. Стратегію розроблено за допомогою кваліфікованих у темі інформаційної безпеки спеціалістів.

«Національна стратегія захисту кіберпростору США» спрямована на захист складних і взаємопов'язаних інформаційних систем, які мають життєво важливе значення для сучасного інформаційного суспільства. Загальна мета цього документа – виокремити організаційні завдання й пріоритетність зусиль задля їх досягнення; визначити напрями та кроки, які повинні зробити як урядові структури, так і підприємства й приватні користувачі для досягнення безпеки кібернетичного простору США [272]. Визначено основне завдання у сфері кібернетичної безпеки: «запобігання кібернетичним нападам на критичну інфраструктуру, зниження вразливості нації до таких нападів і мінімізацію збитків та часу відновлення».

29 травня 2009 р. оприлюднено «Огляд з кібербезпеки» (Cyber Security Review), що мав на меті «виробити стратегічну основу кіберініціатив Уряду США» [315]. У цьому Огляді до ключових завдань керівництва США у сфері кібербезпеки віднесено забезпечення центральної ролі Білого дому у формуванні кібербезпекової політики, аби продемонструвати аудиторії як усередині США, так і міжнародним партнерам серйозність намірів американського керівництва у сфері кібербезпеки; перегляд законодавства та політики у сфері кібербезпеки; посилення федерального законодавства й відповідальності у сфері кібербезпеки; просування інформаційних проєктів державного, регіонального та локального рівнів. Крім того, у цьому документі окреслено ключові завдання, спрямовані на посилення кібербезпеки США, а саме: підвищити готовність суспільства до кіберзагроз; посилити кібербезпекову освіту, збільшити кількість федеральних працівників із підготовкою у сфері інформаційних технологій; просувати кібербезпеку як важливий елемент відповідальності урядів усіх рівнів.

На початку березня 2010 р. президентом США затверджено чергову «Ініціативу зі всеосяжної національної кібербезпеки» Ради національної безпеки США [527], що складається з дванадцяти загальних положень,

реалізація яких дасть змогу захистити країну й уряд від кібератак та хакерів. Ця ініціатива є складовою частиною розділу Воєнної доктрини США, що стосується кібернетичної оборони. Документом передбачено створення єдиної федеральної мережі, пов'язаної захищеними каналами зв'язку. Зв'язок цієї захищеної мережі має здійснюватися через контрольовані точки доступу. Окрім того, Ініціатива передбачає об'єднання всіх шести наявних у США центрів оперативного реагування на кіберзлочини з метою підвищення ефективності їхньої діяльності та проведення більш глибокого аналізу хакерських атак. Також із метою протидії іноземним кібершпигунам документом передбачено створення підрозділів кіберконтррозвідки, яка поширить свій вплив на всі державні органи США, захист таємних внутрішніх мереж Міноборони США від терористичних атак.

Стратегія кібербезпеки США 2011 р. [402], запропонована президентом Б. Обамою, передбачає право Америки вживати заходи у відповідь на ворожі дії в кіберпросторі, розглядаючи їх як будь-які інші загрози. Тобто хакерські атаки прирівняні керівництвом Сполучених Штатів до оголошення війни. У кінці квітня 2012 р. Сенат США прийняв Закон CISPA («Cyber Intelliggence Sharring and Protection Act») [313], який дав змогу Уряду, приватним агентствам безпеки та будь-яким приватним компаніям за наявності підозр про вчинення кіберзлочину отримати доступ до конфіденційної інформації користувачів і комерційних організацій.

Кількість кібератак зростає з кожним роком. Лише в період із 2006 по 2015 р. цифра збільшилася з 5503 до 77 183. У 2017 р. близько 143 млн американців постраждали внаслідок кібератак. Потерпілі становлять більшість американського дорослого населення, яке користується інтернетом. Близько восьми із десяти людей (77 %) зазнали шкоди через кіберзлочин. У результаті кібератак американські споживачі, які стали жертвами кіберзлочинності, утратили близько 19,4 млрд дол. США, що в середньому становить 96 дол. США на одну жертву. Майже 20 год (19,8) американці витрачають на боротьбу з наслідками кіберзлочину [467]. Незважаючи на

кібератаки, населення, зазвичай, продовжує довіряти установам, які впорядковують дані та особисту інформацію в мережі «Інтернет». Проте, за даними 2017 р., близько 53 % споживачів утратили довіру до свого уряду [467].

Американці прагнуть до цифрової грамотності й бажання її покращити виходить далеко за рамки молодого покоління. Понад вісім із десяти опитаних людей сказали, що хочуть поліпшити свої знання й уміння в цій сфері. Загальні мотиватори для бажання покращити навички цифрової грамотності включають заощадження грошей, інформування й підтримку друзів та сім'ї. Поліпшення професійних навичок і безпека інтернету також є пріоритетами для міленіалів. Кожен із чотирьох 18–34-річних людей відзначає використання професійного програмного забезпечення як зону, яку вони найбільше прагнуть розвинути, і 24 % тієї самої вікової групи хотіли навчитися безпечно користуватись інтернетом [330].

Кіберстратегія США 2018 р. визначає п'ять основних напрямів діяльності з питань захисту: 1) постійний моніторинг і безперервна оцінка загроз і вразливих місць державних інформаційних систем; 2) здійснення національних заходів зі зменшення загроз та вразливості кіберпростору; 3) уживання заходів щодо захисту інформаційних систем органів влади; 4) забезпечення якісної освіти й навчання з питань захисту кіберпростору; 5) співробітництво з питань національної безпеки та безпеки міжнародного кіберпростору [455]. Сполучені Штати Америки активно борються з кіберзлочинністю, намагаються запобігти новим атакам і допомагають населенню впоратися з наслідками. У ході дослідження виявлено такі чинники, що сприяли проведенню успішної інформаційної політики США: ефективне нормативно-правове регулювання; розгалуження державних органів; інтенсифікація кіберстрахування; інформованість та довіра населення.

Нормативно-правове регулювання – чи не найголовніший двигун ефективності забезпечення інформаційної безпеки будь-якої держави.

Американський уряд значну увагу приділяв питанням забезпечення безпеки інформації в державних комп'ютерних системах (закони США «Про комп'ютерну безпеку» та «Про удосконалення інформаційної безпеки»), протидії комп'ютерній злочинності (закони «Про комп'ютерне шахрайство та зловживання» і «Про зловживання комп'ютерами»), регулювання співвідношення прав громадян на отримання інформації (закони «Про свободу інформації» та «Про висвітлення діяльності уряду») й конфіденційності їхнього приватного життя (закон «Про охорону персональних даних»).

Важливим аспектом правового регулювання інформаційної безпеки США є забезпечення конфіденційності приватного життя громадян. Особливу роль у регулюванні цього питання відіграє Закон США «Про охорону персональних даних», який прийнято в 1974 р.

Державні структури відіграють важливу роль у забезпеченні інформаційної безпеки. Структура інформаційної безпеки в США є доволі розгалуженою та включає в себе значну кількість компонентів, на кожен із яких покладено відповідні завдання й функції з урахуванням їхньої компетенції. Згідно з законом США «Про національну безпеку» від 1947 р., головною відповідальною особою із питань забезпечення національної безпеки загалом та інформаційної безпеки зокрема є Президент США. Він приймає найважливіші рішення із питань національної безпеки країни.

Політика інформаційної безпеки в багатьох аспектах залежить від вибраного курсу людини при владі. Так, для прикладу, адміністрація Б. Обами приділяла багато уваги питанням кібербезпеки, виділивши при цьому значні ресурси для боротьби з кібератаками. У бюджеті США на 2016 фінансовий рік кібербезпеку закладено пріоритетом діяльності адміністрації, виділено 14 млн доларів США для того, щоб подолати нагальні загрози кібератак [537]. За вирішення окремих питань щодо забезпечення національної безпеки відповідають держсекретар і міністр оборони. Правоохоронні органи США відіграють важливу роль у досягненні цілей кібербезпеки, за допомогою розслідування широкого кола кіберзлочинів – від крадіжки та шахрайства до

затримання й переслідування відповідальних осіб. Департамент внутрішньої безпеки (DHS) співпрацює з іншими федеральними установами для проведення кримінальних розслідувань для знешкодження кіберзлочинців, а також займається підготовкою технічних експертів, розробленням стандартизованих методів і нових інструментів протидії кіберзлочинності. Секретна служба США підтримує цільові групи, які зосереджені на виявленні та пошуку міжнародних кіберзлочинців, пов'язаних із кібератаками, банківським шахрайством й іншими комп'ютерними злочинами. Відділ кіберрозвідки Секретної служби безпосередньо сприяє арештам транснаціональних кіберзлочинців, відповідальних за крадіжку сотень мільйонів номерів кредитних карт і втрату близько 600 млн дол США фінансовими й роздрібними установами. Секретна служба також керує Національним комп'ютерним криміналістичним інститутом, який надає працівникам правоохоронних органів, прокурорам і суддям кіберпідготовку та інформацію для боротьби з кіберзлочинністю. Центр імміграції та митного контролю США (ICE), що включає дослідження національної безпеки (HSI) і Центр кіберзлочинності (C3), надає комп'ютерні технічні послуги для підтримки внутрішніх та міжнародних розслідувань транскордонних злочинів. Центр кіберзлочинності складається з підрозділу з боротьби з кіберзлочинністю, підрозділу з розслідування випадків експлуатації дітей і підрозділу комп'ютерно-технічної експертизи. У C3 також працює обладнана комп'ютерна лабораторія судово-медичної експертизи, яка спеціалізується на відновленні цифрових доказів та пропонує навчання у сфері комп'ютерно-дослідницької й криміналістичної майстерності [272].

Кіберстрахування – це страховий продукт, що використовується для захисту бізнесу й окремих користувачів від ризиків, пов'язаних з інтернетом і загалом ризиків, пов'язаних з інфраструктурою та діяльністю в галузі інформаційних технологій. Атаки на весь бізнес зростають. Малі підприємства схиляються до думки, що їх ця загроза омине, проте Symantec виявив, що понад 30 % випадків фішингу у 2015 р. простежено в організаціях із 250

працівників. Звіт Symantec про загрози інтернет-безпеці у 2016 р. засвідчив, що 43 % усіх атак у 2015 р. були спрямовані на малі підприємства [559]. Кіберстрахування не може повністю захистити організацію від кіберзлочинності, але це може втримати бізнес компанії на стабільній фінансовій основі, якщо відбудеться кібератака. 50 % американських фірм не мають страхування від кіберризиків і 27 % керівників США кажуть, що їхні компанії не планують узяти кіберстрахування, хоча 61 % із них очікують, що кількість кіберпорушенн збільшиться в наступному році [564]. Водночас можемо простежувати позитивну тенденцію за 2016 р.: за цей рік у США виробники заплатили за кіберстрахування 36,9 млн дол. США, що на 89 % більше, ніж роком раніше. Ключовими перевагами кіберстрахування є покриття витрат, починаючи від внутрішнього розслідування інциденту відділу інформаційних технологій і кроків, спрямованих на виправлення ситуації з утраченими доходами та заробітною платою. Страхові поліси зазвичай уключають покриття витрат на реабілітацію репутації компанії: компенсацію клієнтам, постраждалим від інциденту, а також оплату консультантів із кризового менеджменту для надання допомоги у відновленні бренду компанії [524], хоча треба зазначити, що послуги кіберстрахування тільки розвиваються.

Одним із визначальних документів цього періоду стала Національна стратегія кібербезпеки США [455], затверджена адміністрацією Дональда Трампа. У ній закріплено принципи «захисту за замовчуванням», превентивного реагування на кіберзагрози, а також концепцію «активного стримування» противників у кіберпросторі. США проголосили намір реалізовувати політику наступальної кібероборони, передбачаючи застосування превентивних кібердій у відповідь на зовнішню агресію в інформаційному просторі. Стратегія визначала росію, Китай, Іран та Північну Корею як головних кіберсуперників [521].

Подальше посилення інформаційної й кіберполітики відбулося в рамках Національної стратегії кібербезпеки США 2023 р. [456], оприлюдненої

адміністрацією Джо Байдена [349]. Документ уперше чітко артикулював необхідність перекладання відповідальності за кібербезпеку з індивідуальних користувачів на державу та великі цифрові компанії, які володіють або обслуговують критичну інфраструктуру. Водночас акцент зміщено на колективну стійкість (resilience), побудову партнерств між державними й приватними структурами, а також активізацію міжнародної співпраці для стримування держав, що використовують інформаційні технології в деструктивних цілях [520].

Період останніх десяти років ознаменувався також активним розвитком інституційної бази кібербезпеки. Роль центрального координатора в цій сфері виконує Агентство з кібербезпеки та безпеки інфраструктури США (CISA), створене у 2018 р. в складі Міністерства внутрішньої безпеки. CISA відповідає за моніторинг загроз, інформаційне попередження, взаємодію з критичним приватним сектором, розбудову кіберграмотності й захист виборчої інфраструктури. Водночас суттєво активізувалась діяльність Кіберкомандування США (USCYBERCOM), яке отримало повноваження проводити наступальні кібероперації в рамках стратегічного стримування та в умовах конфліктів нижче від порога війни.

Після масштабного зламу SolarWinds у 2020 р., який був приписаний російським спецслужбам, США почали впроваджувати нову архітектуру Zero Trust – концепцію, за якою жоден цифровий користувач чи пристрій не вважається довіреним за замовчуванням. Це передбачає багатофакторну автентифікацію, мікросегментацію мереж, постійний моніторинг доступу та обов’язкову перевірку кожної дії в мережі. Президентський указ № 14028 (2021 р.) ініціював реформу кібербезпеки у федеральному секторі, передбачаючи цифрову модернізацію, обов’язкове шифрування даних і розвиток систем раннього виявлення вторгнень [350].

Особливе місце в американській стратегії посідає боротьба з дезінформацією та інформаційними операціями, що становлять загрозу виборчим процесам і демократичним інститутам. У співпраці з платформами

соціальних медіа держава реалізує програми з верифікації контенту, підтримки незалежного фактчекінгу (наприклад First Draft, Snopes, PolitiFact), а також стимулює розвиток цифрової медіаграмотності серед громадян. У 2022 р. в межах CISA створено Робочу групу з боротьби з дезінформацією, що працює на основі принципів відкритості, етики та захисту свободи слова [416].

Отже, у ході дослідження виявлено чинники, які сприяли проведенню успішної інформаційної політики США. Серед них виокремлено нормативно-правове регулювання, вдалу політику державних органів й адміністрації президента, інформованість і довіру населення, кіберстрахування та міжнародну співпрацю. США має потужну законодавчу базу. Початок розвитку інформаційної безпеки закладено ще в першій половині XX ст. Проаналізовано п’ять основних напрямів діяльності з питань інформаційного захисту, які визначає Стратегія 2017: постійний моніторинг та безперервна оцінка загроз і вразливих місць державних інформаційних систем; реалізація національних заходів зі зменшення загроз та вразливості кіберпростору; здійснення заходів щодо захисту інформаційних систем органів влади; забезпечення якісної освіти й навчання з питань захисту кіберпростору; співробітництво з питань національної безпеки та безпеки міжнародного кіберпростору.

США перейшли від фрагментарного реагування на кіберзагрози до створення комплексної, превентивної та інтегрованої системи інформаційної безпеки. Основний акцент зроблено на зміцнення кіберстійкості держави, розвиток партнерства з приватним сектором, протидію дезінформації та формування міжнародних альянсів цифрової безпеки. Американський досвід демонструє, що кіберстійкість у XXI ст. потребує поєднання технологічних, інституційних і нормативних механізмів, спроможних ефективно реагувати на динамічне середовище інформаційних загроз. Водночас США продовжують будувати трансатлантичну архітектуру кіберстійкості в партнерстві з ЄС і НАТО. У межах альянсу реалізовуються спільні навчання з кіберзахисту (наприклад Locked Shields), розбудовуються обмінні механізми з CERT-

структурами, а також координуються санкції проти суб'єктів, відповідальних за кібератаки (уключаючи державні та недержавні актори).

Європейський Союз зобов'язується забезпечувати своїм громадянам життя в просторі свободи, безпеки й правосуддя без внутрішніх кордонів, де дотримуються спільні цінності, а права та свободи кожного гарантуються й охороняються. Проте загроза тероризму становить суттєву перешкоду для реалізації цих засадничих принципів. Саме тому у 2005 р. ухвалено «Стратегію ЄС із боротьби з тероризмом» [342], яка визначає такі пріоритетні напрями:

а) запобігання радикалізації та залученню осіб до терористичних угруповань;

б) захист громадян і критично важливої інфраструктури від терактів;

в) виявлення, переслідування й нейтралізація терористів, зокрема через обмеження їхньої мобільності, комунікацій і доступу до фінансових ресурсів;

г) забезпечення ефективного та скоординованого реагування на терористичні акти з метою мінімізації їх наслідків.

Політика Європейської комісії щодо кіберзлочинності реалізовується в чотирьох основних сферах. По-перше, це законотворчий процес. Найважливішим законодавчим рішенням є Рамкове рішення Ради міністрів ЄС щодо нападів на інформаційні системи від 17 січня 2005 р. Воно покликане забезпечити мінімальний рівень зближення кримінального законодавства щодо найпоширеніших форм злочинної діяльності стосовно інформаційної системи, такі як несанкціонований доступ, незаконне втручання в систему та дані.

Особливу увагу проблемі пропаганди тероризму була приділена у «Європейському порядку денному з безпеки» (2015 р.) [345], де наголошено на необхідності боротьби з першопричинами радикалізації шляхом упровадження превентивних заходів. Зокрема, ідеться про поширення спільних європейських цінностей – толерантності, культурного розмаїття, взаємоповаги – та підтримку відкритих, плюралістичних суспільств.

У 2015 р., з ініціативи єврокомісара з питань міграції, внутрішніх справ та громадянства Д. Аврамопулоса, у межах діяльності інтернет-форуму ЄС (заснованого у 2000 р.), впроваджено Програму підтримки громадянського суспільства (Civil Society Empowerment Programme). Її основна мета полягає в протидії поширенню терористичного контенту в цифровому середовищі. Європейська комісія констатує, що терористичні й екстремістські організації активно використовують новітні інформаційно-комунікаційні технології для ведення пропаганди, радикалізації аудиторії та вербування нових учасників. Попри обмежені технічні та фінансові ресурси, ефективність їхньої діяльності підвищується завдяки потужному потенціалу інтернету як каналу поширення деструктивних ідеологічних меседжів. Водночас цифровий простір може бути використаний для просування альтернативних наративів, що протистоять екстремістському впливу. У рамках Програми здійснюються навчання та підвищення кваліфікації представників громадянського суспільства й фахівців зі сфери соціальних медіа з метою формування спільних ініціатив, спрямованих на зниження ризиків радикалізації вразливих категорій населення. Такий підхід ґрунтується на усвідомленні важливої ролі громадянського суспільства в побудові стійкого до екстремізму інформаційного простору й превентивної комунікаційної стратегії в умовах зростання гібридних загроз [352].

Своєю чергою, статті 22–23 «Директиви з боротьби з тероризмом» (2017 р.) [331] зобов’язують держави-члени видаляти або блокувати онлайн-контент, що підбурює до вчинення терористичних актів. Водночас такі заходи повинні впроваджуватись у суворій відповідності до національного законодавства та Хартії основоположних прав ЄС, із дотриманням принципів пропорційності, законності та прав людини.

Стабільність мережевих й інформаційних систем, а також безперервність основних послуг є необхідними для належного функціонування внутрішнього ринку, зокрема для подальшого розвитку єдиного цифрового ринку ЄС. Ця директива вимагає, щоб усі держави-члени

створили «Комп'ютерні групи реагування на надзвичайні ситуації» (CERT), ухвалили національні стратегії та плани співробітництва з NIS. Як основне нововведення, запропонована директива вимагає обов'язкового повідомлення операторами ринку про інциденти, які мають значний вплив на безпеку ключових послуг [163]. CERT – це центр реагування на кібератаки. Команда реагування на інциденти у сфері інформаційної безпеки займається їх опрацюванням у межах власної організації або мережі. Її основні завдання – по-перше, запобігати кібератакам, підвищувати обізнаність користувачів, своєчасно виявляти загрози, відстежувати розвиток ситуації та забезпечувати ефективне усунення наслідків.

По-друге, Європейська комісія заохочує транскордонне співробітництво між правоохоронними органами держав-членів ЄС шляхом організації конференцій, створення цілодобових контактних пунктів у країнах-членах ЄС і розробки платформи для підготовки експертів у сфері протидії кіберзлочинності.

Найбільш резонансною була ситуація в Естонії. Кібератака проти неї є скоординованою одночасною атакою хакерів на комп'ютерні системи державних установ Естонії, яка розпочалася 27 квітня 2007 р. Під час загострення російсько-естонських відносин, пов'язаних із передачею пам'ятника Бронзовому солдату в Таллінні. Злагоджена атака на хакерів деякий час ламала вебсайти парламенту, міністерств, банківських установ та медіа. На думку багатьох спостерігачів й експертів, ця кібератака була однією з найкраще організованих та масових в історії інтернету. Події розгорталися трьома хвилями: перші напади зареєстровано 28 квітня, наступна, більш потужна хвиля – 4 травня, а найпотужніша третя хвиля – 9 травня 2007 р. Інтернет-трафік із-за кордону зріс у чотири рази, зробив атаковані сайти недоступними. Через атаки до 90 % банківських операцій в Естонії відчували труднощі з обробкою або не могли бути завершені нормально. На піку зловмисно створений трафік досягав 100 МБ/с. Для атак використано ресурси мережі Storm. Дещо пізніше, коли у квітні 2007 р. відбулися процеси проти

учасників заколоту, боти BlackEnergy були використані для атаки на вебсайт видання delfi.ee [92].

Із початком цієї кібервійни естонська сторона звинуватила росію в її організації, але згодом міністр оборони спростував ці звинувачення за відсутності доказів. У тому самому році депутат державної думи росії Сергій Марков на пресконференції зізнався, що один із його помічників усе ще займається організацією кібератак в Естонії. У 2007 р. лідер народного руху Придністров'я К. Голоскоков також визнав причетність цієї організації до вищезгаданих атак. У відповідь Естонія оголосила нон-гратою Сергія Маркова й лідера цього руху Василя Якименка. Оскільки Придністров'я залишається невизнаним, жодна країна світу не мала можливості притягнути кіберзловмисників із регіону до відповідальності [91].

Естонія зміцнила свій розвідувальний комітет після нападу 2007 р. Це включало запровадження організаційної структури, яка могла б швидко реагувати на напади на офіційні акти, що вимагають від усіх служб життєдіяльності підтримувати мінімальний рівень роботи, навіть якщо вони були відрізані від інтернету [343].

Естонія була однією з перших країн, яка розробила національну стратегію кібербезпеки у 2008 р., після чого опубліковано оновлену стратегію на 2014 р. У країні також є широкий спектр законодавства, що охоплює інформаційну безпеку та кібербезпеку. Сьогодні Естонія – найкраща країна з інформаційної безпеки в Європі. Вона має добре організовану комп'ютерну групу реагування на надзвичайні ситуації, CERT Estonia, яку очолює орган інформаційної системи. Крім національних органів влади, важливо також, щоб Центр кібербезпеки НАТО був в Естонії. Хоча офіційних державно-приватних партнерств немає, державні установи тісно співпрацюють із відповідними приватними організаціями [369].

Однією з найбільших кібератак була WannaCry (відома також як WCry, WCrypt, WannaCrypt, WNCRY і WanaCrypt0r) – комп'ютерний вірус, що вражає операційну систему Microsoft Windows шляхом шифрування файлів.

Вірус атакував уряди та бізнес із 12 травня 2017 р. Одним із перших атакували комп'ютери в Іспанії, пізніше вірус поширився на інші країни. Станом на 17 червня 2017 р. комп'ютери заражено в 150 країнах, їх кількість перевищила 500 000. Вимога переказувати гроші перекладена 28 мовами світу. Вірус атакував комп'ютери під керуванням Microsoft Windows через шифрування файлів користувачів, після чого відображав повідомлення про перетворення файлів із пропозицією протягом трьох днів сплатити ключ розшифровки в біткойнах в еквіваленті 300 дол. США для розблокування даних. Якщо необхідна сума не надійде, сума автоматично подвоїться, а на сьомий день вірус знищить дані. Повідомлення відображається мовою держави, де міститься ПК: у Великобританії – англійською, в Іспанії – іспанською. Розмір викупу скрізь однаковий. В Іспанії була заражена Telefónica, одна з найбільших телефонних компаній світу (четверта за кількістю абонентів). У Німеччині заражено комп'ютери Deutsche Bahn.

Імовірна втрата, понесена WannaCry протягом перших чотирьох днів, перевищила 1 млрд доларів США, ураховуючи масштаби великих організацій у всьому світі [73].

Спочатку відповідальною за цю хакерську атаку британське видання The Telegraph назвало групу Shadow Brokers, пов'язану з урядовими структурами росії. Однак у червні 2017 р. британський Національний центр кібербезпеки поклав відповідальність за напад на КНДР. У грудні того самого року уряд Сполучених Штатів опублікував власні висновки про те, що відповідальність покладено на угруповання «Лазарус» [557].

По-третє, Європейська комісія розвиває співпрацю між державним і приватним секторами в боротьбі з кіберзлочинністю, зокрема співпрацю між правоохоронними органами та приватними компаніями.

По-четверте, Європейська комісія заохочує підписання державами-членами й іншими країнами Конвенції про кіберзлочинність, розроблену Радою Європи, та бере участь у міжнародних робочих групах [306].

У межах боротьби Європейського Союзу з радикалізацією, екстремізмом і тероризмом реалізується стратегічний підхід, що ґрунтується на чотирьох взаємопов'язаних напрямах: запобігання, захист, переслідування та реагування. У документі Ради ЄС від 30 серпня 2019 р. стосовно протидії праворадикальному екстремізму й тероризму, визначено низку практичних рекомендацій для посилення зазначених напрямів [494]. Зокрема, Європейська комісія, за сприяння Радикалізації обізнаної мережі (RAN), повинна розробляти програми з протидії радикалізації з урахуванням локального контексту та сприяти обміну найкращими практиками між державами-членами. Наголошено на важливості підтримки досліджень причин радикалізації, зокрема аналізу переходу від агресивної онлайн-поведінки до офлайн-екстремізму, що є необхідною умовою для створення ефективних контрнаративів. У документі підкреслено потребу поглиблення співпраці між державами-членами й Європолом з метою виявлення проявів онлайн-екстремізму, а також просування європейських цінностей через механізми інклюзивної освіти відповідно до Рекомендацій Ради ЄС 2018 р. Технологічні компанії, своєю чергою, повинні бути обізнані про національні особливості проявів онлайн-екстремізму в різних країнах. Ключовим аспектом є налагодження тристоронньої взаємодії між Європейською комісією, державами-членами та цифровими платформами для виявлення й усунення екстремістських символів і контенту, а також для ефективної комунікації з правоохоронними органами й визначення вразливих аудиторій. Особливу увагу приділено протидії мові ненависті, контенту, що пропагує насильство, а також залученню традиційних медіа до інформування громадськості після терактів із метою запобігання соціальній поляризації. Окремо акцентовано на важливості обміну аналітичними матеріалами й кращими практиками з ключовими стратегічними партнерами ЄС – США, Канадою, Австралією та Новою Зеландією – у сфері протидії тероризму й екстремізму [334].

16 грудня 2020 р. Європейська комісія спільно з Верховним представником ЄС із закордонних справ і політики безпеки представили

оновлену Стратегію кібербезпеки ЄС, що має на меті зміцнення колективної стійкості Союзу до кіберзагроз, а також забезпечення безпеки та надійності цифрових послуг і технологічних рішень [485]. У рамках цієї ініціативи Комісія також запропонувала два ключові законодавчі акти: оновлену Директиву NIS2, яка передбачає заходи щодо досягнення високого спільного рівня кібербезпеки в усьому ЄС, розширює сферу охоплення та підвищує вимоги до управління ризиками; нову Директиву про стійкість критичних організацій, що спрямована на посилення здатності держав-членів захищати критичну інфраструктуру від фізичних і гібридних загроз, зокрема в енергетиці, охороні здоров'я, транспорті та цифрових послугах. Ці документи є частиною комплексного підходу ЄС до цифрової безпеки й формують нормативну базу для реагування на сучасні виклики у сфері кіберзахисту [354].

Зазначимо, що в останні роки різко зріс рівень кіберзлочинності в Німеччині. У 2015 р. в інформаційній системі Бундестагу виявлено кібератаку; серед іншого – пошкоджений комп'ютер федерального канцлера Німеччини Ангели Меркель. Відповідальність за напад покладено на дослідників російської групи кіберзлочинців, групи Sofacy, також відомої як «Буря ломбардів», яка, як вважається, пов'язана з російськими спецслужбами. Ця ж група намагалася зламати інформаційні системи Ради безпеки Нідерландів, щоб отримати доступ до інформації про розслідування випадку з рейсом MH17. А в травні 2016 р. зроблено спробу нападу на поштову систему Християнсько-демократичного союзу – політичної партії Ангели Меркель [302].

У 2016 р. кількість кримінальних правопорушень, скоєних за допомогою інтернет-технологій, становила 82 649 випадків, тоді як у 2015 р. поліція зареєструвала 45 793 кіберзлочинів. Водночас дані кримінальної статистики свідчать про зростання показників розкриття подібних злочинів. Загалом, кількість виявлених порушень цього типу зросла на 5,9 %, досягши рівня 38,7 %. Також наголошуємо, що у 2016 р. кількість злочинів у сфері комп'ютерної інформації (комп'ютерний саботаж) зросла на 25 % –

зареєстровано 4422 випадки. Рівень розкриття таких правопорушень знизився на 4,6 %, опустившись до 22,1 % [163].

Дослідники виявили новий тип шкідливого програмного забезпечення для Android, яке слугує для видобутку криптовалюти Monero. Робота цих програм під час видобування криптографії може пошкодити пристрій фізично. Справа в тому, що вірус Лоапі вимагає надання йому прав адміністратора. Після цього він починає самостійно завантажувати різні шкідливі модулі. Один із цих модулів використовує смартфон для отримання жетонів Monero. Саме ця функція може перегрівати пристрій через тривалу роботу процесора за максимального навантаження. Через два дні після зараження в тестовому смартфоні акумулятор виходив із ладу. Немає жодних ознак того, що шкідлива програма може бути розповсюджена через Google Play [164].

Представлений у 2024 р. в аналітиці DW [242] матеріал відображає зростаючу загрозу, яку становлять державні й недержавні актори з росії та Китаю для кібербезпеки ФРН, зокрема в контексті атак на критичну інфраструктуру. Згідно з даними Німецької асоціації цифрової індустрії Bitkom, кількість атак із росії у 2023 р. подвоїлася, а з Китаю – зросла на 50 %, що вказує на системний і цілеспрямований характер кіберагресії. При цьому 80 % постраждалих компаній стали жертвами саме російських атак, що свідчить про масштабність та координацію дій нападників. Федеральна влада Німеччини, зокрема МВС і Федеральне відомство кримінальної поліції (ВКА) підтвердили ці дані, зазначивши, що загальний збиток від кіберзлочинності у 2023 р. становив понад 205 млрд євро. Рівень розкриття кіберзлочинів залишається низьким (32 %), що частково зумовлено транснаціональним характером злочинів – понад 190 тис. випадків були скоєні іноземними акторами, а ще понад 134 тис. – у межах ФРН. Значну частину кібератак становлять кампанії із застосуванням шкідливого ПЗ, що часто спрямовані на стратегічно важливі об’єкти, зокрема енергетику й медичну сферу. Особливе занепокоєння викликає можливе поєднання кіберзлочинності з новими технологіями, насамперед зі штучним інтелектом, який може бути

використаний для автоматизації фішингових атак і масового шахрайства. Крім того, міністерка внутрішніх справ Ненсі Фезер указала на високий рівень латентності – 90 % кіберзлочинів не фіксуються офіційно, що створює викривлену картину безпеки в цифровому середовищі.

У глобальному вимірі, згідно зі Світовим індексом кіберзлочинності (WCI), Росія посіла перше місце серед держав – джерел кіберзагроз, випередивши Китай, США, Україну та Нігерію. Це підкреслює стратегічний характер кібероперацій, які дедалі частіше мають не лише економічні чи злочинні, а й політичні й воєнні цілі [118].

7 листопада 2016 р. у Фінляндії стало відомо про DDoS-атаку на інформаційні системи: управління опаленням і постачання теплої води у двох житлових будинках у Лаппеенранті на сході держави. Механізм захисту системи управління автоматично перезапустив її внаслідок сплеску трафіка, що зробило систему непрацездатною. Атака тривала з кінця жовтня до початку листопада 2016 р. [96].

Європейська стратегія безпечного інформаційного суспільства, прийнята у 2006 р., стосується боротьби зі злочинністю в інтернеті. Однак дії проти приватних та державних ІТ-систем у країнах-членах ЄС внесли новий відтінок у проблему, демонструючи, що злочинність в інтернеті є потенційно новою економічною, політичною та військовою зброєю. У цій сфері необхідна подальша робота з розробки комплексного європейського підходу, підвищення обізнаності й зміцнення міжнародного співробітництва. Найбільш розвиненими європейськими країнами у сфері інформаційної безпеки є Естонія, Франція та Норвегія, які прийняли низку законів і створили організації світового рівня для захисту країни в інформаційному просторі.

Із 2011 р. у Франції діє національна стратегія кібербезпеки, яка зосереджена переважно на питаннях оборони та національної безпеки. Національне агентство з безпеки інформаційних систем (ANSSI) – це добре організований орган, що спеціалізується на інформаційній безпеці й інтегрований із командою реагування на надзвичайні ситуації в країні, CERT-

FR. Стратегія кібербезпеки містить рекомендації щодо більш тісної співпраці з приватним сектором, але це не стало суттєвим досягненням. ANSSI опублікувала секретні заходи безпеки, які роблять Францію однією з небагатьох країн ЄС, яка прийняла такий цілеспрямований підхід до управління кібербезпекою [369]. У країні існує масштабне навчання з питань кібербезпеки. ANSSI опублікував список визнаних університетів, які надають акредитовані ступені з кібербезпеки.

Третє місце в Європі з найвищим показником нормативно-правового забезпечення посідає Норвегія. Окрім законів про кібербезпеку, інформацію, захист персональних даних та ін., розроблено Національну стратегію кібербезпеки (2012 р.), упроваджено національний центр кібербезпеки й Національну групу реагування на надзвичайні ситуації (NorCERT), що є частиною Норвезького органу безпеки (NSM). Вони справляються з важкими комп'ютерними атаками на критичну інфраструктуру та інформацію. Їхня місія – підвищити стійкість Норвегії в цифровій сфері. На міжнародному рівні це норвезький контактний центр із питань ІКТ-загроз й інцидентів у сфері кібербезпеки [261].

Європейський Союз проводить дуже активну політику у сфері інформаційної безпеки. На цей момент вона об'єднує високорозвинені країни, які мають величезний вплив на міжнародні відносини, установлюючи норми й стандарти поведінки держав у політичній, економічній, соціальній, інформаційній та інших сферах. Основною метою ЄС є посилення діалогу Європейської комісії з міжнародними організаціями й партнерами з питань безпеки мережі та, зокрема, щодо зростаючої залежності від електронних мереж. Політичні пріоритети у сфері інформаційної безпеки, визначені керівними органами Європейського Союзу, реалізуються на національному рівні як державними органами, так і неурядовими організаціями [306].

Тому для забезпечення інформаційної безпеки 10 березня 2004 р. створено Європейське агентство з безпеки та захисту інформації (ENISA), мета якого – зміцнення можливостей європейського співтовариства, держав-

членів та ділової спільноти у сфері профілактики й реагування на питання, пов’язані з інформаційною безпекою.

Основними напрямами діяльності Агентства є надання консультацій і допомоги Комісії та державам-членам у сфері інформаційної безпеки; збір й аналіз даних про інциденти безпеки в Європі, нові ризики; розробка методів оцінки ризиків для підвищення спроможності ЄС реагувати на загрози інформаційній безпеці; підвищення обізнаності та розвиток співробітництва між різними суб’єктами у сфері інформаційної безпеки, зокрема шляхом заохочення взаємодії між державним і приватним секторами [533].

Агентство також допомагає Європейській комісії в її попередній технічній роботі з оновлення та вдосконалення європейського законодавства щодо безпеки мережі й інформації [533]. У своїй діяльності ENISA спирається на щорічні плани / програми роботи, які містять перелік ключових пріоритетів, завдань, запланованих заходів для досягнення цілей.

Так, зокрема, у програмі роботи агентства визначені такі стратегічні пріоритети: підвищення здатності європейських електронних мереж протистояти зовнішньому впливу; розвиток співробітництва між державами-членами у сфері інформаційної безпеки; виявлення нових ризиків у сфері інформаційної безпеки та формування взаємної довіри між зацікавленими сторонами в реагуванні на нові ризики.

Починаючи зі створення Агенції ЄС із кібербезпеки, Європейський Союз пройшов суттєвий етап інституціонального становлення в цій сфері, сформувавши багаторівневу систему, що охоплює координацію дій, моніторинг кіберзагроз, підтримку наукових досліджень і розробок, а також реагування на кіберінциденти. Із 2022 р. ENISA у співпраці з Європейською службою зовнішніх дій (EEAS) розпочала активну діяльність у сферах, де гібридні загрози перетинають межі кібербезпеки та іноземного інформаційного втручання, зокрема в контексті маніпуляцій і дезінформаційних кампаній (Foreign Information Manipulation and Interference – FIMI). Особливу увагу приділено виявленню багаторівневих сценаріїв атак,

коли початковий вплив спрямований на один об’єкт або сектор, проте справжня мета полягає в завданні шкоди іншому. Наприклад, злам акаунта в соціальній мережі може мати на меті не лише шкоду його власнику, а й вплив на ширшу аудиторію підписників шляхом поширення дезінформації або деструктивного контенту. У зв’язку з цим 8 листопада 2022 р. оприлюднено спільний звіт ENISA та EEAS, у якому проаналізовано взаємодію між кіберінцидентами й інформаційними маніпуляціями, а також запропоновано підходи до координації зусиль у боротьбі з такими багатовимірними загрозами. Цей документ став важливим етапом у посиленні цілісного реагування ЄС на виклики, що поєднують цифрові та інформаційно-психологічні аспекти безпеки [360].

Можна зробити висновок, що в рамках ЄС інформаційна безпека розглядається, передусім, як стан інформаційних мереж і систем, що забезпечує належний рівень захисту цілісність, доступність, достовірність та конфіденційність інформації й належний рівень протидії зовнішнім негативним впливам. Пріоритетами політики ЄС у сфері інформаційної безпеки є створення та впровадження програм і різних технічних засобів захисту інформаційно-комунікаційних технологій; розробка нормативно-правових актів, що встановлюють перелік злочинів у сфері ІТ та кримінальну відповідальність; забезпечення високого рівня поінформованості громадськості про ризики, загрози й способи захисту своїх інформаційних систем / мереж від небажаних наслідків.

Відповідно до західного, зокрема демократичного, підходу до розвитку цифрового середовища, Європейський Союз формулює низку стратегічних пріоритетів, спрямованих на захист фундаментальних прав людини в кіберпросторі. Зокрема, ключовими цілями є протидія цензурі, масовому нагляду, порушенням права на приватність та використанню інформаційно-комунікаційних технологій для репресій проти громадянського суспільства й окремих громадян. У цьому контексті ЄС прагне зміцнити свою роль глобального лідера у сфері просування та захисту прав людини й

основоположних свобод в інтернеті, діючи на основі міжнародно-правових зобов'язань [88]. Зокрема, ідеться про дотримання Статуту ООН, Загальної декларації прав людини, а також інших міжнародних документів. Для реалізації цих принципів Європейський Союз активно впроваджує План дій із прав людини та демократії на 2020–2024 рр., ухвалений у листопаді 2020 р. Цей документ визначає практичні інструменти забезпечення цифрових прав і свобод, просування відкритого, вільного та безпечного інтернету, а також підтримки глобальних ініціатив, що ґрунтуються на універсальних цінностях демократії й верховенства права [341].

Якщо застосувати пропоновану нами формулу інформаційної стійкості стосовно США та держав ЄС (додаток Е), то отримаємо такі результати, як відображено в табл. 4.1.

Таблиця 4.1

Порівняння індикаторів інформаційної стійкості*

Країна/блок	КС	ЦК	ІД	ІС	ІСІС	Рівень
США	0,75	0,9	0,75	0,85	0,81	Висока
ЄС	0,7	0,85	0,75	0,8	0,77	Середня
Естонія	0,8	0,9	0,8	0,9	0,85	Висока
Німеччина	0,75	0,8	0,7	0,65	0,72	Середня
Франція	0,75	0,85	0,75	0,8	0,79	Середня
Норвегія	0,8	0,85	0,8	0,8	0,81	Висока
Фінляндія	0,75	0,8	0,75	0,7	0,75	Середня
Японія	0,75	0,85	0,8	0,75	0,79	Середня

* Джерело: розробка здобувача.

Аналізуючи дані, зазначимо, що США демонструють системно високий рівень інформаційної стійкості, що ґрунтується на поєднанні технологічної потужності, міжсекторальної взаємодії та розвиненої культури стратегічної безпеки. Інтегральний показник інформаційної стійкості (ІСІС) становить 0,81, що відповідає високому рівню. Когнітивна стійкість підтримується завдяки масштабним освітнім і просвітницьким програмам, спрямованим на підвищення цифрової грамотності населення. Близько 80 %

громадян усвідомлюють необхідність постійного навчання у сфері цифрових технологій, що створює міцне підґрунтя для формування критичного мислення й медіаосвіченості. Цифрова компетентність у США є однією з найвищих у світі. Вирішальну роль відіграють Агентство з кібер- та інфраструктурної безпеки (CISA), Кіберкомандування США (USCYBERCOM) і реалізація архітектури Zero Trust, закріпленої в президентському указі ЕО 14028. Ці ініціативи передбачають упровадження сучасних стандартів шифрування, багаторівневої автентифікації й сегментації мереж у всіх федеральних структурах. Інституційна довіра в американському суспільстві має певні коливання, спричинені політичними розбіжностями, однак механізми стримувань і противаг, відкритість державного управління та партнерство з приватним сектором забезпечують її стійкість. Інформаційна стабільність США виявляється в здатності держави швидко відновлювати інформаційні системи після кібератак, модернізувати нормативно-правову базу та підтримувати безперервність урядових комунікацій. У підсумку американська модель інформаційної безпеки має системно-інституційний характер і є орієнтиром для багатьох держав.

Інформаційна стійкість Європейського Союзу характеризується середнім інтегральним показником 0,78. ЄС сформував складну багаторівневу архітектуру колективної інформаційної безпеки, засновану на координації між державами-членами, європейськими агенціями та приватним сектором. Когнітивна стійкість підтримується завдяки розгалуженій системі освітніх і медіаосвітніх програм, діяльності мережі RAN (Radicalisation Awareness Network) та проєктів EU Internet Forum, спрямованих на розвиток критичного мислення й протидію радикалізації в онлайн-середовищі. Цифрова компетентність забезпечується роботою ENISA (Агентство ЄС із кібербезпеки) та нормативними актами NIS/NIS2, які встановлюють обов’язковість національних стратегій кібербезпеки, створення CERT/CSIRT, а також системи сповіщення про інциденти. Інституційна довіра ґрунтується на правових гарантіях Хартії основоположних прав ЄС і принципах прозорості

та пропорційності. Водночас нерівномірність розвитку між державами-членами залишається чинником, що знижує інтегральний рівень інформаційної стабільності блоку. Європейський Союз продемонстрував спроможність координувати дії під час криз, проте зберігає проблему неоднорідності імплементації політик. Його модель є прикладом багаторівневої, але фрагментованої системи колективної інформаційної стійкості.

Естонія вважається еталоном інформаційної стійкості в Європі. Після масштабних кібератак 2007 р. країна здійснила глибинну трансформацію національної системи кібербезпеки. Її ICIC становить 0,85 – найвищий серед аналізованих держав. Когнітивна стійкість естонського суспільства формується через системну цифрову освіту та залучення громадян до моніторингу безпеки.

Цифрова компетентність підтримується роботою CERT-Estonia й розміщенням Центру кібербезпеки НАТО в Таллінні. Інституційна довіра зберігається завдяки прозорості електронних урядових послуг, а інформаційна стабільність проявляється в здатності держави реагувати на загрози без утрати функціональності. Естонська модель поєднує технологічну зрілість, суспільну відповідальність і стратегічну далекоглядність, що робить її унікальним прикладом цифрової держави.

Рівень інформаційної стійкості Німеччини оцінюється в 0,73. Попри розвинену правову систему та високі стандарти кіберзахисту, держава стикається з проблемами, пов’язаними з частими кіберінцидентами. Когнітивна стійкість підтримується активною медіаосвітою, однак низький рівень розкриття кіберзлочинів (близько 32 %) свідчить про складнощі у сфері правозастосування. Інформаційна стабільність знижується через значні економічні збитки від атак (205 млрд євро у 2023 р.), що свідчить про високий рівень тиску на інформаційну інфраструктуру. Німецька модель потребує вдосконалення механізмів швидкого реагування та підвищення ефективності управління ризиками.

ICIC Франції становить 0,79, що межує з високим рівнем. Франція володіє потужною технічною базою кібербезпеки, представленою діяльністю ANSSI і CERT-FR, які координують роботу державних та приватних структур у сфері кіберзахисту. Когнітивна стійкість забезпечується інтеграцією цифрових навичок у систему освіти й розвитком науково-технічних компетенцій. Попри певну інерційність адміністративних процедур, французька модель вирізняється високим рівнем стратегічної координації та ефективним реагуванням на кібератаки.

Норвегія з ICIC 0,81 демонструє високий рівень зрілості у сфері інформаційної безпеки. Її модель ґрунтується на синергії технологічних інновацій, культури кіберосвіти та залученні громадян до забезпечення безпеки. Ключовими інституціями є NorCERT і Національне агентство безпеки (NSM). Високий рівень інституційної довіри та міжвідомчої координації створюють стабільну архітектуру реагування на інциденти, що робить Норвегію однією з найуспішніших держав у сфері кіберстійкості.

Фінляндія з показником 0,75 демонструє середній рівень стійкості. Сильна освітня система формує критичне мислення та цифрову компетентність населення, однак окремі інциденти, зокрема кібератаки на інфраструктуру опалення, свідчать про вразливість кіберфізичних систем. Фінська модель залишається демократичною, відкритою, проте потребує посилення технічного захисту критичних об’єктів.

Отже, у XXI ст. цифровізація стала основою глобальної взаємодії та управління, водночас спричинивши зростання кіберзагроз. Це потребує надійної інформаційної політики, що поєднує правове регулювання, ефективне управління, розвиток цифрової грамотності й інструменти кіберстрахування. США демонструють системний підхід до кібербезпеки завдяки стратегіям, інституційній інфраструктурі (CERT, DHS, C3), співпраці з бізнесом та увазі до захисту персональних даних. Країни Європейського Союзу забезпечують комплексну політику через директиви, діяльність ENISA, мережі CERT і міждержавну кооперацію, що ілюструється досвідом Естонії,

Франції та Норвегії. Ключовими чинниками ефективної інформаційної безпеки є чітке законодавство й стратегії кіберзахисту; координація державного, приватного, міжнародного секторів; цифрова обізнаність населення; спеціалізовані органи реагування; міжнародна співпраця. В умовах ескалації гібридних загроз забезпечення інформаційної безпеки стає стратегічним пріоритетом державної політики.

Порівняння інформаційної стійкості свідчить, що найвищі показники інформаційної стійкості мають США, Естонія та Норвегія – держави, які поєднують технологічне лідерство, розвинену культуру стратегічних комунікацій і правові гарантії безпеки. Європейський Союз та Франція демонструють високий середній рівень стійкості, проте їх неоднорідність знижує інтегральний бал. Німеччина й Фінляндія мають потужні інституційні системи, однак залишаються вразливими під час кризових інформаційних навантажень. Отже, інформаційна стійкість є інтегральним показником зрілості держави, який відображає ефективність її політичних, технологічних і комунікаційних інститутів. Високі значення ICIC корелюють із рівнем демократичності, прозорості та суспільної довіри, тоді як їх зниження сигналізує про потенційну вразливість до зовнішніх маніпуляцій та інформаційного тероризму.

4.2. Моделі державного інформаційного контролю: порівняльний аналіз практик Китаю, Японії та Індії

У XXI ст. інформація перетворилася на ключовий стратегічний ресурс, що визначає не лише технологічний розвиток, а й рівень національної безпеки. Японія як високотехнологічна держава з розвиненою демократією демонструє унікальний баланс між свободою слова, інформаційною прозорістю та контролем за інформаційними потоками в цифровому середовищі. В основу японської моделі інформаційного контролю покладено інтеграцію державного управління, корпоративної відповідальності та соціокультурних норм, що

забезпечує високий рівень інформаційної стійкості без прямого порушення прав людини. Японія претендує на одну з найрозвиненіших інформаційних країн світу, і для того щоб зберегти свою репутацію, їй потрібно забезпечити гідний рівень кібербезпеки. Коло груп, які зазнали кібератак (від окремих осіб й окремих сімей до складних підприємств соціальної інфраструктури), стрімко розширюється. Незважаючи на всі зусилля японського уряду, ризик інформаційного впливу зростає та впливає на такі сфери, як національна безпека, управління ризиками, конкурентоспроможність країни.

У Японії термін «інформаційне суспільство» вперше введено в 1960-х рр., а також увагу зосереджено на таких поняттях, як інформатизація, інформаційна індустрія, хоча норми інформаційного законодавства прийнято не відразу. До 1999 р. японське законодавство не могло регулювати нових інформаційних відносин щодо доступу, отримання та розповсюдження інформації, практично не було ухвалено жодних правових актів, які б своєчасно регулювали не тільки сферу застосування електронних носіїв інформації, а й також сферу інформації та телекомунікацій [368].

Із 1999 р. законодавство Японії в галузі інформації й телекомунікацій почало стрімко змінюватися, і сьогодні в країні вже є всі передумови для розгляду всебічної галузі інформаційного розвитку. Нині діє така нормативно-правова база, яка повністю регулює інформаційно-телекомунікаційну сферу та інформаційні відносини в межах:

– регулювання основ розвитку інформаційного суспільства Японії;

– регулювання телерадіомовлення;

– правове регулювання захисту користувачів телекомунікаційних послуг;

– регулювання мережевого зв’язку й процесу впровадження інформаційно-телекомунікаційних технологій;

– правове регулювання вмісту інтернету;

– регулювання порядку доступу, отримання, передачі й захисту інформації [356].

У Японії «право на доступ до інформації» (sirukenri) також означає «право людей знати», тобто право вільно отримувати та вимагати інформацію від органів виконавчої влади. Право на отримання інформації, що перебуває під юрисдикцією органів державної влади й органів місцевого самоврядування, прямо не передбачено Конституцією Японії (1947 р.), проте вона гарантує право на отримання (доступ) інформації (навіть за наявності всіх суперечностей) у статті 13, яка має розширене тлумачення і є основою японської концепції суспільного добробуту [397].

Конституційно-правова доктрина визначення гарантій інформаційних прав громадян та регулювання інформаційних відносин у Японії складається з таких джерел, як Конституція, міжнародні документи, нормативно-правові акти, судові прецеденти, тлумачення та професійні думки юристів, а також традиції, соціальні регулятори суспільства. Інформаційні права громадян уключають такі права, як право на доступ до інформації, а також право на конфіденційність особи, уключаючи право на захист особистої інформації.

Основу інформаційного регулювання Японії становлять Закони про захист персональних даних (2003 р., оновлений у 2020 і 2022 рр.) [263] та про доступ до публічної інформації (Act on Access to Information Held by Administrative Organs, 2001 р.) [262]. Вони забезпечують правові механізми контролю за використанням, поширенням і захистом інформації в державному й приватному секторах. Держава зобов’язана оприлюднювати суспільно значущу інформацію, тоді як обмеження накладаються лише у випадках загрози національній безпеці, громадському порядку або захисту персональних даних. Принципи регулювання ґрунтуються на концепції soft law, що відображає традиційну японську модель адміністративного управління – через рекомендації, настанови, консультації, а не через жорстке примусове законодавство. Це сприяє гнучкості інформаційного контролю, зберігаючи довіру між громадськістю й урядом.

Японія приділяє значну увагу кібербезпеці в контексті загроз із боку інших держав (зокрема КНР, КНДР, РФ). Закон про базові принципи

кібербезпеки (2014 р.), який встановлює базові політики Японії щодо кібербезпеки: відповідальність держави, місцевих органів влади, приватного сектору [523]. Із 2018 р. діє Кіберстратегія Японії, яка оновлюється кожні три роки. У версії 2021 р. особливо акцентовано на формуванні інформаційної стійкості, зміцненні захисту критичної інфраструктури, розвитку спільної відповідальності держави й бізнесу, забезпеченні «вільного, справедливого й безпечного кіберпростору», підвищенні соціально-економічної життєздатності, створенні безпечного суспільства для громадян [410]. Закон про активний кіберзахист (2025 р.) [412] дає державі право на більш активні заходи кібероборони.

У рамках Стратегії інформаційної безпеки можна виокремити чотири основні цілі – забезпечення вільного, безпечного обміну інформацією; підняття проблеми кібербезпеки на вищий рівень; оптимізація дій реагування, спрямованих на розв'язання цієї проблеми; розробка плану дій і зміцнення співпраці на основі принципів соціальної відповідальності. Стратегія також чітко визначає ролі всіх зацікавлених сторін (держави, інфраструктурних підприємств, комерційних організацій (науково-дослідних інститутів), окремих користувачів та компаній, що працюють через інтернет).

Серед ключових гравців й основних інститутів забезпечення інформаційної безпеки Японії є Національний центр готовності до інцидентів та стратегії кібербезпеки (NISC) [304] – центральний орган, що координує політику кібербезпеки держави; Міністерство економіки, торгівлі й промисловості (METI) – відповідає за кібербезпечність промислового / економічного сектору [443]; у приватному секторі є значна кількість компаній-постачальників рішень кібербезпеки (як японських, так і міжнародних), що працюють на японському ринку.

Японська модель передбачає впровадження принципів Zero Trust, постійний аудит цифрових систем, широке застосування шифрування й хмарних технологій із високим рівнем захисту. Водночас держава проводить тренінги для державних службовців, підприємців, громадян, спрямовані на

підвищення кіберграмотності та здатності розпізнавати інформаційні атаки [329].

Особливість Японії – глибоко вкорінена культура соціального консенсусу, ієрархії й корпоративної етики, що відіграє роль м'якого регулятора у сфері інформаційної політики. Такі норми, як giri (обов'язок) і wa (гармонія), сприяють формуванню внутрішньої самоцензури як із боку журналістів, так і користувачів медіа [496]. У Японії діє система неявної державної цензури, яка, з одного боку, сприяє дотриманню закону та журналістської етики, а з іншого – обмежує свободу інформації, оскільки її державне джерело контролює зміст повідомлення, яке надається журналісту (як частині пресклубу), а також зв'язок між офіційними джерелами (урядом, іншими органами влади, органами місцевого самоврядування, найбільшими комерційними організаціями, які є лідерами бізнесу) та медіа, які надають суспільству вже «відфільтровану» інформацію [406]. Така форма, незважаючи на багато спроб як японських, так і іноземних журналістів, що працюють у Японії, і громадянського суспільства, не може бути скасована жодним чином. Хоча японські медіа формально є незалежними, на практиці журналістика нерідко дотримується неофіційних обмежень, уникаючи жорсткої критики уряду в кризових ситуаціях [442]. Таке «узгоджене мовчання» стало предметом міжнародної критики після катастрофи на АЕС Фукусіма у 2011 р., коли частина інформації була тимчасово прихована через міркування національної безпеки та громадського порядку [476].

Для Японії проблема кібербезпеки нерозривно пов'язана з її роллю суверенної, незалежної держави. На початку 2000-их рр. вона посідає четверте місце за величиною експортного доходу у світі та є найскладнішою економікою з погляду Індексу економічної складності (ECI). У 2013 р. Токіо експортував товарів і послуг на 862,5 млрд доларів США, а імпортував товарів на 990 млрд доларів США, у результаті чого сальдо торгового балансу становило 127,5 млрд доларів США. У 2014 р. ВВП Японії становив 4,6 трильйона доларів США, а ВВП на душу населення перевищив 37 тис. доларів

США [406]. Станом на середину 2013 р. в державі було 100,7 млн користувачів інтернету, звідси його проникнення в домогосподарства до 2011 р. становило 86 % і продовжувало зростати. 99 % усього сегменту бізнесу Японії (із більш ніж 100 співробітниками) були підключені до інтернету. У 2012 р. країна посіла друге місце у світі за кількістю вебхостів (власників вебсайтів або сторінок в інтернеті) на території однієї держави.

Традиційно в Японії інформатизація всіх галузей економіки дуже висока. Крім того, вона займає високі місця за кількістю кіберінцидентів Так, у 2015 р. посіла 11 місце в списку країн світу серед джерел кібератак, 16-те – серед одержувачів кібератак. Водночас такі самі високі місця в усіх рейтингах хакерської діяльності посідають і сусідній Китай та США.

Японія все більше розглядає кібербезпеку як питання національної безпеки (протидія державним кібератакам, інформаційній війні) й інтегрує це у свої стратегічні документи [381]. Учасники ринку вказують, що зростає попит на рішення з кіберрозвідки, захисту ланцюгів постачання (supply-chain security) [408], розгортання реагування на інциденти тощо.

Сервісний підхід – одна з базових концепцій сучасних методів і стандартів організації роботи IT-підрозділів, що ґрунтується на принципі «якості наданих послуг» та тісно пов’язана з концепцією «клієнтоорієнтованості». Оскільки якість визначається насамперед користувачем, а не постачальником, ефективність інформаційної безпеки залежить не лише від технічної надійності, а й від зручності використання сервісу й адаптованості його процесів до потреб клієнта. Поширеною формою взаємодії між замовником і ринком кібербезпеки в Японії (як і в багатьох розвинених країнах) є аутсорсинг інформаційної безпеки. Організації дедалі частіше делегують функції захисту власної IT-інфраструктури спеціалізованим компаніям, що мають відповідні сертифікати, досвід і ресурси для впровадження комплексних рішень безпеки. Така модель дає змогу ефективніше реагувати на інциденти, забезпечуючи гнучкість і відповідність міжнародним стандартам [548]. Зокрема, вони закуповують рішення у

постачальників, здійснюють їх налаштування, установлення, налагодження, обслуговування на стороні замовника. Для компаній, які виробляють рішення, такі підрядники є авторизованими дилерами на певній території й постають постачальниками послуг.

Основні принципи аутсорсингу інформаційної безпеки викладено в стандартах управління інформаційною безпекою, наприклад в ISO 27001: 2013; ISO 13335-3; NIST SP800-35; Посібнику зі служб безпеки інформаційних технологій або Cobit (скорочено від версії 4.0 або версії 5.0 цілей управління інформаційними та суміжними технологіями) [411].

Загальною характерною рисою інтернет-індустрії в Японії є добровільна саморегуляція учасників. У державі немає комісії чи урядового органу, безпосередньо відповідального за регулювання інтернету. Міністерству внутрішніх справ та комунікацій (co-mu-sho), що відповідає за телекомунікації, інтернет і мовлення, виділено найбільше коло повноважень щодо регулювання відносин в інтернеті [397].

Для регулювання галузі створено неурядові організації за підтримки комерційних компаній: Форум мобільного вмісту (MCF); Асоціація оцінки та моніторингу вмісту; Японська асоціація сприяння безпеці в інтернеті (JISPA); Японська асоціація соціальних ігор (JASGA) й інші. Найчастіше вони відповідають за визначення неприйнятності та блокування забороненого вмісту, наприклад такого, як дитяча порнографія [314].

Від 2001 р. Законом про обмеження відповідальності, визначено формат взаємодії між учасниками щодо контенту в інтернеті. Відповідно до нього, створено середовище саморегулювання, яке реагує на запити уряду щодо видалення вмісту, що порушує авторські або суміжні права та інші форми власності. У технічному плані основні організаційні особливості японської системи інформаційної безпеки: високий рівень інформаційних загроз; широкий та об’ємний ринок; загальний аутсорсинг інформаційної безпеки; сервісний підхід; висока вартість репутаційних ризиків; низька участь державних регуляторних структур в управлінні Інтернетом; велика частка

внутрішнього трафіка, його переважне значення над зовнішнім; висока залученість кримінальних структур до інформаційної безпеки країни.

Висока вартість репутаційних ризиків на японському ринку інформаційної безпеки пов'язана, з одного боку, із традиційно високими ризиками репутації в цій галузі, а з іншого – зі встановленим форматом ведення бізнесу в Японії. Вона є однією з найбільш інформаційно розвинених країн світу. Конституційно-правова доктрина визначення гарантій інформаційних прав громадян і регулювання інформаційних відносин складається з таких джерел, як Конституція, міжнародні документи, нормативно-правові акти, судові прецеденти, тлумачення та професійні думки юристів, а також традиції й суспільні регулятори суспільства. Інформаційні права громадян уключають такі права, як право на доступ до інформації та право на конфіденційність особи, уключаючи право на захист особистої інформації.

Інформаційна політика в Японії координується Кабінетом Міністрів через Національне агентство цифрових технологій, створене у 2021 р. як відповідь на виклики цифрової трансформації. Основна функція агентства – забезпечення єдиного цифрового управління, зокрема у сфері кібербезпеки, захисту даних й інтероперабельності інформаційних систем. Також важливу роль відіграє Комісія з персональних даних Японії (PPC) – незалежний орган, що здійснює контроль за обробкою персональної інформації та слідкує за дотриманням стандартів кіберетики. Особливістю японської моделі є делікатне поєднання адміністративного контролю й корпоративної відповідальності. Уряд активно співпрацює з IT-компаніями (NTT, SoftBank, Rakuten), підтримуючи спільні ініціативи з боротьби з дезінформацією, фейковими новинами та інформаційними атаками.

За даними звіту «Ландшафт кіберзагроз у Японії» [407] («Japan Cyber Threat Landscape»), у середньому за тиждень компанії Японії зазнають ≈ 1003 кібератак. У 2024 р. уряд зафіксував щонайменше 447 інцидентів, що майже вдвічі більше, ніж за попередній рік. Японський ринок кібербезпеки

оцінювався в близько 2,03 млрд доларів США у 2024 р. із прогнозом зростання до ≈ 3,23 млрд доларів США до 2029 р. [409].

Модель інформаційного контролю в Японії ґрунтується на поєднанні нормативного регулювання, цифрової модернізації, інституційної координації та культурних чинників. Вона є гнучкою, адаптивною, схильною до компромісів між інтересами держави, бізнесу й громадянського суспільства. В умовах глобального загострення інформаційної конкуренції Японія демонструє приклад поміркованого контролю, що спирається не стільки на цензуру, скільки на системну відповідальність усіх акторів інформаційного простору. Ця модель потенційно може слугувати орієнтиром для демократичних країн, які прагнуть захистити інформаційний суверенітет, не порушуючи при цьому основоположних свобод.

Якщо застосувати пропоновану нами формулу інформаційної стійкості стосовно Японії, Китаю та Індії (додаток Е), то отримаємо такі результати, як показано в табл. 4.2.

Таблиця 4.2

Індикатори інформаційної стійкості: Азія

(Японія, Китай, Індія)*

Країна/блок	КС	ЦК	ІД	ІС	ІСІС	Рівень
Японія	0.76	0.84	0.72	0.75	0.77	Середня
Китай	0.45	0.88	0.3	0.85	0.62	Середня
Індія	0.7	0.72	0.65	0.6	0.67	Середня

* Джерело: розробка здобувача.

Інформаційна стійкість Японії характеризується показником ІСІС 0,77, що відповідає середньому рівню у верхній межі. Японська модель поєднує високий рівень технологічного розвитку з особливою культурою комунікаційної відповідальності. Когнітивна стійкість (0,76) підтримується завдяки широкому поширенню цифрової культури, регулярним тренінгам для державних службовців, бізнесу й громадян, а також зрілому медійному ринку. Водночас культурні норми giri та wa, система пресклубів і наявність форм

неявної цензури формують середовище «узгодженої стриманості» щодо висвітлення чутливих тем. Прикладом цього стала комунікаційна обмеженість під час аварії на Фукусімській АЕС. Така модель сприяє громадському порядку, проте зменшує автономію критичного дискурсу, що знижує потенційний рівень когнітивної стійкості.

Цифрова компетентність (0,84) залишається однією з найвищих у регіоні. Регулярне оновлення кіберстратегії Японії (кожні три роки), упровадження принципів Zero Trust, використання сучасних методів шифрування, хмарних рішень, постійного аудиту, а також діяльність Digital Agency та незалежного регулятора PPC забезпечують високу технологічну готовність. Японська система кібербезпеки побудована на сервісно-орієнтованій моделі, що поєднує державну координацію з корпоративною саморегуляцією.

Інституційна довіра (0,72) підтримується наявністю законів про захист персональних даних та доступ до публічної інформації, а також розвиненою практикою soft law – рекомендацій, кодексів і галузевих стандартів. Водночас пресклуби й журналістська самоцензура обмежують прозорість у кризових ситуаціях, що стримує подальше зростання рівня довіри.

Інформаційна стабільність (0,75) забезпечується завдяки високому рівню цифровізації та постійним навчальним програмам із кіберосвіти. Проте зростання кількості кіберзагроз і розширення кола їхніх жертв, зокрема серед критичної інфраструктури, знижують загальний показник стабільності.

Отже, японська модель демонструє гнучке поєднання правового регулювання, саморегуляції та корпоративної етики. Вона гарантує високу технічну готовність і достатній рівень когнітивної стійкості без надмірного обмеження прав, проте потребує більшої прозорості в кризових комунікаціях та зменшення інформаційної монополізації під час надзвичайних подій. Японія сформувала унікальну, збалансовану модель інформаційної безпеки, що поєднує високий рівень технологічного розвитку, правового регулювання й культурної відповідальності. Еволюція її інформаційного законодавства від

поступового становлення у 1960–1990-х рр. до сучасної комплексної системи кіберзахисту свідчить про стратегічну орієнтацію держави на побудову «інформаційного суспільства» нового типу.

Сучасна нормативно-правова база, зокрема закони про захист персональних даних, доступ до публічної інформації, базові принципи кібербезпеки та активну кібероборону, створює основу для ефективного регулювання цифрового середовища. Японська держава активно співпрацює з приватним сектором, розвиваючи модель партнерства й сервісного підходу в управлінні безпекою, що проявляється в широкому використанні аутсорсингу інформаційної безпеки.

Особливістю японської системи є поєднання soft law-регулювання, глибокої культури корпоративної етики та високої репутаційної відповідальності, які відіграють роль «м'яких» механізмів контролю. Інституційна координація через NISC, METI та Національне агентство цифрових технологій забезпечує узгодженість політики між державою, бізнесом і суспільством. Отже, модель інформаційного контролю Японії є гнучкою, еволюційною та орієнтованою на довіру, що дає змогу країні підтримувати баланс між свободою інформації, захистом персональних даних і національними інтересами. Вона демонструє приклад того, як держава може поєднувати інновації, законодавство та культуру в єдину систему стійкої інформаційної безпеки.

У добу глобальної цифрової трансформації Китайська Народна Республіка (КНР) постає як провідний приклад держави, що сформувала цілісну, ідеологічно вмотивовану та технологічно досконалу систему інформаційного контролю (Додаток Є). Її головна мета – забезпечення політичної стабільності, збереження монополії Комуністичної партії Китаю (КПК) на владу й управління громадською свідомістю як усередині країни, так і в міжнародному інформаційному просторі. В умовах цифрового авторитаризму Китай створив модель, що поєднує жорстку цензуру, масове спостереження, алгоритмічний контроль, пропагандистське моделювання

реальності. У політичному дискурсі КНР інформація розглядається як фактор стратегічного управління й інструмент ідеологічної мобілізації. Центральне гасло КПК – «керувати мережею згідно із законом, керувати мережею згідно із мораллю, керувати мережею згідно з ідеологією» – відображає прагнення до централізованого управління цифровим простором як основою збереження режиму [538].

Поняття «інформаційний тероризм» у китайському дискурсі де-факто поєднує онлайн-екстремізм, сепаратизм і терористичну пропаганду, особливо в контексті Сіньцзяну. Закон про протидію тероризму (2015 р., ред. 2018 р.) вимагає від інтернет-сервісів, провайдерів, платформ моніторити, контролювати, виявляти, блокувати й видаляти заборонений контент, вести реєстрацію користувачів та допомагати слідству, сприяння правоохоронцям; публічні наративи МЗС, офіційних структур підкреслюють основні «три зла» – тероризм, сепаратизм, екстремізм [311].

Основою інформаційного контролю є Закон КНР про кібербезпеку (2017 р.), Закон про безпеку даних (2021 р.) і Закон про захист персональної інформації (2021 р., табл. 4.3). Ці акти зобов’язують технологічні компанії співпрацювати з державою, зберігати дані на території Китаю, передавати їх на вимогу спецслужб і фільтрувати контент, що «загрожує соціальній гармонії». Державний нагляд здійснює Адміністрація кіберпростору Китаю (CAC) – головний регулятор, що координує цензуру, розробляє алгоритмічні політики та контролює цифрові платформи. Усі медіа, зокрема онлайн-видання, зобов’язані дотримуватися затвердженої лінії КПК. Змістовна база інформаційної політики Китаю спирається на концепцію інформаційного суверенітету, згідно з якою держава має повне право контролювати інформаційний потік у межах своїх кордонів. Такий підхід прямо суперечить західному розумінню свободи слова й відкритого інтернету [562].

Таблиця 4.3

Нормативно-правова архітектура інформаційної безпеки Китаю*

Рік	Нормативний акт	Фокус	Ключові положення / Виконавець
1	2	3	4
2017	Закон про кібербезпеку (CSL)	КІК, локалізація даних, безпека мереж	Вимоги до операторів критичної інфраструктури; у 2025 р. запропоновано поправки з жорсткішими санкціями. Виконавець: CAC, MPS, MIIT
2021	Закон про безпеку даних (DSL)	Класифікація / категоризація даних	Оцінка ризиків, контроль «важливих даних»
2021	Закон про захист персональної інформації (PIPL)	Захист ПІ	Згода, мінімізація, трансфер за кордон. Активні перевірки у 2024 р.
2022	Положення щодо алгоритмічних рекомендацій	Рекомендаційні системи	Обмеження маніпулятивних ранжувань; прозорість та контроль користувача
2023	Глибокий синтез (дипфейки)	Маніпульований медіаконтент	Обов’язкове маркування й техзасоби виявлення, відключення
2023	Тимчасові заходи щодо генеративного ШІ	Регулювання сервісів ШІ	Реєстрація, аудит, відповідальність за безпечний, «позитивний» контент
2024	Держтаємниці	Розширення захисту «таємниць» і «службової інформації»	Інспекції матеріалів, персоналу, зростання ризиків для бізнесу, журналістики

*Складено за: [322; 294; 289; 487; 290; 298]

На сьогодні інформаційна безпека Китаю спирається на «тріаду» законів CSL–DSL–PIPL (табл. 4.3), яку у 2023–2025 рр. підсилили спеціальні акти щодо алгоритмів, дипфейків і генеративного ШІ, а також оновлений Закон про державні таємниці (2024 р.) [322]. Це дає державі широкі повноваження контролю контенту, даних і платформ. CSL – Закон про кібербезпеку (Cybersecurity Law, 2017 р.) [289] – базовий, визначає загальні принципи кібербезпеки, управління даними й обов'язки операторів критичної інформаційної інфраструктури (CII). Основні положення та мета – установлює вимоги до локалізації даних (усі персональні дані та важлива інформація, зібрана в межах Китаю, повинні зберігатися на території країни); зобов'язує компанії проходити державну перевірку безпеки під час обробки даних, пов'язаних із національною безпекою; визначає систему кібернагляду, технічного контролю, моніторингу та реагування на кіберінциденти; метою є зміцнення державного контролю над інтернет-простором і забезпечення «кіберсуверенітету».

DSL – Закон про безпеку даних (Data Security Law, 2021 р.) [294] зосереджується на регулюванні управління даними в ширшому сенсі (не лише персональними). Основні принципи – класифікація даних за рівнем важливості (державні, комерційні, стратегічні, персональні); установлює режим захисту, експорту й транскордонної передачі даних; визначає обов'язок компаній проводити оцінку ризиків і впроваджувати системи захисту даних. Мета полягає у створені національної системи безпеки даних, яка гарантує контроль держави над усіма потоками інформації, уключаючи іноземні корпорації.

PIPL – Закон про захист персональної інформації (Personal Information Protection Law, 2021 р.) [298]. Аналог європейського GDPR, але з китайською специфікою та своїми принципами: визначає, що збір, зберігання, передача, обробка й видалення персональної інформації повинні здійснюватися з інформованої згоди суб'єкта даних; запроваджує поняття «персональні дані особливої категорії» (біометричні, місцезнаходження, фінансові тощо) з

підвищеним рівнем захисту; передбачає жорсткі санкції за порушення аж до заборони діяльності. Метою є захист прав громадян на конфіденційність та зміцнення державного контролю за цифровими платформами.

Разом вони реалізують концепцію «національного суверенітету в кіберпросторі» й забезпечують тотальний контроль держави над інформаційними потоками, цифровими компаніями та користувачами.

Із моменту оголошення ініціативи «Belt and Road Initiative» («Пояс і дорога» (BRI)) у 2013 р. вона послугувала провідною економічною й зовнішньополітичною програмою Китайської Народної Республіки (КНР). У міру того, як мільярди доларів китайських інвестицій уклали в дорожні, портові та залізничні інфраструктурні проєкти по Євразії й Африці, Китай водночас прагнув побудувати «Digital Silk Road» («Цифровий шовковий шлях») по всій мережі BRI [295]. Цей цифровий вимір фокусується на побудові та розширенні наявної телекомунікаційної інфраструктури й сприянні обміну інформацією через створення цифрових ринків. Китай підтримав ці зусилля шляхом партнерства з кіпрськими фірмами задля забезпечення мережевої безпеки інвесторів BRI. Для того щоб задовольнити попит, КНР прагнув заохотити китайські фірми з кібербезпеки «вийти» та інвестувати в країни-одержувачі BRI. Ця стратегія викладена в документі, опублікованому у 2017 р. Китайським державним інформаційним центром «Leveraging the «Belt and Road» («Використання «Пояса й дороги») для прискорення зростання кібербезпечних підприємств у Китаї [536].

Документ оцінює, що BRI представляє значну можливість для кіпрських кібербезпечних фірм розширити свою зарубіжну присутність, зауваживши, що таким компаніям зараз заважають такі фактори, як відсутність міжнародного розпізнавання бренду та недостатній досвід роботи за кордоном. Замість цього, запропоновано встановити «механізми зв’язків» між урядом КНР і відібрати компанії з кібербезпеки, щоб ці підприємства могли «співпрацювати й підтримувати національні стратегічні цілі [КНР], розуміти потреби країн-

партнерів і будувати інтерактивну архітектуру підтримки між державними та охоронними підприємствами» [558].

Ініціатива, проведена Пекіном – Venustech, є корисним прикладом реалізації цієї стратегії державно-приватного партнерства. Вона є одним із найбільших і найвідоміших постачальників кібербезпеки Китаю, і має тісні зв'язки з урядом КНР. Наприклад, надаються послуги міської безпеки для муніципальних органів влади в Юньнані й Куньміні, керується Центром безпеки Тяньцзіня (SOC), а також співпрацює як із Міністерством громадської безпеки, так і з Національною адміністрацією з охорони державних секретів у розвитку національних стандартів безпеки мережі.

У 2018 р. Venustech підписала «Стратегічну угоду про співробітництво» з Китайською асоціацією дружби (CAFF), щоб сприяти безпеці мережі в країнах BRI у рамках ініціативи «Цифровий шовковий шлях» [300]. CAFF – це установа, яка підпорядковується Міністерству цивільних справ КНР та претендує на дещо туманну місію «підтримки дружби і взаєморозуміння між Китаєм та міжнародним співтовариством», активно залучена до розширення партнерських країн BRI. Крім того, CAFF підтримує міцні зв'язки як із КПК, так і зі службами безпеки Китаю. Наприклад, голова CAFF Чень Жимін є колишнім заступником міністра громадської безпеки, а також є членом 13-го Національного комітету китайської народної політичної консультативної конференції.

Незважаючи на те, що деталі Угоди про стратегічне співробітництво Venustech і CAFF не були оприлюднені, це, здається, зроблено задля розширення присутності Venustech у країнах-партнерах BRI. Відповідно, обидві організації співпрацюють над розширенням інформаційної діяльності країн. Наприклад, у жовтні 2018 р. вони стали співорганізаторами форуму з питань безпеки мережі в рамках «Бізнес-саміту шовкового шляху» в Чжанцзяцзе. Форум зібрав понад 500 представників урядів-учасників BRI, а також відзначений виступом із доповіддю Чень Жиміна, який підкреслив необхідність розвитку інфраструктури мережевої безпеки в рамках BRI. На

форумі також відбулася презентація Мао Вейхуа, старшого віцепрезидента компанії Venustech, який стверджував, що прийняття приватних «рішень безпеки для третіх сторін» є ідеальною моделлю для зміцнення мережевої безпеки в країнах-членах BRI [13].

Загалом, здається, що зусилля Venustech і CAFF, щоб спільно спонсорувати бізнессаміт Шовкового шляху й інші подібні події, є спільними зусиллями для активного прискорення нових інвестиційних можливостей у країнах-партнерах BRI. Однак важливо відзначити, що це не єдине партнерство. Наприклад, Ханчжоу на базі хмаробезпечної фірми DBAPPSecurity Ltd. також підписала подібну угоду про співпрацю з CAFF. Більше того, інші фірми, такі як Meiya Pico і NSFocus Information Technology Co., швидко розширили свою присутність в областях, що одержують BRI.

Ураховуючи діапазон та масштаби цих інвестицій, цілком імовірно, що китайські кібербезпечні фірми відіграватимуть усе більшу роль у майбутній інфраструктурі мережевої безпеки Євразії. Це партнерство між Пекіном та приватними китайськими фірмами матиме значний вплив на мережеву безпеку в Євразії й Африці. По-перше, зрозуміло, що КНР намагається відігравати надзвичайно активну роль, допомагаючи своїм кіберзахисним фірмам швидко розширювати присутність за кордоном. Поширення на ринки BRI представляє величезну інвестиційну можливість для китайських фірм із мережевої безпеки, підкреслюючи потенційні ринки в Пакистані й Лаосі як можливості потрапити та зафіксувати якомога більшу частку ринку. Припускаючи, що ці інвестиції є успішними, цілком можливо, що китайські фірми, такі як Venustech, удосконаляться настільки, щоб конкурувати з іншими основними гравцями, такими як Kaspersky і Symantec, у світовому ринку.

По-друге, цілком імовірно, що КНР використає свої інвестиції в інфраструктуру мережевої безпеки за кордоном, щоб проповідувати власне бачення управління інтернетом. Китай уже намагався побудувати підтримку через такі форуми, як «Один пояс, одна дорога», Міжнародна ініціатива з цифрової економіки», яка виступає за посилення державного контролю над

інформацією під виглядом «кіберсуверенітету». Водночас, коли китайські фірми розширилися в Євразії, вони почали пропонувати навчання з кібербезпеки для військових і правоохоронних органів у таких областях, як Шрі-Ланка. У сукупності ці випадки є унікальною можливістю для Китаю формувати інституційну практику безпеки мережі в країнах-партнерах BRI як на національному, так і на місцевому рівнях. У майбутньому Пекін, безсумнівно, вплине на ці відносини для більш сильного формування глобальних стандартів і норм кібербезпеки.

По-третє, інтеграція китайського програмного забезпечення для забезпечення безпеки в критичну інфраструктуру по всій Євразії може слугувати благом для шпигунства й служб безпеки Китаю. У звіті 2018 р. фірма FireEye оцінила, що інвестиції BRI призведуть до зростання «кіберзагрози». Такі думки повторювались у звіті Ради із міжнародних відносин, яка припустила, що такі проєкти можуть бути використані як засіб для КНР, щоб уставити «бекдор-механізми», які допомагають своїм спецслужбам у рамках телекомунікаційної інфраструктури BRI. Хоча не було переконливо доведено, що китайські підприємства кібербезпеки діяли від імені китайської держави, хоча є чимало доказів, які свідчать про те, що ці фірми мають привітні відносини зі службами безпеки КНР. Крім того, відповідно до Закону про кібербезпеку Китаю, усі підприємства мережі (уключаючи охоронні фірми) зобов’язані надавати дані та інформацію китайським службам безпеки, якщо вони цього потребують.

Інформаційний контроль у Китаї реалізується через багаторівневу систему, що поєднує правові, технічні, адміністративні та поведінкові інструменти впливу. Одним із центральних елементів цієї системи є так званий «Великий китайський фаєрвол» (Great Firewall) – комплексна технічна інфраструктура, призначена для блокування доступу до іноземних вебресурсів, таких як Google, Facebook, Twitter, YouTube, VPN-сервісів, а також фільтрації інформації за певними ключовими словами. Цей інструмент

забезпечує ізоляцію китайського сегменту інтернету та дає змогу здійснювати централізоване управління цифровими потоками [432].

Додатковим елементом є система фільтрації контенту, яка ґрунтується на алгоритмічному виявленні «небажаних» матеріалів і їх модерації. До участі в цьому процесі залучено як державні органи, так і приватні цифрові компанії, що зобов'язані дотримуватися директив Центрального комітету Комуністичної партії Китаю (ЦК КПК). За недотримання вимог щодо цензури передбачено адміністративну або фінансову відповідальність, уключаючи анулювання ліцензій. Важливу роль відіграє соціальна самоцензура, яка є наслідком тривалого впливу авторитарної культури комунікації. Страх перед санкціями, уключаючи кримінальне переслідування, спонукає громадян і журналістів уникати політично чутливих тем, що формує внутрішні обмеження свободи вираження поглядів [293].

До системи інформаційного контролю включено також так звані «50- центові армії» – мережі оплачуваних коментаторів, які виконують завдання з просування офіційних наративів, розмивання критичних дискусій через флуд або дезорієнтуючі повідомлення. Їхня діяльність спрямована як на внутрішню аудиторію, так і на іноземні медіамайданчики.

Особливістю китайської моделі інформаційного контролю є поєднання цензурних практик із високотехнологічними системами моніторингу поведінки громадян, зокрема з використанням великих даних, розпізнавання облич і штучного інтелекту. Ці інструменти функціонують у межах програм соціального управління [373].

Одним із центральних механізмів є система соціального кредиту, яка передбачає оцінювання дій громадян і компаній за певними критеріями соціально схвальної поведінки. Позитивний рейтинг забезпечує привілеї, тоді як негативний – обмежує доступ до банківських послуг, мобільності чи працевлаштування [567]. Також формується система цифрових профілів, що враховує онлайн-активність, перегляди, покупки та комунікацію. Ці дані використовуються не лише для персоналізованої реклами, а й для

прогнозування потенційно нелояльної поведінки. У певних регіонах, зокрема в Сіньцзян-Уйгурському автономному районі, система спостереження має надзвичайно високий рівень інтенсивності. Там застосовуються спеціальні додатки, постійний відеомоніторинг, автоматичний контроль мобільних пристроїв, що спрямовані на тотальний контроль за мусульманськими меншинами [278].

Поряд із внутрішнім контролем Китай реалізовує стратегію інформаційної експансії на зовнішньополітичному рівні. Державні медіа (CGTN, Xinhua, China Daily) активно просувають офіційні наративи на міжнародній арені, зокрема через багатомовні інформаційні ресурси та співпрацю з іноземними в межах ініціативи «Один пояс – один шлях». Ця діяльність спрямована на створення альтернативної глобальної інформаційної архітектури [279].

Ззовні Китай веде масштабні, але малоефективні (за охопленням) впливові операції в соцмережах (табл. 4.4) та експериментує із ШІ-контентом, зокрема проти виборів у США й Тайвані. Ці мережі регулярно зносять Meta, Google/Mandiant і Microsoft. Усередині ж країни діють постійні кампанії «Clear & Bright» із масовими блокуваннями акаунтів / контенту [297]. Згідно з даними Freedom House [292] відображено, що 66,6 тис. self-media акаунтів заблоковано у 2023 р., а окрема кампанія для захисту неповнолітніх у 2024 р. призвела до закриття 130 тис. акаунтів і вилучення мільйонів матеріалів. Технічні інструменти держави включають «Великий брандмауер» і «Великий гармат» (Great Cannon) [296], здатний перенаправляти трафік у DDoS-атаки (найвідоміший кейс проти GitHub/GreatFire у 2015 р.).

Таблиця 4.4.

Зовнішні інформаційні операції

(«Spamouflage / Dragonbridge», AI-контент)*

Рік	Мережа	Тактика	Ціль	Доля ефективності

2023	Spamouflage (Meta)	Тисячі фейк-акаунтів, кросплатформені мережі	50+ платформ, критика опонентів Пекіна	«Найбільша в історії» ліквідована мережа, за версією Meta, низький органічний інгейджмент
2023–2024	Dragonbridge (Google TAG / Mandiant)	Масове «спам-насичення», мімікрія під американців	США, західні аудиторії, вибори	Активна, але низький вплив; хвилі під вибори
2024	China-linked IO з AI-контентом (MTAC, WSJ)	Генеративні зображення, відео, боти	Вибори США, Тайвань	Зростання експериментів зі ШІ; вплив поки обмежений
2025	Різні про-КНР кластери (OpenAI TI)	Спроби використання моделей ШІ для впливу	Міжнародні платформи	Виявлено й зірвано низку операцій

*Складено за [486; 291; 333].

Значного розвитку набули й кампанії цифрової дезінформації, які здійснюються через підставні акаунти, бот-мережі та платформену активність у соціальних мережах. Такі кампанії націлені на підрив легітимності західних урядів, поширення деструктивних наративів під час глобальних криз, як-от: пандемія COVID-19, протести в Гонконгу, війна в Україні – та створення сприятливого іміджу КПК як стабілізувальної сили.

Інформаційна стійкість Китайської Народної Республіки має показник ICIC 0,62, що відповідає середньому рівню й визначається режимно-центричним характером управління (табл. 4.2). Когнітивна стійкість (0,45) залишається низькою внаслідок масштабної системи цензури, алгоритмічної модерації контенту, функціонування «п’ятдесятицентових армій» і застосування соціального кредиту. Такий підхід створює контрольований

інформаційний простір, але обмежує розвиток критичного мислення й автономної медіаграмотності. Стабільність досягається за рахунок зменшення інтелектуальної автономії громадян.

Цифрова компетентність (0,88) у Китаї є однією з найвищих у світі. Її забезпечують Cybersecurity Law (2017), Data Security Law (2021), PIPL (2021), а також діяльність центрального регулятора CAC. Комплекс Great Firewall, широке використання великих даних, біометрії та штучного інтелекту, а також зовнішня стратегія Digital Silk Road створюють вражаючу технологічну інфраструктуру. Інституційна довіра (0,30) залишається мінімальною, оскільки інформаційна політика підпорядкована монополії Комуністичної партії Китаю. Відсутність незалежних ЗМІ, обмеження свободи вираження поглядів і слабкі гарантії приватності позбавляють систему ознак демократичної підзвітності. Інформаційна стабільність (0,85) забезпечується через централізовану вертикаль управління, контроль цифрових платформ і жорстке регулювання інформаційних потоків. Така модель ефективно придушує кризові явища, але підтримує стабільність переважно адміністративними засобами.

Загалом китайська модель відображає феномен «стійкості без довіри»: технічна та режимна стабільність поєднуються з низьким рівнем автономії й порушенням прав людини. Із наукового погляду, це приклад авторитарної інформаційної рівноваги, де контроль переважає над адаптивністю та когнітивним розвитком.

Отже, інформаційний контроль у Китаї є структурно інтегрованим елементом державного управління, що поєднує жорстку цензуру, високотехнологічне стеження, інституційний примус і транснаціональні канали інформаційного впливу. Така модель демонструє ефективність у забезпеченні політичної стабільності, але водночас суттєво обмежує базові права громадян, сприяє ерозії публічного дискурсу й унеможливлює існування незалежної журналістики. На міжнародному рівні ця модель становить виклик для ліберального інформаційного порядку, адже поєднання технологічної

могутності та політичної монополії створює загрозу поширення авторитарних практик в інформаційному середовищі інших країн. Отже, китайський досвід потребує не лише критичного осмислення, а й розроблення механізмів демократичної протидії цифровому авторитаризму.

У сучасному глобальному та конкурентному середовищі бізнесу організації стають усе більш залежними від інформації і її поширення. У такому разі використання комп'ютерних інформаційних систем, а також глобально розпорошених комп'ютерних мереж має велике значення для задоволення цих вимог. З іншого боку, ця залежність робить інформаційні системи організацій поступово більш уразливими до зовнішніх атак та порушень внутрішньої безпеки, що може спричинити фінансові втрати й порушення ділової діяльності. Ось чому дослідження інформаційної безпеки є одним із найактуальніших у наш час. Надзвичайно важливою у цьому контексті є інформаційна безпека Індії як однієї з країн, що стрімко розвиваються та невдовзі займуть гідне місце серед лідерів, оскільки, за даними Cisco звіту, лише ~7 % організацій в Індії нині готові до сучасних кіберзагроз [469]. Водночас є значні випадки витоків даних, порушень безпеки в державному та приватному секторах.

Нормативно-правову базу забезпечення інформаційної й кібербезпеки Індії становлять: Закон про інформаційні технології (2000 р., із поправками 2008 р.) [543] – головний нормативний акт у царині кібербезпеки, який визначає обов'язки організацій щодо інформаційної безпеки, відповідальність за порушення; Закон про захист цифрових персональних даних (2023 р.) [319] – новий закон про захист цифрових персональних даних, який надає права особам і вводить обов'язки для компаній-обробників; Національна політика та рекомендації щодо інформаційної безпеки – політика, яка окреслює захист інформації протягом усього її життєвого циклу в державному секторі; Cyber Swachhta Kendra – центр для аналізу й очищення ботнетів / шкідливого ПЗ, у рамках ініціативи цифрової безпеки.

Основними частинами адміністративної структури є Індійська команда реагування на комп'ютерні надзвичайні ситуації (CERT-In) – національний вузол реагування на інциденти з кібербезпеки, Асоціація кібербезпеки Індії (NCSAI) – консорціум за участю уряду, бізнесу, академії та правоохоронців, який працює над покращенням кібербезпеки, Рада безпеки даних Індії (DSCI) – провідна організація, що спеціалізується на захисті даних, приватності, розвитку екосистеми.

Саме через швидкий розвиток країни й гостру необхідність захисту даних стан інформаційної безпеки Індії активно досліджується й імплементується в різні сфери. На сучасному етапі одним із напрямів залучення іноземних інвестицій до економіки Індії є стратегія «аутсорсингу», яка стала особливо гострою в умовах глобалізації торговельно-економічних відносин. Останнім часом представники багатьох провідних компаній світу цікавляться індійськими фахівцями в галузі інформаційних технологій і телекомунікацій, а також у фінансовій сфері [206]. Індія зробила справжній прорив на світовому рівні в галузі інформаційних технологій. Цьому також сприяла державна підтримка високотехнологічного сектору. Потірбно зазначити, що багато висококваліфікованих спеціалістів індійського походження працюють за кордоном і представляють значну частину працівників таких всесвітньо відомих компаній, як Microsoft (36 %), NASA (32 %) тощо, які також працюють над зміною іміджу Індії на міжнародній арені [512].

Майже десятиліття розвиток цієї сфери вважається пріоритетним у країні, вона користується державною підтримкою та пільгами. Широко відомо, що сучасна Індія поступається лише США у світі за кількістю англомовних IT-фахівців. Із метою координації зусиль і контролю діяльності у сфері інформаційних технологій уведено Національний центр інформатики. Уряд країни лібералізував телекомунікаційний сектор і створив для цього належні умови державної конкуренції із залучення інвестицій в інформаційні

технології. На початку 90-х рр. запущено парки програмних технологій. Наразі існує 30 технологічних парків і ще 14 будуються [206].

У 2000 р. частка Індії на світовому ринку комп'ютерних технологій зросла майже до 20 %, і близько 30 % висококваліфікованих фахівців у галузі комп'ютерів у сучасному світі – індійці за походженням. Збільшення прибутку від експорту програмного забезпечення продовжується й донині (у 2000 р. він перевищив 6 млрд доларів США [53], а прогнози на 2018–2020 рр., які становили 60 млрд доларів США, були виправдані). Ключем до цього слугував той факт, що близько 100 тис. молодих спеціалістів щорічно стають випускниками інженерних програм, а кількість профільних університетів і факультетів постійно зростає. Тільки вищі навчальні заклади в Бангалорі – центрі індійської «Силіконової долини» – випускають 25 000 фахівців на рік – майже стільки ж, скільки всі вищі навчальні заклади США разом [206].

2 липня 2013 р. уряд Індії оприлюднив свою амбітну Національну політику в галузі кібербезпеки. Створення цього документа зумовлене різними факторами, зокрема зростанням індійської індустрії інформаційних технологій, зростанням кількості кібератак та «амбіційністю країни». Політика визначає 14 різноманітних цілей, починаючи від посилення захисту критичної інфраструктури Індії, допомагаючи у розслідуванні та судовому розгляді кіберзлочинності, до створення 500 000 робочих місць для кваліфікованих фахівців у галузі кібербезпеки протягом наступних п'яти років [395].

Для досягнення цих цілей, зокрема, потрібно:

– призначити національне агентство для координації всіх питань кібербезпеки;

– заохотити всі приватні та громадські організації до призначення головного офіцера з питань інформаційної безпеки, відповідального за кібербезпеку;

- розробити динамічну правову базу для вирішення завдань кібербезпеки у сферах хмарних обчислень, мобільних обчислень та соціальних медіа;

- забезпечити функціонування Національного центру захисту критичної інформаційної інфраструктури;

- сприяти дослідженням та розробкам у сфері кібербезпеки;

- посилити глобальну співпрацю у боротьбі із загрозами кібербезпеки;

- удосконалити освітні та навчальні програми у сфері кібербезпеки;

- встановити державне та приватне партнерство для визначення найкращих практик у галузі кібербезпеки [395].

Міністр комунікацій та інформаційних технологій Індії Капіл Сібал зазначив, що впровадження такої політики буде складним процесом, але в кінцевому підсумку необхідним для того, щоб «гарантувати відсутність зривів, які призведуть до дестабілізації економіки».

Індія не є винятком з огляду на різні порушення безпеки та незліченну кількість записів, втрачених під час тривалої цифрової трансформації. Більшість атак сталося в секторах електронної комерції та банківському через високу цінність особистої інформації (ІДЛ). Ці помітні зрушення в державі повинні послужити тривожним сигналом для кожної індійської компанії, щоб краще підготуватися до інцидентів:

- кіберзлочинці зламали веб-сайт Індійської залізничної корпорації громадського харчування та туризму (IRCTC), найбільшого урядового сайту країни, і викрали близько 10 мільйонів записів клієнтів із сервера порталу електронних квитків;

- шахраї підробляли обліковий запис електронної пошти Бінні Бансал, виконавчого директора компанії Flipkart, і надсилали два електронні листи до головного фінансового директора з вимогою перерахування 80 000 доларів США;

- Allegedly Пакистанський кіберзлочин, відомий як Фейсал, нібито порушив веб-сайт Canara Bank. Зловмисник зіпсував сайт, вставивши шкідливу сторінку та заблокувавши деякі його платіжні послуги [500].

Згідно з «M-Trends 2016, Азіатсько-Тихоокеанське видання» Mandiant Consulting, індійські організації більш схильні до порушень даних через погані

інвестиції у високоякісні рішення для безпеки. Кілька організацій досягли зрілості, достатньої для того, щоб вийти за межі антивірусного програмного забезпечення для виявлення шкідливих механізмів по всій території.

Що стосується кібербезпеки в Індії, то усім слід зосередитися на думці, що кібернебезпека може чекати будь-кого, а тому треба відповідально готуватися до майбутнього. Наприклад, губернатор Резервного банку Індії заявив, що Центральний банк покращує свої можливості безпеки, і попросив інші банки наслідувати їхній приклад. Меморандум про взаєморозуміння (МоВ) між національними агентствами з кібербезпеки Індії та Великобританії є кроком у правильному напрямку. Обмін технічною інформацією щодо кібератак, інцидентів у сфері безпеки та їх вирішення принесе користь обом країнам, коли вони разом борються з кіберзлочинністю [500]. Індійський уряд також почав інвестувати час та гроші для залучення експертів із кібербезпеки та партнерства з провідними міжнародними компаніями. Незважаючи на те, що для подолання кіберзлочинності в Індії темпи змін виглядають досить повільно, та краща обізнаність суспільства, ефективні рішення на центральному, місцевому рівнях мають допомогти цій країні більш успішно реагувати на інциденти з кібербезпекою в майбутньому.

Рада з безпеки даних Індії (DSCI) є основним, некомерційним галузевим органом із захисту даних, органом забезпечення інформаційної безпеки цієї країни. Створений NASSCOM® DSCI прагне зробити індійський кіберпростір безпечним шляхом встановлення найкращої практики, стандартів та ініціатив у сфері кібербезпеки та конфіденційності. Для досягнення своїх цілей DSCI співпрацює з урядами та їх відомствами, регулюючими органами, галузевими асоціаціями та аналітичними центрами з метою пропаганди політики лідерства думок, розбудови потенціалу, інформаційно-пропагандистської діяльності [336].

Для зміцнення лідерства в галузі кібербезпеки та конфіденційності DSCI розробляє найкращі практики та основи, публікує дослідження, опитування та статті. Він зміцнює потенціал у сфері безпеки, конфіденційності та кібер-

криміналістики за допомогою програми навчання та сертифікації для професіоналів, правоохоронних органів, залучає зацікавлені сторони за допомогою різних інформаційних ініціатив, включаючи заходи, нагороди, глави, консультації та програми членства. DSCI також намагається збільшити частку Індії на світовому ринку продуктів та послуг у сфері безпеки шляхом ініціатив щодо розвитку глобальної торгівлі. Вони мають на меті зміцнити культуру безпеки та конфіденційності в Індії. Основною місією є розвиток можливостей норм у співпраці з усіма зацікавленими сторонами, включаючи уряд, необхідними для просування до більш безпечного та надійного кіберпростору для покращення торгівлі шляхом збільшення глобальних потоків даних, сприяння інноваціям; зміцнення національної безпеки, захист прав осіб у кіберпросторі, вирішення таких глобальних проблем, одночасно захищаючи національні та галузеві інтереси. Серед цілей:

- співпрацювати з урядами, регулюючими органами, галузевими асоціаціями та аналітичними центрами з питань політики шляхом громадської адвокації;

- встановити лідерство мислення шляхом розробки найкращих практик, стандартів і рамок, публікації досліджень, опитувань та документів;

- нарощувати спроможність: у сфері безпеки, конфіденційності та кіберкриміналістики шляхом навчання та сертифікації окремих осіб, фахівців; у розслідуваннях кіберзлочинності шляхом навчання правоохоронних органів та судової системи;

- взаємодіяти із зацікавленими сторонами через різні ініціативи Outreach, включаючи освітні заходи, різного роду нагороди чи заохочення, розділи, консультації та програми членства;

- розробляти та підтримувати екосистему Assurance для підтвердження практики конфіденційності й безпеки, що впроваджується організаціями;

- збільшити частку Індії на світовому ринку продуктів та послуг у сфері безпеки за допомогою ініціатив із розвитку глобальної торгівлі;

- прагнути до розвитку системи альтернативного вирішення спорів у галузі захисту даних [325].

Рада з безпеки даних Індії діє через шість основних ініціатив та програм: Cyber Surakshit Bharat Initiative [528], мета якої підвищити обізнаність про кіберзлочинність, навчати працівників IT-підрозділів урядових відомств. Ця ініціатива спрямована на державний сектор, а DSCI може бути партнером або учасником; Cyber Swachhta Kendra (Botnet Cleaning & Malware Analysis Centre) [316] – виявити ботнет-інфекції, очистити системи, підвищити кібергігієну. Це один із важливих механізмів на рівні держави, у якому DSCI може сприяти через експертну підтримку; National Critical Information Infrastructure Protection Centre (NCIIPC) [462] – захист критичної інформаційної інфраструктури (енергетика, телеком, фінанси тощо). Це державний орган, але DSCI як асоціація у сфері захисту даних може взаємодіяти з ним; Indian Cyber Crime Coordination Centre (I4C) [394] – координація боротьби з кіберзлочинністю, допомога поліції, аналіз онлайн-загрози. DSCI може бути залучений до партнерств із I4C з боку бізнес-спільноти; Digital Personal Data Protection Act (2023 р.) [530] – забезпечення правової бази захисту цифрових персональних даних. DSCI активно працює з питаннями приватності секторів; Sectoral Privacy Project [502] (зокрема сектор «охорона здоров'я»), в межах якого DSCI запустив «Privacy Guide for Healthcare sector» для великих, середніх підприємств і стартапів. Це приклад того, як він опрацьовує специфічні сектори, розробляє керівництва та підвищує рівень готовності.

DSCI відіграє проактивну роль у створенні «політики», що впливає на залучення та прийняття ІКТ урядом. У своїй пропагандистській роботі вона злагоджено взаємодіє з урядом та іншими ключовими зацікавленими сторонами з питань політики у сфері кібербезпеки, конфіденційності, кіберзлочинності, управління Інтернетом, публічної політики Інтернету, транскордонних потоків даних, хмарних обчислень та Інтернету речей (IoT). На національному рівні цей орган часто співпрацює з Департаментом

електроніки та інформаційних технологій (DeitY), Департаментом комерції (DoC), Міністерством внутрішніх справ (MHA), Міністерством економіки, Секретаріатом Ради національної безпеки (NSCS), Комісією з планування, Бюро індійських стандартів (BIS), тощо [336].

DSCI постійно проводить дослідження, опитування та публікує різного роду звіти задля глибшого аналізу аспектів захисту даних і кібербезпеки. Рада також регулярно організовує заходи, конференції, семінари, круглі столи для взаємодії та залучення зацікавлених сторін. Їхні працівники активно співпрацюють з Урядом та іншими ключовими зацікавленими сторонами з питань політики, пов'язаної з кібербезпекою, безпекою даних, захистом конфіденційності, управлінням Інтернетом та кіберзлочинністю. DSCI займає лідируючі позиції у співпраці з глобальними гравцями та аналітичними центрами з цих питань [325]. Як результат, у 2011 р. опубліковано посібник із розслідування кіберзлочинності, який широко використовувався представниками індійських та міжнародних правоохоронних органів.

Програма членства в DSCI сприяє створенню мережі фахівців із безпеки та конфіденційності, які, починаючи з 2018 р., діляться своїми думками через певного роду платформу – DSCI Excellence Awards [335]. Її мета спрямована на створення надійності індійських компаній, визнаючи та об'єднуючи їх зусилля через три сегменти: корпоративний, LEAS та продукт. Рада активно надає усю необхідну інформацію щодо захисту даних, конфіденційності та кібербезпеки й пов'язаних з ними тем. DSCI бере активну участь у розробці, проведенні тренінгів, розвитку потенціалу для різних урядових і корпоративних організацій з питань безпеки, конфіденційності. Вона постійно навчає працівників поліції, судових органів у галузі кіберкриміналістики в спеціальних кіберлабораторіях DSCI у чотирьох містах Індії. Семінари з розслідування кіберзлочинності також проводяться в рамках проєкту Департаменту електроніки та інформаційних технологій (DeitY). З метою розширення можливостей конфіденційності DSCI запустила програму сертифікації DSCI Certified Privacy Professional (DCPP ©) [325].

Рада також працює над формуванням сприятливої екосистеми для розвитку стійких і орієнтованих на зростання сегменнннн бізнесу, що пропонують продукти та послуги у сфері безпеки.

Ініціативи та заходи, вжиті DSCI для заохочення розвитку національних продуктів: премії DSCI Excellence Awards для найпродуктивніших компаній, до складу яких входять «Компанія року із забезпечення безпеки», «Найновіший продукт року (Innovation Box)», Форум продуктів – це ключова ініціатива з метою підтримки організацій шляхом підключення нових гравців до відомих лідерів безпеки та інноваторів на спільній платформі для обміну ідеями, керівництва та співпраці.

Порушення даних у великих організаціях, таких як JPMorgan Chase & Co, Target та Sony Pictures вказують на три вагомі сфери, які турбують компанії: обробка даних про клієнтів; передача операцій третім сторонам; внутрішнє управління. Як повідомила дослідницька компанія Gartner витрати на продукти та послуги з інформаційної безпеки в Індії у 2017 р. становили 1,5 млрд. доларів США у постійному валютному вираженні, що на 12 % більше, ніж у 2016 р. Ця сума зросла до 1,7 млрд. доларів США у 2018 р. [398], і до приблизно 1,9 млрд. доларів США у 2022 р. Служби безпеки і надалі залишаються найбільш швидкозростаючим сегментом, особливо це стосується аутсорсингу, консультацій та впровадження IT-послуг, так як такі послуги складають 63 % загального ринку підприємств і очікувалось, що вони зростуть до 66 % у 2021 р.

У порівнянні в 2015 р. індійська економіка витратила 13,31 млрд. доларів США на «кібербезпеку» (продукти та послуги), а у 2019 р. обсяги продажів зросли до 66,00 млрд. доларів США. Технологічна індустрія в Індії, особливо з центром у Бангалорі, поступово створює нові способи боротьби з кіберзлочинністю та шахрайством. За даними аналітичних компаній, таких як Gartner, Mordor Intelligence та IMARC Group, ринок демонструє стійке зростання, з фокусом на хмарні рішення, AI-інструменти та сегмент послуг. За 2024 р. обсяг інлійського ринку оцінюється в межах 2,9-9,8 млрд. доларів

США (залежно від джерела). Найконсервативніша оцінка саме від Gartner стосується кінцевих користувачів (end-user spending) [366] – 2,9 млрд. доларів США, тоді як ширші ринкові прогнози (включаючи B2B, B2C та B2G) сягають 9,8 млрд. доларів США (IMARC Group [391]). Це зростання на 12,4% порівняно з 2023 р., зумовлене загрозами ransomware, витоками даних та регуляціями. У 2025 р. було прогнозоване зростання до 3,3-10,8 млрд. доларів США. Основні драйвери: дефіцит кадрів (аутсорсинг послуг), розширення хмарних сервісів та інтеграція GenAI для виявлення загроз.

Єдиним місцем, де об'єднуються зацікавлені сторони з усіх ролей у сфері безпеки, є IFSEC International (International Fire and Security Exhibition and Conference). Вона створює платформу для засвідчення та демонстрації інновацій, активізації співпраці у вирішення найважливіших викликів у світі [390]. IFSEC India, зокрема, є частиною провідного портфоліо у світі безпеки, разом з тим і визнаним авторитетом регіону в галузі експертизи та керівництва з питань промислової безпеки. Захід є центром для більше ніж 18 000 покупців галузі, осіб, які відвідують, щоб ознайомитися з останніми продуктами та інноваціями, налагодити ділові партнерства.

Індія демонструє стрімке зростання цифрового сектору, однак водночас стикається з масштабними кіберзагрозами. Дані свідчать про надзвичайно високий рівень інфікованості, тому що в період з жовтня 2023 р. до вересня 2024 р. зафіксовано 370 мільйонів+ випадків шкідливого ПЗ (близько 702 потенційних загроз на хвилину) на 8,44 млн. кінцевих пристроях [534]. Лише у 2023 р. кількість кібер-інцидентів (зареєстрованих) в Індії сягнула ≈ 1,592,917 [393]. Така інтенсивність атак вказує на системну вразливість як корпоративного, так і державного секторів. Дослідження показують, що лише ≈ 24% організацій Індії вважаються готовими до кібер-атак. Водночас ринок кібербезпеки зростає надзвичайно швидко, так у 2024 р. становив ~6.87 млрд. США, а по прогнозу до 2030 р. – ~20.48 млрд. США (CAGR ~20%) [392]. Це відображає зростання усвідомлення загроз, інвестиції в кіберзахист і державні ініціативи типу Digital India та Cyber Surakshit Bharat.

Розвиток інформаційної безпеки є одним із ключових пріоритетів Індії. Кількість вакансій у цій сфері зростає з кожним роком. Індійський уряд почав активно інвестувати час та гроші для залучення експертів із кібербезпеки та партнерства з провідними міжнародними компаніями. Рада з безпеки даних Індії є провідним галузевим органом із захисту даних, який прагне зробити кіберпростір безпечним і захищеним втілюючи в життя найкращі практики, стандарти та ініціативи у цій сфері. Сьогодні, як ніколи раніше, Індія потребує надзвичайної уваги до інформаційної безпеки.

Індія демонструє середній рівень інформаційної стійкості (ICIC 0,67), який поєднує зростаючий технологічний потенціал із нерівномірністю інституційного розвитку (таблиця 4.2). Когнітивна стійкість (0,70) підтримується високим людським капіталом у сфері IT, активністю спільноти DSCI у просвіті та сертифікації кадрів, а також англомовною технічною освітою. Водночас часті інциденти з безпеки свідчать про різнорівневу підготовленість організацій до протидії кібератакам. Цифрова компетентність (0,72) базується на Національній політиці кібербезпеки (2013 р.), створенні NCIIPC та розвитку IT-парків. Швидке зростання ринку інформаційної безпеки супроводжується недостатніми інвестиціями в якісні рішення, що стримує технологічне вдосконалення. Інституційна довіра (0,65) підтримується партнерством держави з приватним сектором, міжнародними угодами (зокрема з Великою Британією) та розвитком галузевих ініціатив. Водночас нерівномірність цифрової трансформації й повторювані інциденти в державному секторі обмежують стабільність системи. Інформаційна стабільність (0,60) перебуває у стані поступового зростання: розбудова національної інфраструктури супроводжується частими витоками даних і зламами, що вказує на перехідний етап формування ефективної системи реагування. Отже, індійська модель відображає динамічну, ринково-орієнтовану траєкторію розвитку. Ключове завдання полягає у балансуванні між швидкістю цифровізації та якістю захисту, а також у зменшенні розриву між передовими секторами та рештою економіки.

У сучасному глобальному середовищі інформаційна безпека є ключовим чинником національної стійкості та конкурентоспроможності держав. Досвід Японії, Китаю та Індії демонструє різні моделі реагування на кіберзагрози, що формуються відповідно до політичних, економічних та інституційних особливостей кожної країни. Японія реалізує модель сервісно-орієнтованої кібербезпеки з акцентом на соціальну відповідальність і аутсорсинг, однак залишається обмеженою через фрагментарність правового регулювання та неформальні практики цензури. Китай розвиває кібербезпеку як інструмент геополітики, використовуючи приватні компанії для просування цифрового суверенітету в межах ініціативи BRI. Такий підхід супроводжується ризиками щодо прозорості та дотримання прав людини. Індія, натомість, демонструє динамічний розвиток у сфері інформаційної безпеки, поєднуючи інвестиції, розвиток інституцій (зокрема DSCI) та міжнародну співпрацю, але залишається вразливою до кібератак через нерівномірність цифрової трансформації. Загальний висновок полягає в тому, що ефективна система інформаційної безпеки потребує багаторівневої взаємодії держави, бізнесу та суспільства, стратегічного бачення цифрової безпеки, нормативної узгодженості та міжнародного партнерства. Для України досвід зазначених країн є цінним джерелом практик для формування власної політики цифрової стійкості.

Порівняння трьох моделей дає підстави виокремити три траєкторії контролю. Японська траєкторія є комбінованою – вона поєднує правове регулювання, саморегуляцію та сервісність, забезпечуючи баланс між правами людини і безпекою. Китайська траєкторія є централізованою й ідеологізованою – вона демонструє високу ефективність контролю інформаційних потоків, але низьку довіру та порушення прав. Індійська траєкторія є плюралістичною і динамічною, проте відзначається нерівномірною зрілістю інституцій та процесів.

Когнітивний вимір виступає ключовим лімітатором розвитку інформаційної стійкості. Навіть за високого рівня цифрової компетентності

відсутність критичного мислення чи свободи висловлення обмежує реальну спроможність суспільства протидіяти дезінформації. Китайська модель ілюструє феномен «стійкості без довіри», тоді як Індія демонструє приклад поступового інституційного дозрівання. Синтетичний аналіз засвідчує, що японська модель поєднує технічну готовність із поміркованим контролем і культурною відповідальністю, китайська – високий рівень технологічної централізації за рахунок громадянських свобод, а індійська – швидке зростання на тлі інституційної фрагментованості. Теоретично це підтверджує необхідність розрізнення технічної та довірчої стійкості: лише їхня збалансована взаємодія здатна забезпечити захист від інформаційного тероризму без руйнації демократичних цінностей.

4.3. Національні стратегії протидії інформаційному тероризму в країнах Африки та Латинської Америки: регіональні особливості

Інформаційний тероризм – це не лише фальшиві новини чи кібератаки, а систематичне використання дезінформації, пропаганди та маніпуляцій для досягнення політичних, економічних чи ідеологічних цілей, часто з елементами насильства в цифровому просторі. Цей феномен набуває особливої гостроти в регіонах із нестабільними демократіями, високим рівнем бідності та етнічними конфліктами, де соціальні мережі стають ареною для «інформаційних війн».

У країнах Африки та Латинської Америки він проявляється з особливою інтенсивністю через комбінацію факторів: слабкі медіа-регуляції, масовий доступ до мобільного інтернету (за даними Міжнародного союзу електрозв’язків, понад 60% населення Африки південніше Сахари використовує смартфони для новин) та вплив зовнішніх акторів, таких як державні пропагандистські машини чи транснаціональні корпорації.

Першою із пропагандистських груп на теренах африканського континенту була Global Islamic Media Group (GIMG), заснована 29 червня 2001

р. на платформі Yahoo. Доступ до її матеріалів був обмежений – користувачам необхідно було вводити пароль. Уже через шість місяців після створення група налічувала понад 600 абонентів, а згодом їх кількість зросла до 7400 перед тим, як платформа припинила існування навесні 2004 р. Адміністрування здійснювалося з території Канади особою під псевдонімом Abu Banan (Ayed Hamid Mejid). Через GIMG поширювалися навчальні матеріали, ідеологічні праці та пропагандистські тексти. У травні 2004 р., після оприлюднення відео страти американського журналіста Ніка Берга в Іраку, здійсненої за участі Абу Мусаба аз-Заркаві – одного з лідерів «Аль-Каїди в Іраку», ресурс було знищено внаслідок хакерської атаки.

Другою платформою стала Global Islamic Media Centre (GIMC), яку, за деякими даними, заснував Ахмад Аль-Ватикан Біллах, анонімний автор численних джихадистських текстів, присвячених глобальній стратегії ісламістської боротьби. У 2003 р. на сторінках GIMC було опубліковано відео, що закликало до здійснення нападу на Іспанію з метою примусити її вивести війська з Іраку. Хоча цей відеоматеріал не було виявлено на комп'ютерах виконавців терактів 11 березня 2004 р. в Мадриді, він був зафіксований у розсилці GIMC. У серпні 2004 р. Біллах і його медіацентр відкрито закликали до створення єдиної ісламської медіамережі глобального рівня, яка б мала централізоване керівництво та слугувала інструментом мобілізації інтернет-ресурсів в інтересах ісламської умми (громади) [495].

Саме на основі діяльності попередніх структур – GIMG та GIMC – виникла організація Ісламський глобальний медіа-фронт (GIMF) – пропагандистська організація ісламістського руху, пов'язана переважно з «Аль-Каїдою», створена у 2004 р., специфіка якої – зосередження на мусульманській діаспорі [439]. На початковому етапі діяльності GIMF поширював контент виключно арабською мовою, однак згодом було налагоджено публікацію матеріалів і англійською. Від 2005 р. функціонувала німецькомовна секція Globale Islamische Medien Front, яка невдовзі стала провідним джихадистським медіаресурсом у європейському інформаційному

просторі. Організація базувалася переважно на діяльності волонтерів, що забезпечувало широку мережеву присутність, зокрема в безпечному інформаційному середовищі країн Заходу. Це стало конкурентною перевагою GIMF порівняно з іншими ісламістськими медіаструктурами, такими як as-Sahab. Утім, децентралізований характер і відсутність централізованого контролю над авторами контенту призводили до проблем із достовірністю й втратою довіри серед аудиторії [544].

Новостворений «фронт» запустив власний вебсайт і вже у 2007 р. започаткував інформаційний телеканал «Voice of the Caliphate», оформлений за зразком західних новинних програм. Особливістю формату були виступи анонімного ведучого, який відкрито прославляв тероризм. Учасники GIMF також започаткували проєкт «Al Qaeda University of Jihad Studies», спрямований на ідеологічну підготовку бойовиків. Його навчальні матеріали орієнтовані на формування, зміцнення та мобілізацію свідомості моджахедів. У тому ж 2007 р. Інститут дослідження медіа Близького Сходу (MEMRI) повідомив про розробку GIMF програмного забезпечення «Секрети моджахедів», що використовувало високорівневі методи шифрування (зокрема, симетричні ключі 256 біт і асиметричні – 2048 біт), забезпечуючи захист комунікацій і конфіденційність даних.

Організація ефективно використовувала потенціал мусульманської діаспори, розширюючи мовне охоплення своїх публікацій і активно працюючи на різних онлайн-форумах. Вона також поширювала відеоматеріали «Аль-Каїди», здійснювала кібератаки (зокрема блокування сторінок), а також публікувала погрози на адресу органів державної влади. GIMF перетворився на ключову інформаційну платформу джихадистської пропаганди, яка не лише популяризувала насильницький ісламістський дискурс, а й створювала умови для залучення волонтерів і прихильників, формуючи так звану «активність наступництва». Організація поширювала широкий спектр засобів і матеріалів – від інструкцій зі створення вибухових пристроїв до програмного

забезпечення, що сприяло координації та здійсненню терористичної діяльності у цифровому середовищі [128].

На сьогодні у державах із ісламською більшістю або там, де діють радикальні ісламістські організації (Ісламська держава – ІД), цей феномен набуває певної специфіки поєднання ідеології, цифрових платформ, соцмереж, криптовалют, а також зловживання уразливостями кіберсистем. Радикальні ісламістські угруповання активно використовують інтернет-платформи, соцмережі, месенджери, відеохостинги для вербування, створення контенту, поширення ідеології. Наприклад, дослідження показують, що ІД адаптує цифрові навички, об'єднує онлайн-спільноти, навчає прихильників кібербезпеці. Вони створюють чи використовують хакерські групи або об'єднання («кіберхаліфат», «United Cyber Caliphate») для атак типу дефейсу сайтів, DDoS-атак, витоку даних, публікації «kill lists». США в свою чергу вводить санкції щодо кіберпідтримки ІДІЛ, так як офіційно зафіксовано використання кіберінструментів та криптовалют для підтримки терористичної мережі [546]. З іншого боку до боротьби приєдналась організація OIC-CERT [471] (Computer Emergency Response Team організації Organisation of Islamic Cooperation), яка об'єднує 27 мусульманських країн для посилення кібербезпеки в ісламському світі.

Таким чином, GIMF слугував не лише інструментом інформаційної агресії, а й цифровою платформою радикалізації, яка поєднувала технологічні ресурси із системною ідеологічною обробкою для зміцнення глобальної терористичної мережі. [128] Ісламський глобальний медіа-фронт відіграв значну роль у формуванні пропагандистської інфраструктури глобального ісламістського тероризму, забезпечуючи символічну ідентифікацію, «інформаційне наставництво» та можливість залучення волонтерів до так званої «активності наступництва». Через свої канали організація розповсюджувала широкий спектр матеріалів – від інструкцій зі створення вибухових пристроїв до спеціалізованого програмного забезпечення, що полегшувало підготовку та координацію терористичних дій.

Аналізуючи вплив різних видів тероризму, зокрема інформаційного на суспільне життя у тому чи іншому геополітичному регіоні світу, не можемо ігнорувати й африканські країни, що швидко розвиваються, досягають нового значного рівня економічного розвитку та політичного впливу. Тому і для них сьогодні випливає першочергове завдання – захист від негативного інформаційного впливу та від проникнення хакерів у базу даних їх підприємств та державних структур.

Розглядаючи особливості поширення та протидії інформаційному тероризму в африканських країнах, звертаємо особливу увагу на країни-члени Південноафриканського співтовариства розвитку (САДК), де інформаційна політика застосовується для позначення політичних ініціатив, які сприяють використанню інструментів, концепцій, пов'язаних із «глобальним інформаційним суспільством», з метою реалізації їх потенціалу у досягненні цілей національного, соціального та економічного розвитку [270, 2-4]. Існує її три ієрархічні рівні, що використовуються в цьому регіоні:

– політика інфраструктури, яка передбачає розвиток національних (а останнім часом і регіональних) інфраструктур, необхідних для підтримки інформаційного суспільства. Відсутність такої політики, а також її впровадження зробить практично неможливим виконання будь-якої іншої вертикальної чи горизонтальної політики, пов'язаної з ІКТ». Розробка політики в Південній Африці «відображає цю реальність у тому, що загалом політика телекомунікацій підлягає першому перегляду, а потім зосереджується на окремій політиці в таких сферах, як освіта, електронна комерція, свобода інформації, універсальні послуги тощо;

– політика щодо вертикальної інформації включає галузеву політику, таку як освіта, туризм, виробництво, охорона здоров'я тощо;

– горизонтальна інформаційна політика застосовується у всьому суспільстві та впливає на інформаційний сектор як прямо, так і опосередковано впливає на широкі аспекти суспільства (свобода інформації, тарифів, ціноутворення, використання ІКТ державою всередині та у її

стосунках з громадянами, бізнесом, працею, науковими колами тощо) [504, 113-114].

Статистика, представлена на конференції з кіберзлочинності в Кот-д'Івуарі (за даними Gady 2010 р.), показала, що в Африці найшвидше зростають випадки інформаційного тероризму, ніж на будь-якому іншому континенті. Це обговорення стосувалося різних аспектів інформаційної безпеки в САДК та його впливу на регіональний розвиток [364]. М. Гроблер та Дж. ван Вуурен (2012 р.) стверджували, що інформаційний тероризм, вже на той час, включав складні й динамічні технологічні інновації, для яких жодна існуюча правова система не підходить [371, с. 64].

Кіберзлочинність є передумовою розвитку інформаційного суспільства [556], тому й африканські країни намагаються активно протидіяти цій загрозі. Так, Зімбабве у 2017 р. створило повноцінне міністерство, призначене для боротьби з інформаційним тероризмом, під назвою Міністерство кібербезпеки, виявлення та пом'якшення загроз, призначене для стримування злочинів, пов'язаних з кібер-війнами, особливо зловмисних дій, поширених через соціальні медіа-платформи, такі як WhatsApp та Facebook.

В Південній Африці лише за жовтень 2017 р. відбулося понад 6000 кібератак, повідомляє газета Sunday Times, що є свідченням того, що потрібно було щось зробити, щоб приборкати цю тривожну тенденцію, так як більшість великих і малих підприємств погано оснащені, щоб протистояти загрозі кібервійни, особливо якщо їх обліковий запис уже був зламаний. Цей регіон є однією із найбільших кібер-точок доступу через велику кількість населення та досягнення в галузі економічного й технологічного розвитку, а також збільшення можливостей розміщення великих обсягів даних.

Єгипет стикається одночасно з традиційними терористичними загрозами (напад на мечеть в Аль-Равда, Синай, 2017 р., загинуло понад 300 осіб) і зростаючими кібер-ризиками. У 2024 р. було зафіксовано значну кількість кібератак на інфраструктуру держави: системи, мобільні пристрої, соціальну інженерію [318]. У 2023 р. уряд прийняв Національну стратегію

кібербезпеки Єгипту (2023-2027 рр.), в якій серед інших зазначено, що загрози походять не лише від кіберзлочинців, але й від кібер-тероризму та кібервійни. Проте дослідження показують, що політика кібербезпеки в країні також використовується як інструмент контролю протестних рухів і політичної опозиції [437].

До основних питань, пов'язаних з інформаційним тероризмом у цьому регіоні, включають вилучення даних, соціальну інженерію, інсайдерські загрози, порушення бази даних, а також погану ідентифікацію та управління доступом [422]. На думку експертів лабораторії Каперського, близько 20% комп'ютерів, які використовуються в Кенії, вразливі до шкідливого програмного забезпечення, що становить серйозну загрозу для ведення бізнесу в країні, так як багато людей не володіють комп'ютерною грамотністю навіть на рівні користувача. В іншому випадку, зростаюча кількість користувачів мобільних пристроїв, які не знають, як відбувається злом мобільних телефонів.

За даними технологій Check Point Software, статистичних звітів по кіберзлочинність [288], близько двох третин африканських країн-членів INTERPOL заявили, що кіберзлочини (cyber-dependent або cyber-enabled) складають середню-високу частку від усіх зареєстрованих злочинів [405]; у регіонах Західної та Східної Африки кіберзлочини становлять понад 30 % усіх повідомлених злочинів [463]; найчастіші види кіберзлочинів – онлайн-шахрайства (фішинг), бізнес-компроміси електронної пошти (BEC), програмне забезпечення-вимагачі (ransomware) та цифрова шантаж (digital sextortion); за період 2019-2025 рр. втрати від кіберзлочинності в Африці оцінюються у понад 3 млрд. доларів США; перехід до цифрових технологій (мобільний банкінг, хмари, IoT пристрої) в Африці створив збільшення вразливих точок: більше ніж 500 млн. користувачів інтернету на континенті; зростання кількості виявлень шпигунських програм та локальних (on-device) загроз (зростання шпигунського ПЗ на 14 % у бізнес-секторі у 2024 р. порівняно з 2023 р.) згідно звіту від Kaspersky Lab [266].

Впровадження оптоволоконного зв’язку стало причиною зростання інформаційного тероризму в Африці. Країни, які повинні збільшити свою інфраструктуру, включають країни з більш розвиненою економікою, такі як Південна Африка, Кенія та Танзанія в межах регіону САДК. Інформаційний тероризм є зростаючою глобальною загрозою, і навіть такі розвинені економіки, як Сполучені Штати Америки, показали, що вони можуть бути вразливими, що було помічено у передбачуваному зломі серверів DNC, а також виборах підозрюваних російських хакерів. Африка не є винятком, і САДК, зокрема, має бути пильною у боротьбі з цією новою світовою війною, чиї виконавці в більшості невідомі.

В Африці організації в середньому зазнають ~3 325 кібер-атак на тиждень, що приблизно на 72 % більше за глобальне середнє [267]. Станом на кінець 2024 р. виявлено понад 131,5 мільйонів веб-загроз. У бізнес-секторі регіону, згідно з Kaspersky, шкідливі програми-шпигуни (spyware) зросли на ~14 % у 2024 р. порівняно з 2023 р. Серед організацій найбільш атаковані: урядові, фінансові, телекомунікаційні, виробничі [266].

Розглянемо перелік країн, що постраждали від кібер-атак за 2024-2025 рр., із вказанням метрики, за якою вони вирізнялися: Ефіопія – №1 у світі за кількістю виявлень шкідливого ПЗ у 2024 р. (показник масштабу атак на організації в країні); ПАР – найбільше виявлень ransomware в Африці (17 849, 2024 р.); Єгипет – друге місце за ransomware-виявленнями (12 281, 2024 р.), також серед найбільш цифровізованих економік регіону; Нігерія – стабільно серед топ-цілей; зростання атак (підйом у глобальному індексі, 2025 р.); Кенія – серед лідерів регіону за частотою атак на організації та помітними інцидентами проти держсектору; Марокко – найвищі веб-загрози для бізнесу (13,9 млн. детекцій, 2024 р., дані Kaspersky); Ефіопія (локальні загрози) – також у топі за зростанням локальних (on-device) загроз для організацій (2024 р.); Зімбабве – входить у топ-десятку глобального індексу ризику атак (високі показники malware / ризик-індексу серед африканських країн); Ангола – у переліку країн з найвищими веб-загрозами для бізнесу (2024 р.); Танзанія, Кот-

д’Івуар, Камерун (паритет) – країни з підвищеними веб- та локальними загрозами для організацій (2024 р.).

Отже, континент перебуває на етапі швидкої цифрової трансформації, що супроводжується суттєвим зростанням кібер-ризиків. Частка кіберзлочинності серед кримінальних проявів є суттєвою (30 %+ у деяких субрегіонах), що свідчить про те, що кіберзагрози перестали бути лише «додатком» до традиційної злочинності. Найслабшою ланкою є готовність інституційних, правових та кадрових механізмів реагування. Зокрема, ~90 % країн зазначили потребу значного покращення здатності правоохоронних органів чи прокуратури для боротьби з кіберзлочинністю. Зростає технічна складність атак: крім фішингу, ransomware, BEC – вже присутні шпигунське ПЗ, модульні шкідливі програми, APT-групи, локальні уразливості. Для бізнесу й держави стають ключовими питання захисту мобільних платформ, управління IoT, хмарної безпеки, підвищення цифрової грамотності користувачів.

Інформаційний тероризм є зростаючою глобальною загрозою, і Африка не є винятком, оскільки уряди регіону поки що не продемонстрували своїх впевнених заяв про повний намір боротися з кіберзлочинністю. Зокрема, дії країн САДК мають бути спільні у боротьбі з ним, шляхом удосконалення національних правових баз (адаптувавшись до сучасних типів кіберзлочинів), розвитку кадрів та інституційної спроможності (поліція, кіберполіція, прокуратура, суди), підвищення обізнаності населення та малого/середнього бізнесу про основні кіберризики (фішинг, небезпечні мобільні додатки, слабкі паролі), посилення міжнародної і регіональної співпраці, інвестицій в технологічні засоби захисту зокрема для бізнесу: рішення з шифрування, багатофакторної автентифікації.

Сучасна інформаційна політика в розвинених країнах – це сукупність напрямів і способів діяльності компетентних органів держави з контролю, регулювання та планування процесів у сфері одержання, зберігання, оброблення, використання та поширення інформації. Держава регулює

відповідний розподіл інформаційних ресурсів, загальні принципи інформаційної діяльності, встановлює пріоритети для забезпечення національних інтересів [167].

У 1990-х роках після поширення демократії в Латинській Америці пріоритетами Організації американських держав (ОАД) виступали посилення демократії, захист прав людини, сприяння розвитку зовнішньої торгівлі, боротьба з корупцією і наркотиками, просування цілей сталого розвитку, а також боротьба із зміною клімату та інформаційна безпека.

На самітах ОАД регулярно відзначається успішна демократизація американського континенту (лише Куба залишається державою з диктаторським режимом). При цьому 34 голови держав регіону свідомо ігнорують, що істотна складова плюралістичного суспільства – свобода медіа – в більшості держав-членів ОАД не консолідована. І хоча наразі триває масштабний процес відмови від грубої цензури, у багатьох країнах існують репресивні закони, які ставлять під приціл свободу преси, політичний контроль застосовується практично повсюди.

В цілому, можна стверджувати що в Латинській Америці медіа – це стосується преси, радіо, телебачення, а також Інтернету – знаходяться під тиском відповідної політики уряду. У друкованій галузі родини видавців тримаються на плаву завдяки партійно-політичним та ідеологічним союзам або завдяки крайньому опортунізму (концерн «Глобо», Бразилія). Якщо йдеться про приватні медіа, то репресії наразі майже без винятків мають опосередкований характер. Там, де в телевізійній галузі йдеться про «державні канали», політика часто відкрито втручається в кадрову політику каналів («ТіВіЕн», Чилі).

На думку незалежних об’єднань, законодавство є недосконалим. Як приклад країни з особливо репресивною політикою можна навести Чилі. Там журналісти притягаються до кримінальної відповідальності «за зведення наклепу». Особливою в цьому зв’язку видається позиція парламенту. Після політичного відступу попереднього диктатора Августо Піночета

демократичний уряд видалив із тодішнього законодавства про державну безпеку статті, що стосувалися преси. Після цього парламентарі, що називали себе демократами, перенесли видалені статті в переробленій формі до Кримінального кодексу [321].

Окрім того, проти представників преси в Південній Америці часто застосовуються «делікатні методи» боротьби. Це стосується, наприклад, мовчазного, ніколи відкрито не оголошуваного відтоку рекламних оголошень державних підприємств та інституцій. Крім того, видавців або окремих журналістів швидко «знешкоджують» (прикладом може слугувати позбавлення права власності Баруха Івхера, власника Каналу 2 «Frecuencia Latina», Перу).

Непоодиноким явищем є ідеологічна журналістика, яка занадто наближена до влади. Колумбійська газета «Ель Тьємпо» була протягом довгих восьми років рупором ліберальної партії та уряду колишнього президента Альваро Урібе. В той час як президентом Аргентини був пероніст соціал-демократичного спрямування Нестор Кіршнер, деякі спостерігачі відзначали значну деградацію колись лівої, з індивідуальним ухилом газети «Пагіна 12» до ролі відомчого видання. У державі газети «Кларин» та «Пагіна 12» були де-факто рупорами уряду і як винагороду за це вони отримували ексклюзивно всю відповідну інформацію.

Прямий вплив законодавства стосується переважно лише телебачення та радіомовлення. Газети є приватним продуктом. В галузі електронних медіа точиться гра навколо розміщення замовлень і концесій. Ринок довгий час ділять між собою такі медійні монополісти, як «Глобо» (Бразилія), «Групо Кларин» та «Сітікорп Еквіті Інвестмент» (Аргентина) або група «Сіснерос» (Венесуела) [492].

Особливо вдалим прикладом політичного розміщення замовлень є Бразилія. Концерн «Глобо» продемонстрував стрімке зростання під час правління воєнного режиму. Натомість права особистості (медіаправо), захист інформації та авторські права в країні зовсім ніяк не врегульовані. Відверто

репресивні законодавства, наприклад, такий як у Чилі, постійно призводять до спорів із між американським союзом видавців SIP або до розгляду справ у міжамериканському суді з прав людини.

Бразилія є найвпливовішою країною Південної Америки та й її медіаринок – мабуть, найбільший на південноамериканському континенті. У країні діють тисячі радіостанцій і сотні телеканалів, у великих кількостях видаються газети і журнали, набирає обертів і сегмент Інтернету. У Бразилії майже 90% всієї газетно-журнальної продукції зосереджено в руках кількох об'єднань. Такі провідні газети, як «Глобо», «Жорнал ду Бразил», «Естаду ді Сан-Паулу», «Фольяді Сан-Паулу», наприклад, відбивають інтереси великих промисловців, клерикалів, правих кіл [563].

У країні є всім відома «медіаеліта» – власники цілих конгломератів, що займаються сферою медіа. Ці національні корпорації, в тому числі сама процвітаюча з них – «Глобо» – домінують на ринку медіа, володіючи радіо і телевізійними мережами, а також безліччю газет і платних телеканалів одночасно. Популярні бразильські серіали, здебільшого вироблені тим же лідером Globo, експортуються в багато країн світу. Великим глядацьким попитом також користуються ігрові програми і такий жанр, як реаліті-шоу.

Можна сказати, що в Латинській Америці у політиків, у еліти та суспільства загалом немає розуміння функції медіа як «четвертої влади». В основному «брати і давати» – ось звичай, що склався у відносинах між медіа та політикою на цьому тлі. Так як, редактори програм і газет більшості держав-членів ОАД піддаються внутрішній цензурі, а також на них чиниться значний тиск, який за оцінками організації «Репортери без кордонів» є гіршим за середні умови роботи в Африці.

Бразилія є провідною державою Латинської Америки і учасницею G-20. В останнє десятиліття в країні спостерігається значне збільшення кількості послуг, що надаються громадянам через Інтернет. Серед них виділяються такі: реєстрація, отримання довідок, сплата податків, дублікат документів та консультації, які надаються на онлайн-платформах федерального, державного

та муніципального рівнів. Проте проблема кібербезпеки для Бразилії є актуальною як ніколи. Відповідно до глобального звіту компанії «Kroll» про шахрайство та ризики за 2017/2018 рр., 86% опитаних керівників компаній стикалися з кібершахрайством по всьому світу. В Бразилії ж цей показник становить 89%, що перевищує загальносвітовий рівень. Найбільш поширеним видом шахрайства є шкідливий код, що становить 45% випадків, а також фішинг через електронну пошту – 37%, як наслідок 63% респондентів непокояться про вразливість систем до нових атак [259].

Відповідно до звіту бразильської лабораторії безпеки, що спеціалізується на виявленні цифрових загроз «DFNDR Lab», кількість кібератак у Бразилії майже подвоїлася в 2018 р. у порівнянні з 2017 р. Лабораторія інформує, що 63,8 мільйони кібератак було виявлено лише у другій чверті 2018 р., в середньому 8 кожної секунди і більше 28 тисяч на годину [490].

Відсутність відповідного законодавства про кіберзлочинність сприяє тому, що Бразилія є ціллю номер один і водночас провідним джерелом онлайн-атак у Латинській Америці; 54% кібератак нібито походять зсередини країни. Подібно до США, Бразиліа є одним із найпопулярніших осередків фішингових сайтів. Усе це призвело до того, що вона є однією з перших в десятці світових джерел кібератак [404, с. 66].

Для того, щоб підвищити стійкість Бразилії до кіберзагроз, зробити її процвітаючою та надійною у цифровому середовищі та посилити успішність держави на міжнародній арені, президент республіки затвердив Національну стратегію кібербезпеки. Документ включає десять стратегічних кроків [340]:

Спершу, створення централізованої моделі управління на національному рівні передбачає об’єднання державних і недержавних суб’єктів для стратегічної та оперативної координації дій. Така система має бути під керівництвом урядової установи за участі всіх верств суспільства, за винятком питань кіберзахисту й воєнної сфери, що залишаються в компетенції Міністерства оборони. Подібний підхід успішно застосовується в таких

країнах, як США, Велика Британія, Франція, Південна Корея та ін., де центральні структури забезпечують ефективну координацію та інтеграцію кіберполітики. У Бразилії доцільно використати вже наявну інституційну базу – зокрема, Управління інституційної безпеки Президентства, без створення нових установ. Додатково пропонується створення національної ради з питань кібербезпеки та галузевих робочих груп для залучення експертів і формування політик, адаптованих до специфіки національних потреб і цифрових викликів.

Сприяти спільному, надійному та безпечному середовищу між державним, приватним секторами та суспільством. Стратегія передбачає посилення обміну інформацією про кіберінциденти, створення ефективних механізмів взаємодії між державними, приватними та міжнародними структурами, а також розвиток інфраструктури реагування. Пріоритетними діями є модернізація урядового центру CTIR.gov, підтримка національних CSIRT, розвиток технологічних команд реагування, а також зміцнення спроможності до розслідування кіберзлочинів. Хоча профілактика на основі оцінки ризиків важлива, вона не виключає потреби у швидкому реагуванні на інциденти для зменшення шкоди. У цьому контексті актуальним є створення надійної системи обміну інформацією між усіма секторами, з урахуванням міжнародного досвіду моніторингу кіберзагроз. У Бразилії основними структурами є CERT.br (для приватного сектора) та CTIR.gov (для державного), проте їхня діяльність потребує посилення.

Підвищення рівня захисту уряду. Оцифрування державних послуг супроводжується зростаючим тиском на урядові мережі та системи, які мають забезпечувати належний рівень захисту, відповідний до їхньої важливості. Зі збільшенням інтеграції баз даних і цифрових платформ фіксується зростання вразливостей, що підвищує ризик зовнішніх атак. Витік інформації негативно впливає на надання послуг населенню, тому необхідним є створення актуальних резервних копій, зберігання яких має бути автоматизованим та захищеним. Особливу загрозу становлять мобільні пристрої, що використовуються державними службами, особливо в умовах політики BYOD

(«принеси свій пристрій»). Попри ефективність і економію ресурсів, така практика створює ризики втрати даних та поширення шкідливого ПЗ. У зв'язку з цим доцільним є запровадження чітких нормативів щодо використання пристроїв у державному секторі.

Підвищити рівень захисту національних критичних інфраструктур. Захист критичних інфраструктур заслуговує конкретного підходу. У Бразилії цими інфраструктурами є телекомунікаційний, транспортний, енергетичний та фінансовий сектори. Окрім того стратегічне значення має фармацевтична галузь. За даними порталу CSO, фармацевтичні організації є вразливими мішенями для кіберзлочинності, головним чином через можливість втрати інтелектуальної власності [312]. У 2018 р. було затверджено Національну політику безпеки національної критичної інфраструктури, що спрямована на забезпечення безпеки та стійкості критичної інфраструктури країни та безперервності надання її послуг.

Вдосконалення правової бази щодо кібербезпеки. Для вдосконалення нормативно-правової бази кібербезпеки необхідно оновити чинні положення та запровадити нові інструменти регулювання. Серед рекомендованих дій – виявлення прогалин у законодавстві, включення нових видів кіберзлочинів до Кримінального кодексу, створення стимулюючої кадрової політики, а також розробка проєкту закону про кібербезпеку під координацією Управління інституційної безпеки при Президентові. Акцент робиться на необхідності інновацій та досліджень у сфері кібербезпеки. В умовах технологічної революції це сприятиме формуванню національного продукту в критично важливій галузі. У Бразилії існує розрив між освітніми проєктами та потребами сектору, тому потрібен діалог між університетами, державою й бізнесом. Рекомендується зміцнювати партнерство з Міністерством освіти задля розвитку шкільних програм з кібербезпеки, а також сприяти адаптації університетських досліджень до потреб промисловості. Магістерські та докторські програми з різних дисциплін мають стати інструментом підготовки кваліфікованих фахівців у сфері цифрової безпеки.

Розширити міжнародне співробітництво Бразилії у сфері кібербезпеки. На сучасному етапі існує нагальна потреба у співпраці між країнами з метою пом'якшення загроз, таких як кіберзлочини, кібер-шпигунство, перехоплення даних тощо. У цьому напрямку необхідно посилити дії Бразилії при підготовці та перегляді міжнародних інструментів, пов'язаних з кібербезпекою, шляхом стимулювання дебатів та заохочення міжнародної співпраці з цього питання. Окрім того необхідно сприяти інтеграції між Бразилією та країнами Латинської Америки, з акцентом на регіональному лідерстві Бразилії.

Примітно, що країна має намір шукати двосторонніх угод про співпрацю в кібербезпеці з якомога більшою кількістю країн, що демонструє намір встановити у цій галузі плідні, конструктивні та прозорі відносини. Наразі Управління інституційної безпеки Президентства республіки здійснює моніторинг десятків угод щодо обміну та взаємного захисту секретної інформації.

Розширити партнерство у сфері кібербезпеки між державним й приватним секторами, науковими колами та суспільством. Співпраця між державним управлінням, приватним сектором та суспільством у кількох сферах зазвичай приносить корисні результати та сприяє підвищенню довіри громадян до державних, приватних установ, покращує стосунки між цими суб'єктами. У сфері кібербезпеки цей взаємозв'язок є суттєвим.

На сьогодні в Бразилії процеси координації між різними суб'єктами в кібер-середовищі містять широкий спектр домовленостей, які не завжди є інституціоналізованими та багаторічними, а також не пов'язані зі звичайними механізмами регулювання. До цього факту додається наявність великої кількості установ, які безпосередньо чи опосередковано займаються кібербезпекою, що створює значні труднощі для співпраці та координації для бразильської держави. Тому рекомендується створити відповідні канали комунікації, щоб можна було почути та взяти до уваги думки усіх сегментів бразильського суспільства при розробці, реалізації та просуванні публічної політики пов'язаної з кібербезпекою.

Підвищити рівень обізнаності суспільства щодо кібербезпеки є ключовим чинником формування цифрової культури безпеки та зрілості суспільства в умовах сучасних кіберзагроз. Люди повинні розуміти ризики кіберпростору й ефективно використовувати захисні інструменти для безпечного функціонування у цифровому середовищі. У цьому контексті стратегія передбачає: проведення інформаційних кампаній у державному, приватному секторах, впровадження державної політики з просвітництва, інтеграцію знань із кібербезпеки в базову освіту, а також розвиток вищих навчальних курсів. Пропонується створення програм для студентів, стимулювання підготовки фахівців, участі в міжнародних заходах та активізація співпраці між академічною, дослідницькою і бізнес-спільнотами.

Підсумовуючи наведені спостереження та детально проаналізувавши Стратегію кібербезпеки Бразилії, можна стверджувати, що у країні на сучасному етапі немає єдиної та всеосяжної системи захисту кіберпростору, яка б сприяла зміцненню національної кіберстійкості. Чинні норми, вказівки та стандарти пов’язані із кібербезпекою не були належним чином втілені державними та приватними структурами. Хоча в останні роки активізовано посилення нормативно-правової бази і як наслідок – Закон про захист персональних даних (LGPD) і правила повідомлення щодо інцидентів, які створюють грунтовну основу боротьби. LGPD схожий до GDPR (законодавчого акту Європейського Союзу, який встановлює стандарти для захисту персональних даних), встановлює подібні стандарти для захисту персональних даних громадян або резидентів Бразилії, застосовується до всіх організацій, які їх обробляють.

Цифровий ринок кібербезпеки Бразилії зростає і може стати ключовим гравцем, так як ринкова оцінка станом на сьогодні ~ 3,7 млрд. доларів США у 2025 р. і з подальшим прогнозом до ~ 6 млрд. доларів США у 2026 р. Також важливим фактом є створення Task Force з боротьби з ransomware, коли державні та приватні актори об’єднуються для розробки стратегій.

57,4% кіберзлочинів держави складає «фішинг» – шахрайська схема, метою якої є виманювання у користувачів Мережі конфіденційної інформації, наприклад, паролів та номерів соціального страхування. Вона зазвичай передбачає надсилання повідомлення спаму, яке справляє враження, ніби походить із довіреного джерела, наприклад із банку. У ньому міститься посилання на шахрайський веб-сайт, що видається за довірене джерело. Користувач, нічого не підозрюючи, вводить інформацію, яка цікавить хакерів, вважаючи, що перебуває на сайті, який заслуговує на довіру. Вартий уваги той факт, що в законодавстві Бразилії немає конкретного положення, яке регулює фішинг [277].

Отже, Бразилія – приклад країни, де зростання цифровізації супроводжується зростанням кіберризиків і складних інформаційних загроз. Модель забезпечення інформаційної безпеки тут формується навколо поєднання державного регулювання, співпраці з приватним сектором і прискореного розвитку ринку безпеки. Проте ключовими залишаються питання: захист критичної інфраструктури, ефективне реагування на кібератаки, і протидія інформаційним операціям, які можуть підривати суспільну довіру.

У своїй діяльності мережу Інтернет активно почали використовувати й терористичні організації. Активісти угруповання ХАМАС створили кілька сайтів, орієнтованих на дітей. Прихильники «Хезболли», в свою чергу, можуть скачати із сайту угруповання відеогру, сюжет якої війна з ізраїльтянами в Лівані. У мережі вивішена значна кількість текстів виступів Бен Ладена, книги по ідеології і зразки поезії джихаду, інформація про полонених талібів на базі Гуантанамо. Багато хто знає про мексиканські картелі, але мало хто стикався з їхньою активною діяльністю у мережі Інтернет, яка стає все поширенішою і загрозливішою.

Як відомо, ще з часів сухого закону американо-мексиканський кордон особливо приваблював мексиканських контрабандистів. Однак до 1980-х рр. Мексика залишалася лише транзитною країною наркотиків, так як і

виробництво, і споживання наркотичних речовин у країні були незначні. Проте, у 80-х рр. XX століття у США загострилася проблема наркотиків, і головною загрозою стали великі колумбійські картелі з Медельїн і Калі, лідером яких був відомий Пабло Ескобар. Управління по боротьбі з наркотиками зробило все, щоб перекрити шляхи постачання наркотиків у країну і нанести удар по картелям безпосередньо в Колумбії. В результаті до середини 90-х р. XX століття Медельїнський і Калійський наркокартелі були практично знищені.

Новоутворена порожня ніша на ринку була цікавою мексиканським наркокартелям, які спочатку заробляли лише на транзиті наркотиків, а пізніше, почавши брати плату за транзит безпосередньо кокаїном, почали вигідно перепродавати його на американський ринок. Звичайно, коли колумбійські картелі втратили колишню силу, мексиканські картелі стали головними постачальниками наркотиків у США.

Збагачення картелів природним чином призвело до боротьби за сфери впливу і транспортні шляхи. Пізніше, коли президент Феліпе Кальдерон у 2006 р. оголосив війну наркомафії, збройна боротьба картелів між собою перетворилася в повномасштабний збройний конфлікт із залученням поліції і урядових військ Мексики. За п’ять років, з 2006 по 2011 рр., у цій «війні» загинуло, за офіційними даними – 26 тисяч осіб, а за неофіційними – близько 50 тисяч осіб.

У Мексиці існує кілька десятків картелів, однак, фактично є декілька найвпливовіших. Найбільшими вважаються картелі: «La Familia», «Los Zetas», «Cártel del Golfo» («The Gulf Cartel»), Тихуанський картель, картель Хуареса, Нове покоління Jalisco (CJNG) і картель Сіналоа. Всі ці картелі відстоюють свої позиції на ринку і зміцнюють на карті. Адміністрація з питань боротьби з наркотиками США (DEA) визначила їх домінуючими в Мексиці організаціями з незаконного обігу наркотиків, а також заявила, що цих 7 організацій нині розбито на 9 та дотичні до близько 20 великих світових організацій [445].

Більшість методів в їх арсеналі далеко не мирні, велика частина «акцій» картелів спрямована на залякування населення та опонентів і відрізняється непомірною жорстокістю. Тим не менше, цікавими залишаються дані про інформаційні методи протиборства. Ці групи діють як компанії з розгалуженими виробничими та дистрибуційними мережами, системами розвідки й безпеки, і використовують соціальні медіа для спілкування та Інтернету для проведення своєї діяльності. Вони беруть участь у всіх видах злочинної діяльності, включаючи крадіжку осіб, шахрайство, вимагання, викрадення, торгівлю людьми, органами та вогнепальною зброєю.

Поряд із Facebook та Twitter є веб-сайти, які повідомляють про діяльність різних організованих злочинних організацій. Зростаюча група кібер-дружинників використовує Інтернет, щоб заперечувати наркокартелі, які, зазвичай, створюють їх конкуренти.

Слід зазначити, що до інформаційних методів протиборства відноситься не тільки боротьба безпосередньо в кібер-просторі, але і такі методи інформаційно-психологічного впливу як пропаганда, поширення неправдивої інформації, організація «витоків» інформації про конкуруючих картелів і так далі.

В першу чергу слід відзначити, що Інтернет став найбільш поширеним джерелом інформації, а також одночасно став великим пропагандистським майданчиком, де анонімні компанії використовуютьють сайт youtube.com для розміщення відеороликів, що вихваляє лідерів одного наркокартелю в порівнянні з іншим. Інтернет – це і головне джерело залякування населення з боку наркокартелів. Так наприклад, в місті Рейнос (штат Тамауліпас) виникла паніка і на кілька днів місто спорожніло, а все тому, що жителі отримали повідомлення «Увага! У вашому напрямку виїхали п’ять вантажівок, набиті важкоозброєними людьми. Не виходити з дому! Не висовуватися!».

Ще один випадок, який доводить, що наркокартелі володіють можливостями використання інформаційних технологій трапився в 2011 р., коли група активістів Anonymous у відповідь на викрадення одного зі своїх

членів картелем Los Zetas пообіцяла опублікувати фотографії та імена 70 членів картелю, політиків, ділових людей, військових, журналістів та інших, що задіяні у роботі картелю кур'єрів і дилерів, якщо вони не звільнять учасника групи. В результаті, активістам довелося скасувати свою операцію, оскільки картель активізував роботу власних комп'ютерних експертів і почав пошук інших членів Anonymous [257]. Anonymous відступив, а викраденого члена було звільнено.

Наркокартелі ведуть постійну та активну пропагандистську діяльність. Картель «Тамплієрів», що утворився в 2011 р. і був до цього бойовим осередком картелю la Familia Michoacana, нагадує більше релігійний культ, ніж кримінальну організацію, який провадить свій вплив на населення лише за допомогою комп'ютерних технологій. Варто зазначити, що вони досить часто набирають добровольців, яких активно навчають комп'ютерній грамотності. На підконтрольних територіях вони за допомогою Інтернету поширюють брошуру з викладом принципів свого «ордена»: не проявляти жорстокість, не пити і не вживати наркотики, не ганьбити невинних жінок і неповнолітніх силою, або обманом». За порушення цих правил винного необхідно зв'язати і чотири доби поливати холодною водою, щоб той «виправився» [501].

Широке висвітлення подій у медіа, а також масові протести жителів із різними вимогами, в основному, що стосуються зменшенню впливу картелів на загальну ситуацію у районах непідконтрольних державній владі, спонукали федеральний уряд створити загальнонаціональний план по боротьбі зі злочинністю. Таким чином, цей спосіб, в загальному, можна назвати методом боротьби з організованою злочинністю, хоча як могли спостерігати наприкінці 2019 р. шокуюче відео, що розповсюдили місцеві медіа у погодинних новинах, побачивши, як одночасно швидко і вільно рухалися представники картелів по різних вулицях і як нахабно бойовики залишилися на знімках камер різних районів, легко давали інтерв'ю, погрожуючи місцевому населенню. Мешканці зробили десятки фотографій озброєних злодіїв, які почали невпинно циркулювати в соціальних мережах, посилюючи тим самим страх і загрозу

[382]. Однозначно це яскраво підвищило вплив мексиканських картелів, який як виявилось є набагато потужнішим, аніж їхня армія, що може призвести до трагічних наслідків для управлінців державою. Здавна з'явилося зображення торговців людьми, як повстанців, а деякі в Сіналої називають їх «валієнтами» або «сміливими» («valientes», «brave ones»). На сьогоднішній день, ці повстанці практично контролюють усі державні органи влади.

Надзвичайно потужна підтримка наркоторговців відображається, як не дивно, і у творчому підході – в піснях, в коротких промо роликах, відомих як наркокоріоди або балади наркотиків, що постійно оспівують та висвітлюють їхні найбільші «подвиги». Після чергової розправи різні пісенники, як це буває з певною періодичністю, швидко пишуть нові тексти, особливо про Овідіо Гузмана та розміщують свої вірші в Інтернеті, переважно у соціальних мережах. Варто наголосити, що кількість груп у таких мережах значно збільшується і вони поширюються не лише у великих містах зосередження молоді, а також уже таргетовано зосереджені на уражені підлітків 10-12 років.

Варто зауважити, що «завдяки» інформаційним технологіям на сьогодні територія впливу картелів і поширення наркотиків стрімко збільшується. Так, з 2006 по 2012 рр. значна частина вбивств у ході наркотичної війни сталася лише у визначеному ряді міст Північної Мексики – Сьюдад Хуарес, Тіхуана, Куліакан, Рейноса і Нуево Ларедо. А на разі вона більш розпорошена, і це також ускладнює контроль», – заявив Алехандро Хоуп, аналітик з безпеки в Мексиці [446]. У 2017 р. фінансовий сектор активно співпрацював із офіцером Генерального прокурора (PGR), який створив спеціальний підрозділ, присвячений розслідуванню кіберзлочинів; цей підрозділ активно і тісно співпрацює з Банком Мексики, щоб швидко виявляти та санкціонувати усіх осіб, відповідальних за кібератаки.

Що характерно, поняття кібербезпеки та кіберзлочинності чітко не прописані в мексиканських законах; проте Національна стратегія кібербезпеки 2017 р. визначає їх таким чином: кіберзлочини – злочинні дії, що здійснюються особами, які використовують інформаційні та комунікаційні

технології як засіб або як ціль, і які зафіксовані у кримінальному кодексі чи іншому національному кодексі. Відповідно, Федеральний кримінальний кодекс регулює незаконну поведінку, вчинену електронними засобами, що можуть бути ідентифіковані як кіберзлочини шляхом використання електронних засобів для їх вчинення [444].

Відповідно до мексиканських законів (зокрема, закону про конфіденційність Мексики), організації змушені застосовувати коригувальні, профілактичні та вдосконалювальні заходи, щоб зробити заходи безпеки адекватними, щоб уникнути порушення. Вони повинні мати можливість розмежовувати матеріальну та нематеріальну шкоду відповідно до мексиканських законів шляхом проведення аналізу ризиків. Матеріальна шкода повинна надавати пріоритет перед нематеріальною шкодою і завжди залежатиме від бізнесу, обсягу, контексту та обробки даних, порушених у результаті інциденту. Таким чином, галузеве визначення ризику матеріальної та нематеріальної шкоди є таким важливим для всіх компаній, які стикаються з інцидентом кібербезпеки.

Стикаємось зі ще одним різновидом соціальної інженерії, яку ефективно використовують задля підривання мережевої безпеки – фішинг. Йому не має чіткого визначення і тлумачення у Федеральному кримінальному кодексі Мексики, прописано лише, що це кримінальне правопорушення, яке може розглядатися як шахрайство. В загальному розумінні метою його є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів он-лайн аукціонів, сервісів з переказування або обміну валюти, інтернет-магазинів, де шахраї використовують усіляки методи, які найчастіше змушують користувачів самостійно розкрити конфіденційні дані – наприклад, посилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернеті. Зовнішній вигляд якого зображає дизайн відомого користувачу ресурсу [93].

Відповідно до статті 386 Федерального кримінального кодексу, особа чинить шахрайство, коли обробляє інформацію шляхом обману, користується

помилками або вводить в оману особу з метою отримання фінансової вигоди. У такому випадку відповідний орган призначає тюремне покарання від трьох днів до 12 років, а також штраф у розмірі від 2400 до 24,012 песо. Крім того, такі дії, як шпигунство, змова, злочини проти засобів зв'язку, підслуховування комунікацій, корупційні дії, вимагання та відмивання грошей, можуть розглядатися як загроза безпеці, конфіденційності, цілісності чи наявності будь-якої IT-системи, інфраструктури, комунікацій, мережі, пристрою або даним [320].

Експонентне збільшення кіберпростору призвело до корельованої ескалації злочинної діяльності в Мексиці, зокрема у випадку незаконного злому, крадіжки особистих даних, шахрайства з кредитними картками та експлуатації неповнолітніх. У 2011 р. онлайн-команда активістів Anonymous взяла питання безпеки у власні руки та провела віртуальну виставу у портовому місті Веракрус із картелем Los Zetas. Операція #opcartel або Cartel була створена з метою викриття злочинної діяльності, корупції уряду, викрадення пасажирських автобусів на дорогах та згвалтування.

У 2013 р. Мексика займала позицію номер один у світі за порнографічними матеріалами, в яких брали участь неповнолітні, і друге місце за її виробництвом в Інтернеті. Також наркокартелі були пов'язані з проституцією неповнолітніх. За оцінками 2016-2017 рр., 800 тисяч дорослих та 20 тисяч дітей перебували під загрозою сексуальної експлуатації й стали частиною прибуткової галузі порнографії в Мексиці на суму 30 мільйонів доларів США [385].

Перелік основних статутів та правил, що сприяють кібербезпеці, включаючи закони, що застосовуються до моніторингу, виявлення, запобігання, пом'якшення та управління інцидентами: Конституція Мексики; Федеральний закон про телекомунікації та радіомовлення (FTBL); Федеральний закон про захист персональних даних, який зберігається приватними сторонами (Закон про захист даних), його положення, рекомендації, вказівки та подібні положення про захист даних; Федеральний

закон про прозорість та доступ до публічної інформації; загальний закон про прозорість та доступ до публічної інформації; Загальні стандарти як офіційний стандарт Мексики щодо вимог, яких слід дотримуватися при зберіганні повідомлень про дані; Закон про переговорні інструменти та кредитні операції; Податковий кодекс Мексики; Закон про кредитні установи; Єдиний циркуляр для банків; Закон про промислову власність; Мексиканський закон про авторські права; Федеральний кримінальний кодекс; Закон про національну безпеку; Федеральний закон про працю; Федеральний закон про федеральну поліцію; Національний план розвитку на 2013-2018 рр.; Національна стратегія кібербезпеки 2017 р.; Національна програма громадської безпеки на 2014-2018 рр.; і Національна програма безпеки на 2014-2018 рр. [539].

Оскільки на сьогоднішній день Telegram і Twitter найпоширеніші платформи, то як підтвердження цьому «Нарко-Twitter» (Мексика) – неформальна спільнота акаунтів, які публікують кадри нападів, тіла, послання. У Колумбії 2016-2020 рр. картелі й залишки ФАРК використовували інформаційні кампанії у цих соціальних мережах для дискредитації уряду й спотворення даних про насильство під час мирного процесу, а також активна їхня присутність у TikTok і YouTube, де величезна кількість музичних кліпів, що романтизують «нарколідерів». У фавелас Бразилії наркосиндикати контролюють інформаційні потоки через месенджери, локальні медіа та навіть Wi-Fi-мережі. Інформаційна агресія цілковито використовується для залякування поліцейських і формування «інформаційного вакууму», відтак жителі бояться повідомляти про злочини. Під час пандемії COVID-19 бразильські картелі поширювали власні «інформаційні бюлетені» з наказами, «заборонами», «санітарними правилами», імітуючи державну владу.

Таким чином, напрошується висновок, що в організованій злочинності в обличчі наркокартелів є власні фахівці не тільки в області хімії, військової і банківської справи, але й у сфері інформаційних технологій і пропаганди. Враховуючи величезну кількість ресурсів, якими володіють злочинні

організовані групи не лише в Мексиці, а й у Колумбії та Бразилії мало сумнівів у тому, що вони не набрали експертів із кібербезпеки та «чорних ненависників», щоб встановити їх власні підрозділи цифрової контррозвідки.

Організовані злочинні групи використовують цифрові медіа для своєї користі та контролю, маніпулювання та поширення інформації, а деякі навіть погрожують насильством для тих, хто публікує несприятливу інформацію про їхні організації, а особливо про картелі. Вони не лише замовчують тих, хто «маскується» у соціальних мережах, але прагнуть домінувати над цим простором, зосереджуючись на тих, хто його використовує проти них. Усе це створює певний вакуум, який вони потім використовують для встановлення власної влади, закріплення легітимності, граючи роль своїх конкурентів із негативною пропагандою.

Якщо застосувати пропоновану нами формулу інформаційної стійкості по відношенню до Японії, Китаю та Індії, то отримаємо такі результати як у табл. 4.5.

Таблиця 4.5.

Регіональні оцінки

(Африка / САДК; Латинська Америка; Бразилія; Мексика)*

Країна/блок	КС	ЦК	ІД	ІС	ІСІС	Рівень
Африка (САДК)	0.4	0.55	0.45	0.5	0.48	Низька
Латинська Америка (усереднено)	0.68	0.75	0.6	0.65	0.67	Середня
Бразилія	0.75	0.8	0.65	0.7	0.73	Середня
Мексика	0.6	0.7	0.55	0.6	0.61	Середня

* Джерело: авторська розробка.

У сучасній системі глобальної безпеки інформаційна стійкість набула статусу одного з ключових індикаторів політичної, економічної та соціальної стабільності. Аналіз країн Африки та Латинської Америки засвідчує, що

цифровізація не гарантує безпеки – у регіонах із недостатніми інституційними можливостями або політичними обмеженнями технічний прогрес часто супроводжується зростанням інформаційних ризиків. Зіставлення показників когнітивної (КС), цифрової (ЦК), інституційної довіри (ІД) та інформаційної стабільності (ІС) дозволяє виявити різні моделі формування інформаційної стійкості.

Південна Африка демонструє відносно збалансовану модель із середнім рівнем ICIC (3,0) та високими когнітивними показниками (3,5) (Додаток Е). Розвинена інфраструктура, наявність національних центрів реагування на кіберінциденти та активна участь приватного сектору забезпечують відносну сталість інформаційного середовища. Водночас проблемою залишається нерівномірність регіонального розвитку та обмежені людські ресурси у сфері кібербезпеки. ПАР ілюструє позитивну взаємодію правових, інституційних та культурних чинників, яка дозволяє підтримувати інформаційну стійкість у межах демократичної системи.

Кенія, навпаки, репрезентує низький рівень інформаційної готовності (ICIC 2,5). Попри активну цифровізацію економіки, розширення мобільних фінансових сервісів і зростання кількості користувачів, відсутність ефективної координації державної політики призводить до високої вразливості перед кіберзагрозами. Недостатня когнітивна стійкість населення та обмежена компетентність державних структур у сфері реагування на інциденти спричиняють залежність від зовнішньої допомоги. Це типовий приклад «цифрової модернізації без безпеки», коли технологічні інновації випереджають розвиток інституцій.

Бразилія характеризується середньо-високим рівнем інформаційної стійкості (ICIC 3,2) і найвищими когнітивними показниками (4,0). Державна стратегія кібербезпеки, створення CERT.br, розвиток наукових досліджень і цифрової освіти забезпечують системний підхід до управління ризиками. Високий рівень цифрової компетентності (3,5) супроводжується активною участю приватного сектору у формуванні стандартів захисту критичної

інфраструктури. Попри часті інциденти, Бразилія поступово перетворюється на регіональний центр кіберзахисту, поєднуючи технічні спроможності з правовою модернізацією. Її досвід доводить, що інформаційна безпека потребує не лише технологічних, а й культурних та освітніх складових.

Мексика демонструє низький рівень інформаційної стійкості (2,5), зумовлений поєднанням зовнішніх і внутрішніх чинників. З одного боку, у країні діє національна стратегія кібербезпеки, з іншого – організована злочинність активно використовує цифровий простір для пропаганди, залякування та контролю над територіями. Вплив наркокартелів на інформаційне середовище підриває інституційну довіру та зменшує ефективність державного контролю. Мексиканський кейс ілюструє, як нестабільність безпекового середовища може нейтралізувати навіть формально наявні політики захисту.

Венесуела має найнижчий показник інформаційної стійкості (1,8), що відповідає моделі «режимної стабільності без довіри». Державна монополізація медіа, системна цензура, обмеження доступу до інтернету та відсутність незалежних інституцій формують ілюзію контрольованої стабільності. Низькі значення когнітивної (2,5), цифрової (2,2) та інституційної (1,5) складових відображають системну кризу довіри та деградацію суспільного дискурсу. Цей приклад демонструє, що інформаційна стійкість, побудована на примусі, є нестійкою і не здатна забезпечити легітимність політичного режиму.

Серед аналізованих країн простежуються три типи інформаційної динаміки. Інтегративна модель (Південна Африка, Бразилія): поєднання технічних інновацій, освітніх програм і правового регулювання забезпечує поступове зростання довіри та стабільності. Перехідна модель (Кенія, Мексика): швидка цифровізація без інституційного супроводу створює ілюзорну модернізацію, що посилює вразливість. Авторитарна модель (Венесуела): контроль і цензура генерують «інформаційну стійкість без свободи», у якій стабільність досягається коштом знищення критичного

мислення. Узагальнюючи, можна стверджувати, що ефективна інформаційна стійкість не може ґрунтуватися виключно на технологічних чи силових ресурсах. Її основою є довіра, відкритість, освіта та підзвітність. Саме вони визначають межу між крихкою стабільністю і справжньою стійкістю, що гарантує безпеку в умовах глобальної інформаційної конкуренції.

ВИСН0ВКИ ДО РОЗДІЛУ 4

У XXI столітті інформаційні технології перетворилися на критично важливу основу глобальної взаємодії, державного управління та економічного розвитку. Проте цифровізація зумовила загострення проблем інформаційної безпеки, зокрема зростання кіберзагроз і вразливості інфраструктур. Досвід провідних держав засвідчує, що ефективна інформаційна політика потребує синергії нормативно-правового регулювання, функціональної інституційної моделі, розвитку цифрової компетентності населення, впровадження інструментів кіберстрахування.

США реалізують системну модель забезпечення кібербезпеки, що базується на стратегічному плануванні, створенні профільних органів (CERT, DHS, CISA), розвитку цифрової освіти та взаємодії з приватним сектором. Європейський Союз формує комплексну політику безпеки кіберпростору шляхом нормативного регулювання (зокрема через директиву NIS2), координації через ENISA і розбудови європейської інфраструктури CERT. Приклади Естонії, Франції та Норвегії демонструють ефективність поєднання стратегічного планування, інституційної спроможності та правової визначеності. Узагальнюючи, до ключових компонентів ефективної системи інформаційної безпеки слід віднести: наявність нормативної бази і національних стратегій; інтеграцію державних, приватних і міжнародних зусиль; розвиток цифрової грамотності; функціонування спеціалізованих центрів реагування; активізацію міжнародного співробітництва.

У досвіді Японії, Китаю та Індії простежуються відмінні інституційні моделі. Японія реалізує сервісно-орієнтований підхід, який поєднує державний контроль, механізми саморегулювання та аутсорсинг, хоча і страждає від фрагментарності правового регулювання. Китай використовує кіберпростір як інструмент геополітики: модель «цифрового суверенітету» реалізується в рамках ініціативи BRI через залучення державних технологічних корпорацій, що ставить під сумнів дотримання прав людини та прозорість. Індія, попри високий IT-потенціал, демонструє нерівномірність цифрового розвитку, що послаблює її кіберстійкість, попри формування спеціалізованих органів (DSCI) та ухвалення політик. Сучасна кіберполітика має бути багаторівневою, включати баланс між безпекою і правами людини, стратегічне бачення цифрового суверенітету, міжсекторальну координацію та активну участь у глобальному цифровому врядуванні.

Порівняльний аналіз підходів країн Латинської Америки демонструє схожі виклики: слабку координацію між інституціями, фрагментарне законодавство, нестачу ресурсів та зростаючу вразливість до кіберзлочинності. Мексика та Аргентина перебувають на етапі формування відповідної інституційної архітектури, проте зазнають труднощів з реалізацією. Бразилія намагається поєднати децентралізоване управління з пріоритетом цифрових прав. Колумбія демонструє найбільш системний підхід, однак стикається з проблемою ресурсного забезпечення. Для країн регіону актуальними є такі пріоритети: створення координаційних центрів, уніфікація законодавства за міжнародними стандартами, розвиток цифрової освіти, регіональне співробітництво та інтеграція правових, технічних і організаційних інструментів.

Відзначимо, що Україна може враховувати ці практики для формування власної моделі інформаційної безпеки, орієнтованої на стійкість до гібридних загроз, забезпечення прав людини та інтеграцію до глобального цифрового порядку.

РОЗДІЛ 5
ПРОТИДІЯ УКРАЇНИ ІНФОРМАЦІЙНОМУ ТЕРОРИЗМУ РФ: ВИКЛИКИ, ДОСВІД ТА ПЕРСПЕКТИВИ

5.1. Інформаційна агресія Російської Федерації проти України: етапи, цілі, інструменти

Інформаційна агресія Російської Федерації проти України є невід'ємною складовою частиною гібридної війни, що має системний, багатовимірний і тривалий характер. Її витоки простежують із 2004 р., коли зафіксовано перші масштабні спроби впливу на український інформаційний простір. В умовах загострення геополітичного протистояння інформаційна агресія перетворилася на самодостатній інструмент стратегічного впливу, спрямованого на досягнення зовнішньополітичних цілей Кремля без прямого застосування збройної сили. Ця агресія охоплює широкий спектр деструктивних дій, зокрема системне продукування й трансляцію фейкових наративів, масове поширення дезінформації, проведення кібератак, організацію інформаційно-психологічних операцій (ІПсО), спрямованих на деморалізацію українського суспільства, маніпулятивний вплив на національну ідентичність.

У Доктрині інформаційної безпеки Російської Федерації термін «інформаційна безпека» використовують у широкому змісті й наголошують на стані захищеності національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особи, суспільства та держави загалом [61]. 22 лютого 2017 р. Міністерство оборони РФ оголосило про створення військ інформаційних операцій. З огляду на аналіз попередніх подій, це не створення нових, а легалізація вже давно наявних підрозділів, які володіють достатнім досвідом здійснення кібератак та ведення інформаційних війн.

РФ активно використовує всі свої медійні ресурси у світі. Одним із ключових інструментів інформаційного впливу в ЄС є мережа державних медіа, насамперед RT (Russia Today), яка з 2005 р. позиціонується як канал м'якої сили. RT уключає кілька мовних філій (англійська, іспанська, арабська), окремі офіси в США й Великій Британії (RT USA, RT UK), документальний підрозділ RTD та відеоагентство RUPTLY, що розміщена в Берліні. Спочатку Russia Today створено для покращення іміджу РФ за кордоном, однак згодом канал переорієнтувався на трансляцію критики Заходу. RT активно використовує дезінформаційні методи, транслюючи змови, антизахідні меседжі й проросійську пропаганду (зокрема щодо війни в Україні), і широко представлений на YouTube.

Іншим важливим ресурсом є мережа Sputnik, запущена у 2014 р. Вона охоплює понад 130 міст у 34 країнах світу, веде мовлення 30 мовами й спрямована на посилення російських наративів у міжнародному середовищі. Обидва проєкти фінансуються державою через агенцію RT. Крім того, РФ використовує партнерські формати з провідними західними медіа, як-от Russia Beyond the Headlines, що публікувався у 22 країнах світу 16 мовами в таких впливових виданнях, як The New York Times, Le Figaro, El País тощо.

Особливість інформаційної стратегії Росії – використання суперечливих наративів: Захід водночас зображується як агресивний і слабкий, ЄС – як неспроможна структура на межі розпаду. Такі меседжі спрямовані на делегітимацію європейських інституцій та підрив суспільної довіри. Станом на 27 лютого 2022 р. Європейський Союз заборонив діяльність RT, Sputnik і їхніх дочірніх структур у межах заходів із протидії дезінформації [517].

В українському дискурсі поняття «інформаційної безпеки» вперше визначено в «Концепції (основах державної політики) національної безпеки України», яка була прийнята Верховною Радою України у 1997 р. [182] .У ній ішлося про захист національної безпеки як однієї з найважливіших функцій держави. Інформаційна безпека розглядається, як мінімізація шкоди через неповноту, несвоєчасність або недостовірність інформації чи негативний

інформаційний вплив через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації [172]. Вона передбачає можливість безперешкодної реалізації суспільством й окремими його членами своїх конституційних прав, пов'язаних із можливістю вільного одержання, створення й розповсюдження інформації. Це поняття потрібно також розглядати в контексті забезпечення належних умов існування інформаційних технологій, які включають питання захисту інформації, як такої інформаційної інфраструктури держави, інформаційного ринку, створення безпечних умов існування й розвитку інформаційних процесів. Необхідний рівень інформаційної безпеки забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення й нейтралізацію тих обставин, факторів і дій, які можуть вчинити збиток чи зашкодити реалізації інформаційних прав, потреб й інтересів країни і її громадян [94].

На думку експертів Українського центру економічних та політичних досліджень (УЦЕПД), затверджена парламентом Концепція національної безпеки не виконала функцію базового документа для побудови системи забезпечення інформаційної безпеки держави. Її наступницею стала Доктрина інформаційної безпеки України (2017 р.), розроблена Апаратом Ради національної безпеки і оборони. Документ акцентував увагу здебільшого на тих самих викликах, які постали перед державою ще в 1997 р. Забезпечення національної інформаційної безпеки в ньому пропонувалося здійснювати на засадах інформаційної демократії, що передбачає:

– гарантування свободи створення, збору, зберігання, використання та поширення інформації;

– забезпечення достовірності, повноти й неупередженості інформаційних потоків;

– обмеження доступу до інформації лише на підставі чинного законодавства;

– досягнення балансу між особистими, суспільними та державними інтересами;

– запобігання й нейтралізація правопорушень в інформаційній сфері;

– гармонізацію національного законодавства з міжнародними правовими стандартами;

– підтримку національного інформаційного продукту як пріоритетного елементу [187].

Ще в червні 2017 р. (кібератака NotPetya) росіяни порушили кіберпростір десятків країн світу, але лише на інформаційному полі України активно «відшліфовували» свої злочинні вміння та навички ведення одного з елементів гібридної війни. Кібератаки обставлено як вимагання, однак справжньою метою вірусу було не отримання викупу, а порушення роботи українських держустанов, фінансового та енергетичного секторів економіки. Загалом, наша держава зазнала величезних збитків (найбільше із шістдесяти чотирьох країн), недоотримавши 0,4 % ВВП, що склало майже 10 млрд грн.

До таких утрат, як стверджують окремі вітчизняні аналітики, Україну призвела відсутність на цей час дієвої системи кіберзахисту, зокрема її законодавчого підґрунтя. Так, на думку колишнього голови парламентського комітету з питань інформатизації та зв'язку Олександра Данченка, «країна виявилася неготовою до нападу, причому не готова вже втретє чи вчетверте. Координація між службами відсутня, приватний бізнес узагалі не долучений до системи захисту й ніяк не співпрацює з державними органами» [54].

Певною мірою з політиком можна погодитися. Наприклад, базовий для цієї сфери Закон України «Про основні засади забезпечення кібербезпеки України» готувався, розглядався та вдосконалювався роками. Ще у 2015 р. група народних депутатів із комітету інформатизації та зв'язку подала в Секретаріат Верховної Ради підготовлений нею законопроєкт, коли ж лише в червні 2017 р. він був переведений на повторне друге читання, у цілому ж цей Закон 257-ма голосами «за» був ухвалений лише 5 жовтня 2017 р., а чинності він набирає 9 травня 2018 р. Він визначив організаційно-правові засади

взаємодії державних органів, суб'єктів приватного сектору та громадянського суспільства у сфері кіберзахисту.

Закон започаткував формування належної нормативної бази і є надзвичайно важливим із погляду створення системи кібербезпеки Української держави. До того часу це питання в країні регулювали лише три Укази Президента, одним із яких 15 березня 2016 р. затверджено Стратегію кібербезпеки України [186], а також окремі рішення Ради національної безпеки й оборони (РНБО).

Новий закон запроваджує ще й таке поняття, як Національна система кібербезпеки. Ключовими інституціями стали Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ); Кіберполіція Національної поліції України; Центр реагування на комп'ютерні надзвичайні події CERT-UA (CERT – центр реагування на кібератаки, де команди реагування на інциденти здійснюють управління інцидентами інформаційної безпеки в межах своєї організації або в мережі; завдання – запобігати нападам та підвищувати рівень обізнаності громадян, виявляти потенційні інциденти до фактичного відстеження й вирішувати уже наявні [285]); Рада національної безпеки і оборони України (РНБО), яка координує міжвідомчу політику у сфері кіберзахисту.

Поряд із відповідальними за гарантування кібербезпеки закон чітко визначає й об'єкти захисту від кібератак. Під захист потрапляють комунікаційні системи, якими, зокрема, користуються органи влади та правопорядку, ресурси у сферах електронного урядування й комерції. Крім того, згідно із законом, захищеними мають бути «критично важливі об'єкти інфраструктури» – це низка установ і підприємств у галузі енергетики, інфраструктури, банківського сектору, стратегічних підприємств, перелік яких затверджують Уряд і Національний банк.

У законі йдеться також про так звану «державно-приватну взаємодію» у сфері кібербезпеки. Документ зобов'язує держустанови, підприємства й навіть окремих громадян сприяти органами держбезпеки, повідомляючи, наприклад,

про кіберзагрози. Важливим у цьому законі є й те, що він запроваджує відповідальність, у тому числі й кримінальну, за злочин, учинений саме в кіберпросторі. Перевірка дотримання інформаційної безпеки на критичних об'єктах інфраструктури здійснюватиметься за допомогою незалежного аудиту, що має проходити за стандартами ЄС і НАТО, котрі володіють сьогодні багаторічним досвідом його проведення. Це, безумовно, сприятиме тісній міжнародній співпраці України в інформаційній сфері. Крім того, із 2015 р. наша держава стала активним учасником міжнародних ініціатив у сфері кібербезпеки, зокрема у форматі Trust Fund on Cyber Defence під егідою НАТО, співпраці з Агентством ЄС із кібербезпеки (ENISA), проєктів USAID, а також інтеграційних механізмів ЄС (наприклад EU Cyber Resilience Initiative).

Закон України «Про основні засади забезпечення кібербезпеки», з одного боку, став законодавчим базисом для розробки та розгляду інших документів забезпечення як національної, так і інформаційної безпеки, а з іншого – сприяв створенню в умовах гібридної війни реальних механізмів інформаційного та кіберзахисту у дуже стислі терміни.

Результатом подальшої роботи над забезпеченням інформаційної безпеки України стало схвалення Стратегії інформаційної безпеки у вересні 2021 р. Вона спрямована на формування інформаційного суверенітету, стійкості держави до інформаційних загроз, спроможної ефективно реагувати на гібридні інформаційні впливи, особливо в умовах збройної агресії РФ. Стратегія вдало поєднує національні пріоритети безпеки з європейськими стандартами демократичного врядування.

Її основні завдання:

– протидіяти дезінформації, пропаганді, психологічним операціям;

– захищати інформаційну інфраструктуру, державні інформаційні ресурси;

– розвивати національний контент, підвищувати медіаграмотність;

– забезпечувати кібербезпеку, захист персональних даних;

– формувати систему стратегічних комунікацій держави [185].

Попри здійснені кроки, національна система інформаційного й кіберзахисту залишалася вразливою через низку структурних проблем, серед яких – недостатній рівень підготовки кадрів і відсутність кадрового резерву в державному секторі; фрагментарність міжвідомчої взаємодії; слабкий захист локальних мереж органів державної влади; брак сучасного програмного забезпечення українського виробництва; обмежена обізнаність населення щодо основ цифрової безпеки.

Зазначимо, що значно активізувалася Служба безпеки України у сфері боротьби з кібератаками та кіберзагрозами. У 2017 р. її фахівці відбили близько 50 кібератак різного ступеня ураження, а окремі з них могли бути небезпечнішими за «NotPetya». Основний напрям хакерських кібератак, які, без сумніву, мали російське походження, був спрямований на системи та об’єкти критичної інфраструктури нашої країни, урядові й банківські установи. Однією з найбільших кібератак була WannaCry (також відома як WCry, WCrypt, WannaCrypt, WNCRY та WanaCrypt0r) – комп’ютерний вірус, який уражає операційну систему Microsoft Windows за допомогою шифрування файлів. Вірус атакував урядові й бізнес-структури 12 травня 2017 р. Одним із перших зазнали нападу комп’ютери Іспанії, пізніше вірус поширився також на інші країни. Станом на 17 червня 2017 р. заражено комп’ютери в 150 державах світу та їх кількість неупинно зростала й перевищила 500 000 одиниць. Вимога переказувати гроші зловмисникам перекладена 28 мовами світу [550, с. 37]. Усе це знову ж таки є яскравим прикладом того, як треба створювати умови для фахівців, котрі за потреби можуть захистити державу, зокрема її інформаційний простір.

26 січня 2018 р. у Києві відкрито Ситуаційний центр забезпечення кібернетичної безпеки, створений на базі Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ. Для організації роботи Центру в рамках виконання першого етапу Угоди про реалізацію Трастового фонду Україна–НАТО з питань кібербезпеки Служба отримала

необхідне сучасне технічне обладнання та програмне забезпечення. Ключовими можливостями центру стали система виявлення й реагування на кіберінциденти, лабораторія з комп'ютерної криміналістики. Вони уможливлять ефективні превентивні заходи попередження та знешкодження потенційних кібератак, установлення розробників і їх походження, аналіз для вдосконалення майбутньої протидії, захисту тощо [47].

У лютому 2018 р. відкрито Центр реагування на кіберзагрози Держспецзв'язку (Cyber Treat Response Centre, CRC). Його створено як центральний цілісний компонент і ядро національної системи кіберзахисту України. CRC організовано на основі останніх досягнень у сфері кібербезпеки як вітчизняних, так і провідних IT-компаній світу, сучасні технологічні та аналітичні системи Центру розроблено на рівні найкращих світових аналогів і вже закономірно є одними з найбільш потужних у Європейському Співтоваристві. CRC – це технічна платформа чіткої взаємодії основних суб'єктів забезпечення кібербезпеки (Держспецзв'язку, СБУ, Нацполіції), що на порядок підвищує ефективність й оперативність діяльності правоохоронних структур із протидії та розслідування кіберзлочинів. Ефективний механізм координації зусиль усіх учасників кіберзахисту як державного, так і приватного секторів, який є однією з ключових ланок прийняття оперативних рішень Національним центром кібербезпеки РНБО України [27].

Завдяки унікальним технологічним рішенням цього Центру Держспецзв'язок здатен із великою вірогідністю й точністю здійснювати в режимі «24/7» попереднє виявлення аномальних атак та потенційно небезпечних дій у системах і мережах, підключених до інтернету в державі.

Умовно інформаційну агресію РФ проти України можна розділити на кілька послідовних етапів, що відповідають еволюції методів і стратегічних завдань:

– перший етап (2004–2013 рр.) – період поступового формування проросійського медіаполя в Україні. Основну увагу зосереджено на створенні

позитивного іміджу РФ, поширенні меседжів про «спільність історичної долі», «слов'янську єдність», а також на делегітимізації проєвропейського курсу України. Цей період відзначався активним проникненням російських медіа на український інформаційний ринок, формуванням мережі агентів впливу серед журналістських і політичних кіл, використанням інтернет-ресурсів для формування сприятливого до РФ інформаційного контексту;

– другий етап (2014–2021 рр.) – фаза активної інформаційної війни, яка супроводжувала анексію Криму, розгортання бойових дій на Донбасі та численні інформаційні атаки на Українську державу. У цей період РФ використовувала повний спектр інформаційно-психологічних засобів: створення й поширення фейкових новин, маніпуляції в соціальних мережах через «ботоферми», ретрансляцію наративів культурної та мовної ворожнечі, спрямованих на розкол українського суспільства. Активізувалися російські платформи масової комунікації (RT, Sputnik), що систематично просували викривлену інформацію як усередині України, так і за її межами;

– третій етап (із 2022 р. – дотепер) – повномасштабне вторгнення супроводжується безпрецедентним рівнем інформаційного терору. Росія здійснює постійні спроби деморалізувати населення, посіяти недовіру до влади, дискредитувати Збройні сили України й західних союзників, а також створити хаос через фейки, deepfake-відео, кібератаки та інформаційні диверсії.

Після початку російської збройної агресії у 2014 р. особливу кіберпростір поступово перетворився на один із ключових вимірів гібридної війни, у якому виконується системна деструктивна діяльність, спрямована на дестабілізацію державного управління, підрив функціонування критичної інфраструктури, викрадення інформації, дискредитацію державних інституцій та вплив на суспільну свідомість.

У табл. 5.1 висвітлено перелік численних кіберінцидентів, які за масштабами, методами й наслідками стали прецедентними у світовій практиці. Характерною ознакою зазначених атак була їх інтеграція в загальний

сценарій гібридної агресії, що поєднувала військові, інформаційні, економічні та політичні інструменти впливу.

Таблиця 5.1

Ключові кіберінциденти (2014–2024 рр.)*

Рік	Опис інциденту	Ціль атаки	Тип атаки
1	2	3	4
2014	Атака на інформаційні системи Центральної виборчої комісії під час президентських виборів	ЦВК, державні органи	Злам, фальсифікація даних
2015	Злами урядових сайтів та інформаційна кампанія проти мобілізації	урядові портали, мобілізаційна система	DDoS, психологічна операція
2016	Атака BlackEnergy на енергосистему – масове відключення електроенергії в Івано-Франківській області	Енергетична інфраструктура	Кіберфізична атака (SCADA)
2017	Масштабна кібератака NotPetya, яка паралізувала роботу банків, аеропортів, медіа	Фінансові установи, інфраструктура, медіа	Шкідливе ПЗ (wiper)
2018	Атаки на військові відомства та стратегічні підприємства, спрямовані на шпигунство	Військові структури, оборонні підприємства	Цільове шпигунство (APT)
2022	Масова кампанія DDoS-атак та зламів державних сайтів	Державні інституції, медіа	DDoS, злам, фішинг
2023	Злам та публікація листувань українських посадовців, атаки на Укрзалізницю й обленерго	Транспорт, критична інфраструктура	Інформаційний злам, викрадення даних
2024	Кібератаки з використанням deepfake, спрямовані на дискредитацію влади та дестабілізацію суспільства	Громадська думка, політична стабільність	Дезінформація, deepfake, соцмережі

* Джерело: розробка здобувача.

Виокремимо декілька найрезонаншніших кібератак, що вразили Україну в період із 2014 р. по 2024 р.:

– злам інформаційних систем державних органів (2014 р.): Міністерства оборони, Міністерства закордонних справ, Адміністрації Президента; супроводжувалося витоками конфіденційної інформації;

– кібератаки на енергетичний сектор (2015–2016 рр.). Унаслідок дій хакерської групи «Sandworm» вперше у світі зафіксовано фізичне відключення електропостачання через утручання в промислові системи SCADA;

– масове зараження українських й іноземних комп'ютерних мереж шкідливим ПЗ NotPetya (2017 р.), що спричинило порушення роботи банків, урядових установ, транспортної системи, енергетичних компаній та інших об'єктів критичної інфраструктури;

– акти кібершпигунства й інформаційного саботажу (2019–2020 рр.), реалізовані APT-групами Gamaredon, Fancy Bear (APT28), які здійснювали цілеспрямовані атаки на українські державні, військові та дипломатичні структури;

– масова кампанія DDoS-атак і хакерських зламів державних сайтів після повномасштабного вторгнення (24 лютого 2022 р.), спрямована на критичні урядові інформаційні ресурси. Основними цілями стали вебсайти Кабінету Міністрів, Міністерства оборони, Міністерство внутрішніх справ, Офісу Президента, Національного банку України, а також національні медіа. Атаки були скоординованими, супроводжувалися спробами фішингу та розповсюдженням дезінформації про капітуляцію України. Усе це стало частиною інформаційно-психологічної операції, яка мала за мету дезорієнтувати населення, паралізувати комунікацію й знизити довіру до державних інституцій;

– злам і публікація листувань українських посадовців, атаки на Укрзалізницю та обленерго (2023 р.). Хакерські атаки на електронні пошти й месенджери українських посадовців, із подальшою публікацією компрометувальної або сфабрикованої інформації. З іншого боку, зазнали атак

стратегічно важливі об’єкти – Укрзалізниця та регіональні обленерго, що викликало перебої в роботі інфраструктури, збої в логістиці й постачанні електроенергії. Це були цілеспрямовані кампанії зі сторони російських APT-груп, орієнтованих на виведення з ладу критичних сервісів та деморалізацію населення;

– кібератаки з використанням deepfake, спрямовані на дискредитацію влади й дестабілізацію суспільства (2024 р.). Кількість кібератак із застосуванням технологій штучного інтелекту, зокрема deepfake-відео, на яких українських політиків і військових зображували в контекстах, що мали дискредитувати їх у суспільній думці, значно зросла. Вони поширювалися через соціальні мережі, месенджери та ботоферми, зокрема напередодні ключових політичних подій або на тлі військових утрат. Основна мета – посіяти недовіру до керівництва держави, розпалити паніку, знизити моральний дух населення й підірвати міжнародну репутацію України.

Кіберінструменти, що використовуються Росією, охоплюють широкий спектр дій – від фішингу та фальсифікації листування до використання складного шкідливого ПЗ, бот-мереж, вірусів-вимагачів, deepfake-контенту тощо. Ці атаки часто супроводжуються інформаційно-психологічними кампаніями, які мають на меті підірвати довіру до органів державної влади, спровокувати панічні настрої серед населення та призвести до міжнародної ізоляції України.

Отже, упродовж 2014–2024 рр. кіберпростір перетворився на один із головних фронтів гібридної війни Росії проти України. Цей період засвідчив як глибину вразливостей українського кіберсередовища, так і спроможність держави до інституційного реагування. Успішна протидія сучасним загрозам потребує системного підходу, що поєднує технічні, правові, інформаційні й освітні заходи в межах єдиного національного кіберщита, що має бути інтегрований у європейську та трансатлантичну систему безпеки.

Говорячи про інформаційний тероризм як фактор негативного впливу однієї держави на громадську думку іншої, також зосередимося на

внутрішньому його прояві, прикладом чого можуть слугувати окремі факти, проаналізовані після оприлюднення опитуванням, проведеного Levada Center у Москві в березні 2015 р., де громадяни Росії вважали головними ворогами США (73 %), ЄС (64 %), Україну (55 %), а Білорусь (85 %) і Китай (76 %) навпаки друзями. 50 % росіян підтримували заяви В. Путіна щодо можливості застосування ядерної зброї під час анексії Криму. 49 % вбачали головним досягненням зовнішньої політики повернення Росії статусу «великої держави» [431]. В опитуванні, проведеному цим же Центром у травні 2015 р., звертаємо увагу на такі дані:

– лише 6 % росіян вважали, що війна на сході України триває у зв'язку з утручанням у конфлікт керівництва Росії, яке підтримує «ДНР» і «ЛНР» своїми військами, зброєю та військовою технікою;

– 38 % обрали відповідь: «Навіть якщо в Україні є російські війська та військова техніка, але за нинішньої міжнародної ситуації заперечувати ці факти – правильна політика для Росії»;

– 56 % сприймали те, що відбувається на сході України, як агресію Заходу, яка підтримує війну, щоб послабити вплив Росії у світі;

– 60 % убачали найкращою формою політичної системи в Росії – радянську або нинішній режим Путіна;

– лише 11 % росіян хотіли б жити в демократичному суспільстві західного зразка [431].

Порівнюючи дані Левада-Центру уже після 2022 р., бачимо, що опитування показують погіршене ставлення до США, ЄС; лише ~14 % опитаних у РФ мали позитивне ставлення до Америки. Загальна тональність – негативна. Однак дані 2025 р. свідчать, що Сполучені Штати втратили позицію «найголовнішого ворога», оскільки на перший план вийшли Німеччина, Великобританія, Україна [119]. Щодо позитивного ставлення до країн-«союзниць», то такі держави як Китай та Іран, показують позитивніші оцінки в очах росіян. У 2025 р. зазначено, що серед «друзів» вони все частіше називають Білорусь, Китай, Казахстан, Індію.

Результати опитування щодо війни проти України засвідчили, що відбувається поступове наростання критичності в російському суспільстві, тому що на питання «Війна проти України: чи більше шкоди чи користі?» (2024 р.) 47 % російських респондентів відповіли, що війна принесла «більше шкоди, ніж користі», звідси наступне – «Переговори / мир vs. продовження воєнних дій», нащо реакція була такою: 54 % підтримують переговори, 38 % – за продовження воєнних дій [565].

Підсумовуючи, зазначимо, що в умовах відкритої російської агресії, нових військово-інформаційних викликів Україна, як ніколи, повинна бути готовою в законодавчому, науковому, технічному та військовому плані до забезпечення своєї інформаційної й кібербезпеки. Як свідчить практика, вони можуть бути реалізовані лише за умови узгодження та чіткої координації діяльності в цьому напрямі всіх силових відомств, інших органів і структур.

Володіючи значним внутрішнім потенціалом в особі фахівців інформаційної галузі, а Україна має вдосконалювати систему контролю за використанням власного інформаційного простору та поширювати розповсюдження українського контенту у світі, кардинально збільшуючи фінансові й матеріально-технічні можливості для цього.

Задля забезпечення системного підходу до вивчення інформаційної безпеки України скористаємося SWOT-аналізом, тобто сукупним розглядом сильних і слабких сторін інформаційної війни та безпеки нашої держави (strengths and weaknesses), а також висвітлимо всі наявні її можливості й загрози (opportunities and threats).

До сильних сторін (Strengths) відносимо:

– наявність досвіду протидії гібридним загрозам та інформаційній агресії з боку РФ після 2014 р.;

– активну участь громадянського суспільства й волонтерських ініціатив у сфері кібероборони (наприклад ІТ-армія України);

– співпраця з міжнародними партнерами, зокрема НАТО, ЄС, США, у сфері кібербезпеки та стратегічних комунікацій;

– розвиток нормативно-правової бази у сфері кіберзахисту (Закон України «Про основні засади забезпечення кібербезпеки України» та ін.);

– посилення інформаційної стійкості суспільства завдяки розвитку незалежних медіа й проєктів із протидії дезінформації.

До слабких сторін (Weaknesses) належать:

– фрагментованість державної політики у сфері інформаційної безпеки, відсутність єдиного координаційного центру;

– недостатній рівень кадрового потенціалу у сфері кібербезпеки, відтік спеціалістів за кордон;

– уразливість державних і місцевих IT-систем через застаріле програмне забезпечення та недостатнє фінансування;

– низький рівень цифрової грамотності серед широких верств населення;

– недостатня швидкість реагування держави на нові типи інформаційних атак (deepfakes, ІІ-маніпуляції тощо).

До можливостей (Opportunities) спрямували:

– інтеграцію України в європейський і євроатлантичний простір із запозиченням практик та стандартів кіберзахисту (наприклад NIS2 Directive);

– розвиток національної інфраструктури кіберстійкості й CERT-систем;

– розширення освітніх та наукових програм з інформаційної безпеки, залучення молоді до дослідницьких ініціатив;

– формування державної політики стратегічних комунікацій як засобу захисту від ворожих інформаційних впливів;

– створення інноваційних хабів, інкубаторів і стартапів у сфері кіберзахисту за підтримки міжнародних донорів.

Серед загроз (Threats) виокремили:

– триваюча інформаційна та кіберагресія з боку РФ, спрямована на підрив суспільної довіри, знищення критичної інфраструктури, провокування паніки;

– використання штучного інтелекту й нейромереж для створення високоточних фейків, deepfake-кампаній, маніпуляцій громадською думкою;

– залежність від іноземного програмного забезпечення та хмарних сервісів, що ускладнює контроль за безпекою даних;

– криміналізація кіберпростору: зростання випадків фішингу, шантажу, витоку персональних даних;

– потенційна інформаційна втома суспільства в умовах тривалої війни, що знижує критичне мислення й відкриває шлях до маніпуляцій.

Отже, інформаційна агресія РФ проти України є багаторівневою стратегією, що поєднує пропаганду, фейки, кібератаки та інформаційно-психологічні операції. Вона еволюціонувала від проросійського інформаційного впливу до системного інформаційного терору, що супроводжує повномасштабну війну. Основні цілі агресії – делегітимізація державних інституцій, розкол українського суспільства, деморалізація населення й дискредитація України на міжнародному рівні. У відповідь Україна здійснила низку кроків: запровадження санкцій, оновлення законодавства, створення інституцій з кіберзахисту (CERT-UA, Кіберполіція, Ситуаційний центр СБУ), розвиток стратегічних комунікацій та міжнародного співробітництва у сфері інформаційної безпеки. Проте залишаються й виклики – фрагментарність державної політики, кадровий дефіцит, уразливість IT-інфраструктури та низький рівень цифрової грамотності. Для ефективної протидії інформаційній агресії потрібне посилення кіберстійкості, розвиток медіаосвіти, модернізація інфраструктури, а також поглиблення інтеграції в європейську систему інформаційної безпеки. Тільки системний, скоординований підхід з участю держави, громадянського суспільства та міжнародних партнерів спроможний забезпечити захист інформаційного суверенітету України.

5.2. Стратегічні напрями вдосконалення державної політики протидії інформаційному тероризму в Україні

У межах гібридної війни Російська Федерація здійснює системну, багаторівневу інформаційну агресію проти України, що є невід'ємною складовою частиною її загальної воєнно-політичної стратегії. Цілеспрямовані інформаційні впливи мають стратегічний характер й охоплюють широке коло завдань, спрямованих на підрив національної стійкості, ослаблення демократичних інститутів та формування вигідної для агресора картини реальності як усередині України, так і за її межами.

Серед ключових стратегічних цілей інформаційної агресії Росії проти України виокремлено:

a) дестабілізацію внутрішньополітичної ситуації, провокування міжрегіональних, етнічних, мовних та соціально-економічних конфліктів із метою руйнування національної єдності й мобілізаційної спроможності суспільства;

b) підрив довіри громадян до інститутів влади, зокрема до Збройних сил України, Президента, уряду, парламенту, органів місцевого самоврядування, що створює передумови до делегітимізації влади як такої;

c) вплив на міжнародну громадську думку з метою делегітимізації українського спротиву та нав'язування наративів про Україну як «недієздатну державу» або «інструмент Заходу», що, своєю чергою, має за мету знизити рівень зовнішньої підтримки;

d) розмивання межі між правдою й маніпуляцією, нав'язування суспільству альтернативної картини реальності через поширення дезінформації, напівправди, фейків і теорій змови;

e) зниження рівня міжнародної підтримки України шляхом дискредитації українських лідерів, просування меседжів про «втому від України», «неефективність допомоги» тощо в інформаційному полі країн ЄС і США.

Російський інструментарій інформаційної агресії є надзвичайно різноманітним, високотехнологічним та гнучким. Його основу становлять:

1) державні інформаційні ресурси РФ, зокрема телеканали RT (Russia Today), агентства Sputnik, РИА Новости та інші, які є головними провідниками кремлівської пропаганди на глобальному рівні;

2) масовані кампанії в соціальних мережах, що здійснюються через фейкові акаунти, ботоферми й координовані мережі тролів, які поширюють деструктивні меседжі та підривають інформаційний простір як України, так і інших держав;

3) діяльність спеціалізованих кіберпідрозділів, насамперед APT28 (Fancy Bear) й APT29 (Cozy Bear), які здійснюють цілеспрямовані кібератаки на державні установи, критичну інфраструктуру, медіа, а також злами з подальшими інформаційно-психологічними маніпуляціями;

4) використання агентів впливу в політичному, академічному, журналістському та культурному середовищах як в Україні, так і за кордоном для поширення вигідних наративів;

5) широкомасштабні дезінформаційні операції проти країн-членів ЄС і НАТО, які включають маніпуляції темами безпеки, енергетики, біженців, санкцій тощо;

6) операції інформаційно-психологічного впливу (ІПсО), що мають на меті ослаблення морального духу населення України, стимулювання почуття безпорадності, зневіри в перемозі, нагнітання страху й внутрішньої недовіри.

Отже, інформаційна агресія Російської Федерації є системною, стратегічно вмотивованою діяльністю, спрямованою на підрив основ національної безпеки України. Її успішна протидія потребує не лише технічної модернізації кіберзахисту, а й розвитку національної інформаційної стійкості, зміцнення стратегічних комунікацій і формування критичного мислення в суспільстві.

Отже, інформаційна агресія РФ є прикладом багатокомпонентної, багатоетапної гібридної стратегії, що поєднує традиційні засоби пропаганди з

інноваційними цифровими технологіями. Вона становить системну загрозу не лише національній безпеці України, а й міжнародній стабільності загалом. Складність цієї форми агресії полягає в її прихованості, адаптивності, а також спроможності проникати в демократичні суспільства, використовуючи їх відкритість і свободу слова як вразливості. Саме тому протидія інформаційній експансії Росії потребує розробки комплексних заходів як на національному рівні, так і в межах ширшого міжнародного безпекового партнерства.

Отже, у нашій країні почала кардинально змінюватися тактика кіберзахисту – від реакції на заподіяну від кібератак шкоду до ефективних дій на випередження та максимальної локалізації можливих уражень. Роблячи сьогодні перші кроки в цьому напрямі, держава повинна вивчити кращий досвід країн, які зуміли вийти переможцями в інформаційному протистоянні.

Інформаційно-психологічні операції (ІПсО) у воєнний час є системними, цілеспрямованими діями, спрямованими на формування, зміну або дестабілізацію психологічного стану ворожого населення, військових, лідерів громадської думки та міжнародної аудиторії. Їхня мета полягає в зниженні морального духу, провокуванні хаосу, створенні атмосфери недовіри до власного уряду, а також у мобілізації громадської підтримки серед союзників і нейтральних держав.

Специфіка ІПсО полягає у використанні психологічних тригерів – страху, зневіри, втоми, відчаю, – які підсилюються візуальними образами, маніпулятивною риторикою, фейками та дезінформацією, поширеними через соціальні мережі, медіа або «чутки». Такі операції здійснюються за допомогою мікротаргетингу, бот-мереж, AI алгоритмів, а також через лідерів думок, які свідомо або несвідомо ретранслюють ворожі меседжі. На прикладі російсько-української війни ІПсО мають гібридний характер і поєднують інформаційний, психологічний і навіть економічний компоненти. Російська стратегія включає деморалізацію ЗСУ, дискредитацію українського керівництва, розпалювання паніки серед цивільного населення, експлуатацію тем гуманітарних катастроф або внутрішньої нестабільності. У відповідь

Україна вибудувала власну систему контрнаративів, спрямованих на мобілізацію, єдність, міжнародну підтримку й викриття фейкових кампаній супротивника. ІПсО стали ключовим елементом сучасної гібридної війни, що потребує інтегрованої відповіді на перетині інформаційної безпеки, стратегічних комунікацій і психолого-соціального захисту населення.

Починаючи з 2014 р., збройна агресія Російської Федерації проти України супроводжується масштабною інформаційною кампанією, що є невід'ємною складовою частиною гібридної війни. Системний інформаційний вплив, здійснюваний з боку РФ, характеризується комплексним використанням як традиційних, так і новітніх цифрових засобів комунікації з метою підриву державного суверенітету України, делегітимації українських інституцій, дестабілізації внутрішньополітичної ситуації.

Інформаційна агресія Росії реалізується шляхом цілеспрямованого поширення дезінформації, фейкових повідомлень, маніпулятивних наративів, уключаючи ідеологеми «русского мира» та конспірологічні конструкції на кшталт «зовнішнього управління Україною» або «Українська держава як failed state». Особливу загрозу становить використання інформаційно-психологічних операцій (ІПсО), які мають на меті формування альтернативної реальності в масовій свідомості, підрив суспільної довіри до Збройних сил України, органів державної влади, а також до інститутів громадянського суспільства.

До інструментів інформаційного впливу РФ належать:

– системна дезінформація через соціальні мережі, месенджери, відеоплатформи (зокрема Telegram, YouTube) та інші цифрові канали комунікації;

– створення й поширення проросійських медіаресурсів, зокрема телеканалів та онлайн-платформ (до 2021 р. – «112 Україна», ZIK, NewsOne, «Страна.ua», «Шарій.net» тощо);

– використання бот-мереж і механізмів соціального інжинірингу для імітації громадської думки та деструктивного впливу на суспільні настрої;

– координація кібероперацій за участі груп APT28, APT29 й інших суб'єктів, афілійованих зі структурами військової та політичної розвідки РФ.

У відповідь на зростаючі виклики у сфері інформаційної безпеки, Українська держава сформувала нормативно-інституційний комплекс протидії, що включає:

1. Запровадження персональних санкцій і блокування проросійських інформаційних ресурсів. Відповідно до рішень Ради національної безпеки і оборони України, припинено трансляції телеканалів, пов'язаних із проросійськими політичними колами, а також обмежено доступ до низки інтернет-ресурсів (указ Президента України №43/2021);

2. Удосконалення нормативно-правової бази у сфері медіа. Прийняття Закону України «Про медіа» (2022 р.) передбачає посилення регуляції цифрових платформ, запровадження механізмів моніторингу й відповідальності за поширення шкідливого контенту;

3. Інституціоналізація контролю за інформаційним простором. Національна рада України з питань телебачення і радіомовлення виконує функцію системного нагляду за дотриманням стандартів інформаційної політики, реалізовує процедури контентного маркування та виявляє ознаки інформаційної агресії;

4. Інтеграція в міжнародні механізми протидії дезінформації. Україна є активним учасником міжнародних ініціатив, таких як East StratCom Task Force, EUvsDisinfo, Глобальна коаліція протидії дезінформації, NATO StratCom COE, що дає змогу узгоджувати дії в рамках глобального спротиву інформаційним загрозам.

Важливе значення в забезпеченні інформаційної безпеки має також активність громадянського суспільства, незалежних медіа та волонтерських

ініціатив. Зокрема, проєкт StopFake із 2014 р. здійснює верифікацію й спростування російських дезінформаційних повідомлень; ресурси Detector Media, VoxUkraine, Texty.org.ua забезпечують аналітичний супровід моніторингових кампаній і розвиток медіаграмотності населення.

Попри реалізовані заходи, Україна продовжує стикатись із низкою критичних викликів у сфері інформаційної стійкості, серед яких:

– низький рівень критичного мислення та цифрової обізнаності громадян;

– розповсюдження анонімного контенту в неконтрольованих телекомунікаційних каналах;

– олігархічна залежність низки медіа, що ускладнює формування плюралістичного й незалежного медіапростору;

– повільна інституційна реакція на новітні інформаційні загрози, зокрема пов’язані з deepfak та генеративними системами штучного інтелекту.

Отже, інформаційна агресія РФ є не лише зовнішнім викликом безпеці України, але й чинником, що висвітлює структурні дисфункції вітчизняної інформаційної системи. Ефективна протидія цьому феномену передбачає не лише оперативне реагування, а й довгострокову стратегію, що ґрунтується на інституційній спроможності, прозорості медіавласності, високому рівні медіаосвіти, а також інтеграції в глобальні системи інформаційної безпеки.

Кремль та підтримувані Росією, самопроголошені ЛНР і ДНР через український інформаційний простір проводять потужні маніпулятивні спецоперації. Вони спрямовані на спотворення минулого, викривлення теперішнього й моделювання майбутнього, створення вигаданої доданої реальності в українському суспільстві, а в підсумку – на жорстке управління Україною загалом.

Аналізуємо маніпуляцію як політичну інформаційну обробку суспільної думки в інтересах визначених економічних, соціальних, політичних й інших груп та осіб, як систему засобів інформаційного й психологічного впливу на

свідомість за допомогою масового поширення фейків задля нав'язування певних ідей, цінностей. Досить актуальними є пошук і вироблення механізмів захисту інформаційного простору України від інформаційно-маніпулятивних посягань в умовах, коли Російська Федерація проводить повноцінну інформаційну окупацію.

Довгий час в Україні серйозною проблемою є інформаційна ізоляція окупованих територій. Так, станом на квітень 2015 р. у Донецькій області працювали: 10 новинних і понад 30 загалом російських каналів телебачення; три сепаратистських телеканали – «Оплот», «Новоросия», «Донецкая республика»; сайти – «Новороссия», «Новости Донецкой республики», «Оплот». Політику російських окупантів також ідеологічно забезпечували газети: російські – «Комсомольская правда», «Российская газета»; сепаратистські – «Новороссия», «Донецкая республика» і «Мирный Донбасс»; радіо – «Республика». У Луганській області працювали телеканали – «Луганськ-24» і ГТРК ЛНР – сепаратистський канал, що діє на захоплених потужностях телеканалу ІРТА; провідний сайт сепаратистів – «Луганський інформаційний портал» і сайт «Исток», «Молодежное информационное агенство». Функціонували друковані видання – «Жизнь Луганска»; «XXI век» та «Экспресс-клуб».

У цей час російські канали розповсюджували інформацію маніпулятивного змісту й на територіях, підконтрольних Україні та навіть у деяких прикордонних районах Харківської, Херсонської, Сумської, Чернігівської, Миколаївської та Запорізької областей. Натомість українські канали на окупованих територіях ще не працювали, а на звільнених, підконтрольних українській владі, комунальні й державні ЗМК майже не фінансувалися [78]. Окрім того, деякі регіональні медіа замовчували війну (газета «Донецкие новости», харківська «Время», «Харьковские известия»), деякі видання передруковували інформацію із сепаратистських сайтів («Таймер» (Одеса)).

За результатами експерименту відділу стратегічних комунікацій НАТО (Stratcom, 2019 р.) виявили, як соціальні мережі (маніпулятивний інструмент та потужне джерело (дез)інформації, завдяки якому індустрія фейків постійно зміцнюється) справляються з обіцянками протидіяти маніпулятивним намірам і розповсюдженням фейків на своїх платформах [200]. Практично два роки дослідники активно вивчали здатність соцмереж реагувати на «фальшиву активність»: лайки, кліки та репости. Для експерименту інфлюенсери маніпулювали системою з реклами (більше активності – більша виручка), підвищували популярність замовника (приватної особи) в інтернеті, досить легко знаходили «провайдерів маніпулятивних послуг», які діють відкрито, і все це робилося через несправжні облікові записи, які й формували думки користувачів соцмереж.

Експерт із соціальної комунікації І. Парфенюк виокремив такі фейки («псевдоподії») російських медіа, як подання сюжетів, фотографії подій, що відбувалися в інших військових конфліктах; задіяння в сюжетах людей під виглядом свідків події, якої не було; монтаж різних за часом і місцем подій; поширення неправдивої інформації без посилань на джерело; використання дезінформації та негативної інформації про Україну в інтерв'ю й коментарях відомих людей; поширення неправдивої інформації про історичні події або персоналії; висміювання інформації, яка начебто поширюється для «зомбування» українців [170]. Власне, такі фейки формують негативне ставлення до України, створюють негативний образ українців і зводяться до стандартних звинувачень противника у веденні війни проти цивільного населення – від навмисного вбивства до навмисного руйнування об'єктів цивільної інфраструктури; у знищенні культурних цінностей, культових споруд, спалюванні заповідних лісів; в аморальній поведінці солдатів (зґвалтування, мародерство); у геноциді.

Російські пропагандистські фейки будували дестабілізаційні та деструктивні коди щодо українців: «збройний переворот», «київський режим», «хунта», «дезертирство» – й наголошували на героїзмі Росії («Росія

допомагає братнім народам», «Росія не веде війни», «російська армія благородна та миротворча»). Таким чином медіа штучно формували певні міфи й уявлення, застосовували прийом ціннісної та етичної інверсії, коли злочинця зображують жертвою, а жертва обвинувачується в скоєнні злочину.

Із початком бойових дій на Донбасі комунікаційні стратегії українських, російських і проросійських медіа значно радикалізувалися. Для позначення українських військових у сюжетах застосовуються відповідні слова: «фашисти», «нацисти», «силовики», «карателі», з протилежного боку, образ «іншого/чужого» – «звичайні роботяги», «шахтарі», «трудівники». Низка досліджень на тему «як висвітлюють медіа події на Донбасі» фіксують високий рівень використання мови ворожнечі в російських, українських й особливо в сепаратистських медіа.

У 2017 р. Громадська організація «Донецький інститут інформації» представила свої результати моніторингу масмедіа по обидві сторони лінії розмежування [150]. За її даними, 20 % усієї інформації, яка подається в медіа на тимчасово окупованій території Донецької області містить мову з ознаками ворожнечі («окупанти», «хунта», «укрофашисти», «бандерівці», «п’ята колона», «гейропа», «вишивата», «кати», «вбивці російськомовних» тощо), формуючи з Української держави в цілому та окремих її представників образ ворога. У медіа й соціальних мережах на контрольованій Україною території тієї ж Донецької області, за цими даними, рівень лексики ворожнечі значно менший – 2 % (здебільшого це вирази «терористи», «окупанти», «ватники», «сєпари», «кремлівські маріонетки», «рашисти», «мордор», «лугандон», «колорад») [246].

Ще однією особливістю російських фейків – поєднання «негативних» українців із «Заходом як ключовим ворогом», який веде глобальну геополітичну війну проти Росії. За повідомленнями медіа РФ, саме Захід, США й НАТО ведуть в Україні війну і, як доказ цього, – заголовки до сенсаційних матеріалів: «На стороні України воюють найманці зі США», «В українській армії воюють афроамериканці», «На стороні України воює

польська приватна компанія ASBS Othago», «П'яні американські солдати спричинили бійку в Маріуполі».

У російських інформаційних військах існує окрема стратегія для кожної країни: на міжнародну аудиторію працюють англомовні канали «Sputnik» і «Russia Today», на яких транслюють повідомлення, котрими намагаються вплинути на Е. Макрона, А. Меркель (а потім і О. Шольца), ЄС, США.

У 2016 р. тематика України набирає нового змісту – пропаганду застосовують уже до різних країн – Сирії, Туреччини, ФРН. Це сюжети: «Туркобандерівці: на Україні воюють джихадисти» (телеканал «Росія 24»), «Батальйон «Азов» готовий разом із Туреччиною воювати проти Росії в Сирії» (RT), «За сирійських терористів воюють українці» (nbnews.com.ua).

Негативний наратив «недодержава» – це лейтмотив великої кількості сучасних постів про Україну. Спільним для більшості повідомлень є те, що Україна залежна від США, її економіка в занепаді, а громадяни – «нетямущі». Цікаво, що проросійські користувачі «ВК» «не любили» українських партій із проросійською риторикою. Так, «Опозиційну платформу» критикували за кволу політичну позицію, її членів називали «зрадниками» через недостатнє просування інтересів Росії в Україні [141].

Будучи найбільшим соціальним медіасервісом у кожній великій країні, Facebook із 2016 р. став засобом поширення фейкових новин й іншої пропаганди. Україна також потрапила до цього глобального тренду експлуатації соцмереж у політичних цілях. Тому компанія змушена глобально реагувати на поширення неправдивих повідомлень серед своїх користувачів.

У 2018 р. Facebook посилив правила розміщення передвиборної агітації – політична реклама може бути розміщена лише тими рекламодавцями, які розміщені в цій країні; зобов'язав зазначати замовника й проходити процедуру авторизації. Facebook усе частіше закривав фейкові акаунти, сторінки та групи. Наприклад, у квітні 2018 р. заблоковано понад 270 сторінок і профілів російського «Агентства інтернет-досліджень» (ТОВ «Інтернет-дослідження», відоме в медіа як «фабрика інтернет-тролів»).

Наведемо декілька прикладів фейків російської пропаганди: у жовтні 2018 р. в окупованій РФ Керчі сталися вибух і стрілянина в політехнічному коледжі. Канал «Россия 1» у програмі «60 минут» узяв інтерв'ю начебто в студентки цього коледжу Аліни Керової. Проте дівчина з таким ім'ям загинула [133]. Заборонений в Україні російський «Первый канал» показав розчарованого Євромайданом українця: «Нічого мені особисто не дав Євромайдан. Ось, подивіться, де ми опинилися. Потрібно було дивитися в майбутнє, а ми в майбутньому залишилися без тепла, із дорогою енергією й не зрозуміло, коли все це закінчиться» [174]. Фейковий українець Кирило Чубенко насправді виявився білорусом Віталієм Юрченком. Згодом він розповів, що працював у фірмі, яка на замовлення робить сюжети для телеканалів. Його колеги попросили зіграти незадоволеного українця. На телеканалі всю вину звалили на стрингерів.

Несправжній допис в. о. міністра охорони здоров'я України У. Супрун з'явився у Фейсбуці у 2018 р. Після цього на офіційному сайті Міністерства охорони здоров'я України ввели рубрику «Антифейк», де публікують детальні спростування неправдивої інформації.

Наприклад, фейкову новину також опублікував УНІАН, хоча на перевірку інформації потрібно було лише кілька хвилин. Першоджерелом інформації був російський сайт фейкових новин «Панорама». Ішлося про продавчиню з м. Нижній Новгород (РФ), 62-річну Людмилу, яка під час чемпіонату світу з футболу 2018 р. проколювала презервативи й зіпсовану продукцію начебто продавала іноземним уболівальникам для покращення генофонду [232].

Чимало маніпуляцій у соціальних мережах було з приводу надання УПЦ КП Томосу. Серед топ-фейків 2018 р. – допис ексрегіонала Ю. Бойка про створення Православної церкви України. До цього допис устиг набрати сотні репостів навіть серед журналістів. «Сьогодні найтрагічніший день в історії України – більше ніж за 340 років її існування. Сьогодні Україна померла. Пішов Бог з країни», – так починалось це повідомлення [60]. Також у мережі

з’явився начебто проєкт Статуту нової церкви, хоча точно невідоме походження цього документа. У таких матеріалах «розганяли зраду про не такий Томос і не таку автокефалію». Зауважимо, що ця тактика з’явилася синхронно та із застосуванням маніпуляції «не можна завадити – треба дискредитувати». Основними «пунктами» зради ПЦУ вважали статус митрополії, патріархату; місце в диптиху Константинопольського патріархату; ідею щодо річного Синоду, який функціонуватиме з постійною ротацією; вкиди про те, що «тепер Вселенський патріархат буде всім керувати» і про нав’язування ним офіційної назви церкви; про миро – церковну олію. Цей вкид інформації мав на меті дискредитувати ще не отриману автокефалію і ставив під сумнів наявні церковні традиції [49].

Значну частину дезінформації продукувала сама Українська православна церква (МП), її портал СПЖ (spzh.news/ru/), повністю підконтрольний та підтримуваний Московським патріархатом, й офіційний сайт УПЦ (МП) [216]. У публікації «В Україні одна законна Церква – УПЦ: Синод Грузинської Православної Церкви висловився щодо автокефалії» [24], – ідеться про відвідування 23 червня 2018 р. делегації УПЦ Константинопольського патріарха. Автор публікації свідомо не представив думку члена грузинського Синоду митрополита Чкондидського Петра (Цаави). В оригінальній грецькій новині сказано, що митрополит підтримував ідею незалежної (автокефальної) церкви в Українській державі. Натомість московські церковні діячі інтерпретували ці слова по-своєму: «У розмові з грузинськими журналістами член Синоду Грузинської православної церкви митрополит Чкондидський Петр (Цаава) зазначив, що обговорення питання про автокефалію в Україні почне серйозно обговорюватися після того, як свою позицію висловить Вселенська Патріархія» [303]. Свідомо «не згадали» про те, що митрополит Петр (Цавва) у своєму інтерв’ю грузинському телебаченню, згадав про Патріарха Кирила: «Першоієрарх країни-агресора не має згадуватись у молитвах». Натомість «мирянин Василь» звинувачує представників і симпатиків «ПЦУ» (Епіфанія, Є. Зорю, А. Юраша й

В. Бородянського) у маніпулятивних тезах [146]. А саме про тиск РПЦ і Росії на Помісні Церкви; захист УПЦ своїх прав у судах різних інстанцій називають тиском; прихильники «ПЦУ» ототожнюють релігійну общину з територіальною та таким чином фальсифікують волевиявлення прихожан. Закінчується публікація цілком пропагандистськи – звинуваченням опонентів у перекручуванні фактів із ніг на голову.

Аналітики «Інтерньюз-Україна» провели триетапне дослідження українського сегменту Facebook, Instagram і VK у період парламентських виборів 2019 р. в Україні. Щоб відстежити динаміку й зміну настроїв, вони проаналізували два періоди до дня голосування (1 травня –17 червня та 17 червня –15 липня 2019 р.), 400 постів у Facebook і VK одразу після виборів (22–28 липня 2019 р.) та один період після початку роботи нового складу ВРУ дев'ятого скликання (29 серпня–15 вересня 2019 р.). Вони з'ясували, що:

– Україна потрапила до глобального тренду експлуатації соціальних мереж у політичних цілях. Найполітизованішою серед трьох популярних соцмереж за кількістю постів про українську політику виявилася Facebook;

– в Instagram, на відміну Facebook і VK, зафіксовано найбільший відсоток позитивних та нейтральних постів про українські партії й політиків;

– український сегмент «В Контакті» – сприятливе середовище для жорсткої мови ненависті до України, її політики, суспільства, культури. Це можна пояснити тим, що проросійські журналісти, аналітики, представники влади часів В. Януковича та сепаратисти – найпопулярніші автори «ВК» за кількістю вподобань і поширень. Вони заповнили цю соцмережу презирством до всіх українських партій і політиків.

Треба зазначити, що в Україні вже чотири роки діє заборона на російські інтернет-сервіси, які ще в травні 2017 р. заборонили Kaspersky Lab і Dr. Web, усі сервіси Яндексу, компанії ABBYY, 1C і Mail.ru Group, якій належать соціальні мережі ВКонтакте та Одноклассники.

Ще однією відомою маніпуляцією 2019 р. можна назвати репост заяви каналу «Росія 1» про те, що В. Зеленський дав їм велике інтерв'ю, яке

виявилося брехнею. Його опублікували «Апостроф», «Новое время», «Фокус», «Українська правда» й багато інших. Наприклад, журналісти Liga.net зробили лише один дзвінок прессекретарю В. Зеленського Ю. Мендель, щоб не повестися на фейк. Медіаексперти Liga.net і проєкту «StopFake» запропонували дослідити найпопулярніший фейк російських медіа в листопаді 2019 р. Вони виокремили такі аспекти:

– зміст фейку: у листопаді 2019 р. ведуча телеканалу «Россия 1» О. Скабєєва озвучила сюжет про «суперсекретний план України». Вона заявила, що нова влада України «виношує насильницький план» для Донецька й Луганська. «У мережу потрапив секретний план українського Радбезу. Мешканців окупованих територій, за цим документом, чекає зачистка та тотальна українізація. Хто не розмовляє українською мовою – відправлять до Росії в кращому випадку. У гіршому – силоміць переселять до Львова на перевиховання у бандерівців» [68]. На підтвердження – два аркуші з назвою «проєкт РНБО» за «підписом» секретаря О. Данилова;

– поширення фейку: його передрукували російські медіа: «Комсомольская правда», «ПолитНавигатор», «Наша газета», «РенТВ», ТАСС, сайти терористів у Донецьку й Луганську;

– фейк як продовження фейків: «депортація» мешканців Донецька та Луганська продовжує історію про «поїзди націоналістів», які нібито повинні були їхати в Крим, для перевиховання російськомовних;

– цільова аудиторія, на яку розрахований фейк: на росіян і мешканців захоплених Донецька й Луганська, щоб підтримати негативний імідж України;

– причини активізації фейку: створити перешкоди для мирної реінтеграції Донецька та Луганська в Україну. Фейк виник перед важливою датою – нормандським самітом, щоб «підняти ставки» Росії [98]. Експерти детальніше перевірили фейк і з'ясували, що в шапці «паперу» зазначена стара адреса РНБО – вулиця Командира Камєнєва (перейменована в Петра Болбочана, 2015 р.). Ще один прокол – забули перекласти українською мовою по батькові (ініціали) голови Офісу президента А. Богдана, котрого теж

згадали. Написали: «Богдан А.И.», – замість Йосипович, а не Іосифович. Експерти нагадали, що фейки тиснуть на емоції, їх мета – виключити критичне мислення цільової аудиторії, раціональність і логіку. Тоді той, хто маніпулює, запропонує рішення, яке вигідне маніпулятору, а не споживачу інформації.

Фейк-інформацію про «Офіційний маніфест «жовтих жилетів» на цей раз поширили українські сайти й телеканали, а народні депутати репостили текст у соціальних мережах. У цьому «офіційному маніфесті» протестанти вимагають виходу Франції з ЄС та НАТО – Frexit [169].

Медіаексперт О. Довженко вважає, що «найменше свідомих маніпуляцій у незалежних медіа, які піклуються про свою репутацію – таких як Liga.net, «Новое время», «Українська правда», а набагато частіше вони трапляються у виданнях, які входять до великих олігархічних холдингів. Найбільше маніпуляцій – на ресурсах, що використовують як інструмент політичного впливу або боротьби проросійський ресурс «Страна», сайти Шарія» [59]. Саме вони стають проміжною ланкою для поширення фейків українськими медіа як це було у випадку з придуманим убивством українського військового під Львовом.

У таких інформаційних спецсайтах, хоч офіційно вони подають себе як українські видання, переважно відсутні відкриті дані про власників, наявні лише форма зворотного зв’язку або e-mail. Такі маніпуляції проводять у рамках інформаційної політики власників, які диктують свої правила: із ким дружимо, кого критикуємо, кому допомагаємо чи шкодимо. У потужних медіахолдингах проводиться й централізовано підтримується єдина політика для всіх, наприклад сайт ZIK після купівлі його В. Медведчуком. «Зливними бачками люкс» експерти називають холдинг «Znaj». Тут можуть розмістити свої маніпулятивні та токсичні матеріали практично всі, і користуються цим активно.

Боротись із розповсюдженням фейків надзвичайно складно. Спростування фейків є не найбільш ефективним підходом для боротьби з ними, навіть якщо існують факти й аргументи для їх спростування, досить

легко схилити читачів зайняти позицію оборони та ще глибше повірити в неправдиву історію. Окрім того, якщо повторювати фейк раз за разом, навіть для того, щоби його спростувати, це може надати йому більше ваги й сили.

Спочатку тематичну типологію ключових пропагандистських фейкових тем, які конструювали уявлення та формували прихильників серед російської, української й західної аудиторій запропонували фахівці проєкту «StopFake.org» – сайт для перевірки фактів, запущений у березні 2014 р. Ініціаторами його створення стали викладачі, випускники й студенти Могилянської школи журналістики та програми для журналістів і редакторів Digital Future of Journalism [222]. Вони проаналізували 1000 матеріалів російських пропагандистських видань 2014–2016 рр. і виокремити такі: «Україна, що не відбулася», «Незаконне захоплення влади в Україні» (2014 р.), «Україна – фашистська держава» (2014–2015 рр.), «Росія не є окупантом, а захищає «своїх», «Переселенці та біженці в Росію» (2014–2015 рр), «Територіальний розпад України та «територіальні претензії» сусідніх країн» (2015–2016 рр.), «Занепад світової підтримки України» (2015 р.), «Провальні рішення українського уряду» (2015–2016 рр.) [196].

Створений в Україні Проєкт VoxUkraine (2015 р.) розвиває перший фактчекінговий (англ. *Factchecking* – перевірка фактів) проєкт в Україні – VoxCheck [38], який викриває брехню та маніпуляції в заявах політиків.

У 2017 р. програма ЄС Horizon 2020 профінансувала створення нового плагіну для виявлення фейкових відео. InVID дає користувачеві змогу швидко отримувати контекстну інформацію з відеофайлів у Facebook та YouTube, здійснювати зворотний пошук зображень у пошукових системах, фрагментувати відео, із різних платформ детально досліджувати зображення тощо.

Однак із фейками й маніпуляціями можна боротися. Вважаємо за корисне запропонувати та дотримуватися деяких порад, щоб уникнути їх розповсюдження:

1. Визначити зміст повідомлення. Для цього потрібно прочитати не лише назву повідомлення, оскільки заголовок може бути не пов’язаний із текстом новини або ж не містити даних, котрі підтверджують її правдивість;

2. Оцінити надійність джерела повідомлення (звідки пішла інформація). Незнайомі сайти, заповнені оголошеннями й назвами, написаними капслоком, повинні викликати недовіру, тому потрібно перевіряти через пошукові системи тексти, опубліковані раніше, а також URL підозрілих сторінок;

3. Звертати увагу на дату й час публікації. Поширений елемент фейкових новин – видавати старі публікації за нові. Якщо в новині наявні посилання на інші джерела, то їх треба переглянути, звертаючи увагу на те, коли вони були опубліковані та як у них описано подію, особливо коли йдеться про час;

4. Ознайомитися з автором публікації і його попередніми постами: його бекграунд допоможе зрозуміти, чи справді автор є надійним журналістом, чи не писав він фейкових статей до цього;

5. Ознайомитися з джерелами, на які посилається новина та, власне, місце події. Відсутність посилань або джерел, із яких запозичено заяви, є очевидним сигналом того, що пост може бути фейком;

6. Звертати увагу на те, що зображено й чи відповідає воно подіям, висвітленим у повідомлені;

7. Визначити чи є суперечності у висвітленому повідомлені із Вашими уявленнями, проаналізувати навіщо це поширюють;

8. Ділитися новинами лише тому, що поділяєте думку автора або ж приймаєте одну зі сторін конфлікту, не варто;

9. З’ясувати, що інші видання пишуть із цього приводу. Якщо жодне інше надійне джерело не повідомляє про ці події, то, очевидно, новина є фейковою.

Отже, інформаційно-маніпулятивні посягання Росії в інформаційному просторі України поширюються різними медіа – телебаченням, радіо, онлайн-видання, а найбільше – різними соціальними мережами. Найактивніші пропагандистські медіа – це канал «Росія24», «RT», «LifeNews», «Звезда»,

«1 канал», «Вести.ру», «Известия», «LifeNews», «Новая газета», «Российская газета».

Крім того, на тимчасово окупованих територіях України діє тотальна заборона проукраїнських засобів масової інформації, а в Україні є кілька джерел, які планомірно поширюють повідомлення, співзвучні з російською пропагандою. Найчастіше інтернет-агітатори в соцмережах закликають до зміни державних кордонів України та популяризують терористичні організації «ЛДНР», у них напрацьована певна тематика «фейків» і схеми їх розповсюдження, відомі цілі «фабрики тролів». Постійний монітор за поширенням і спростуванням фейків ведуть українські спецслужби.

Російські ботоферми, самопроголошені ДНР і ЛНР, які позиціонують себе, як демократичне суспільство, в інформаційній війні проти України масово використовували такі теми як «ввічливі люди», «гейропа», «фашисти – каратели – бандерівці», «кіборги». Однак історія про «розіп'ятого хлопчика» та «снігурів» викликали резонанс і зумовили зворотний ефект, а слово «укроп», зі зневажливого ярлика антиукраїнських медіа стало національним брендом.

Ознаками, що можуть засвідчити, що причиною інформації, фото чи новин-фейк є відсутність джерел інформації, застосування анонімних джерел, інформація, узята із соціальних мереж, акаунтів, що не верифіковані, link на підозрілі, маловідомі джерела, дані соціологічних компаній, які не були активними в міжвиборчий період чи помічені у співпраці з політичними силами, недостовірні й повністю вигадані цитати.

Отже, протидія російській інформаційній агресії в українському медіаполі та цифровому середовищі після 2014 р. набула характеру системного й багаторівневого процесу, який охоплює законодавчу, інституційну, технологічну й громадянську складові частини. Масштабність і гнучкість дезінформаційних операцій з боку РФ, що охоплюють традиційні медіа, соціальні мережі, месенджери, бот-мережі та кіберсферу, продемонстрували необхідність формування цілісної стратегії інформаційної

безпеки, орієнтованої не лише на реагування, а й на проактивну стійкість. Оцінка практик, упроваджених Україною у відповідь на ці загрози, свідчить про поступове зміцнення національної інформаційної політики. Серед найефективніших механізмів виокремимо санкційне блокування проросійських медіаресурсів (NewsOne, ZIK, «112 Україна»), заборону на використання російських цифрових платформ («ВКонтакте», «Яндекс», «Mail.ru»), ухвалення Закону «Про медіа», який регламентує діяльність онлайн-платформ, а також активну участь у європейських і міжнародних програмах протидії дезінформації (EUvsDisinfo, East StratCom Task Force, NATO StratCom COE). Ці заходи дали змогу суттєво зменшити вплив ворожого інформаційного контенту в українському медіапросторі. Особливу роль у забезпеченні цифрової безпеки відіграє Національна рада з питань телебачення й радіомовлення, яка реалізовує моніторинг контенту, упроваджує маркування медіа та протидіє поширенню токсичних наративів. Треба також відзначити підвищення ролі державних інституцій у сфері цифрового регулювання, кіберзахисту й захисту персональних даних.

Однак, незважаючи на прогрес, Україна залишається вразливою до інформаційних атак через низку чинників: недостатній рівень критичного мислення та цифрової освіти в суспільстві; залежність окремих медіа від олігархічних структур, що ускладнює їх редакційну незалежність; затримки в оновленні нормативно-правової бази; поширення неконтрольованих анонімних Telegram-каналів та обмежені ресурси незалежних ініціатив. Отже, протидія російській пропаганді повинна розглядатися як довгостроковий стратегічний пріоритет, що потребує скоординованих зусиль держави, громадянського суспільства, освітньої системи, міжнародних партнерів і цифрової індустрії. Лише в умовах постійного оновлення інформаційної політики, інституційної стійкості, зміцнення кіберзахисту та медіаосвітнього середовища можливе ефективне забезпечення інформаційного суверенітету України в цифрову епоху.

Інтегральна модель індикаторів (когнітивна, цифрова, інституційна, стабільність) дає змогу оцінити стан інформаційної стійкості України в динаміці. На основі компаративно,го аналізу держав-референтів можна запропонувати орієнтовну шкалу як у таблиці 5.2. (додаток Ж).

Таблиця 5.2

Стан інформаційної стійкості України у динаміці*

Компонент	Поточна оцінка (2025)	Цільовий показник (2030)	Коментар
Когнітивна стійкість (КС)	0,68	0,80	Розвиток медіаосвіти, критичного мислення, протидія дезінформації
Цифрова компетентність (ЦК)	0,75	0,88	Уніфікація стандартів, упровадження Zero Trust і кіберсертифікації
Інституційна довіра (ІД)	0,62	0,80	Прозорість комунікацій, відповідальність влади, партнерство з громадянським сектором
Інформаційна стабільність (ІС)	0,70	0,85	Розбудова системи реагування, аудити, відновлення після атак
ІСІС (інтегральний індекс)	0,69	0,83	Висхідна траєкторія до рівня високої стійкості

* Джерело: розробка здобувача.

В умовах триваючої гібридної війни підвищення інформаційної стійкості України є критичним чинником забезпечення державної й суспільної безпеки. Вивчення міжнародного досвіду – зокрема США, країн Європейського Союзу, Естонії, Норвегії, Франції, Японії, Індії та Бразилії – дає змогу сформувати набір політико-інституційних і технологічних орієнтирів, релевантних українському контексту. При цьому врахування негативного досвіду Мексики дає змогу уникнути помилок криміналізації цифрового простору й підміни державної політики реактивними заходами.

З огляду на це, рекомендації доцільно систематизувати за п’ятьма ключовими напрямами: інституційна архітектура та координація, технічна модель захисту, правове поле, стратегічні комунікації й освітньо-когнітивний компонент.

У політико-інституційному вимірі досвід США засвідчує, що ефективна інформаційна стійкість неможлива без єдиного центру координації. Створення органу, аналогічного до Агентства з кібер- та інфраструктурної безпеки (CISA), із чітким цивільним мандатом й узгодженням дій із військовим сегментом (за принципом USCYBERCOM) забезпечить системність реагування на інциденти. Європейська модель, представлена діяльністю ENISA та імплементацією Директиви NIS2, доводить необхідність уніфікації вимог до операторів критичної інфраструктури – запровадження регулярних аудитів, ведення журналів інцидентів і чітких термінів їх повідомлення. Приклад Норвегії демонструє ефективність створення національної мережі галузевих центрів обміну інформацією (ISAC) під координацією CERT-UA, що підсилює горизонтальну взаємодію держави, бізнесу й громадянського суспільства.

Технічний компонент передбачає перехід до архітектури Zero Trust, яка, як показує досвід США і Японії, є основою сучасної цифрової безпеки. Упровадження багаторівневої автентифікації, мікросегментації мереж, постійного моніторингу доступів та програмного білого списку постачальників (SBOM) має стати державним стандартом для органів влади й операторів критичної інфраструктури. Уроки Естонії після кібератак 2007 р. підтверджують ефективність щорічних стрес-тестів інформаційної стійкості, що охоплюють як технічний, так і комунікаційний виміри кризових ситуацій.

Правове поле потребує кодифікації понять і процедур у сфері кіберзлочинності. Французький досвід діяльності агентства ANSSI та практика ЄС у межах NIS2 демонструють доцільність запровадження єдиних дефініцій кіберзлочинів і правових норм цифрової форензики. Для України важливо встановити імператив обов’язкового повідомлення про інциденти в

межах 24–72 годин, що забезпечить оперативність реагування й статистичну прозорість. При цьому мексиканський приклад є застереженням від надмірної мілітаризації чи криміналізації цифрового середовища, адже ефективна боротьба з кіберзагрозами можлива лише за умови збереження балансу між безпекою й правами людини.

Вимір стратегічних комунікацій безпосередньо пов'язаний із рівнем інституційної довіри. Європейська практика підтверджує необхідність прозорих кризових комунікацій – регулярних брифінгів, публікації офіційних технічних висновків після інцидентів, а також уніфікованої термінології для запобігання панічним інтерпретаціям. Досвід Норвегії та Естонії свідчить, що участь громадян у моніторингу інформаційного простору (через волонтерські кібергрупи, OSINT-спільноти та фактчек-проєкти) не лише підвищує когнітивну стійкість, а й зміцнює легітимність державних дій. Для України це означає потребу в інституціалізації таких ініціатив у межах етичних рамок співпраці з державою.

Освітній компонент – ключова довготривала інвестиція в інформаційну безпеку. Естонія, Японія та Індія демонструють переваги системного впровадження медіа- й кіберосвіти, що охоплює всі рівні – від шкільної освіти до державної служби. В українських умовах це може бути реалізовано через єдину освітню траєкторію «цифрова грамотність – кібергігієна – професійна компетентність», – доповнену національним тестуванням базових знань для користувачів і сертифікацією для фахівців. Потрібно також використати досвід Бразилії щодо масових антифішингових кампаній, що об'єднують державу, фінансові інституції та провайдерів зв'язку.

Візуально-структурне узагальнення пропонується у формі дорожньої карти підвищення інформаційної стійкості (табл. 5.3), де послідовність етапів має вигляд: «Право та координація» → «Технічні стандарти Zero Trust/SBOM» → «ISAC та обмін індикаторами компрометації» → «Кризові комунікації» → «Освітні траєкторії та антифішинг». Першими мають реалізовуватися рішення, які підвищують рівень інституційної довіри та інформаційної

стабільності, тоді як заходи з підвищення цифрової компетентності та когнітивної стійкості повинні стати постійною складовою політики.

Таблиця 5.3

Дорожня карта підвищення інформаційної стійкості*

Етап	Зміст дій	Цільові індикатори	Очікуваний ефект
1	2	3	3
Право та координація	створення єдиного національного координатора з інформаційної та кібербезпеки (аналог CISA); розробка державної стратегії інформаційної стійкості; узгодження міжвідомчої взаємодії	ІД ↑ (інституційна довіра), ІС ↑ (інформаційна стабільність)	Централізація управління, прозорість, підзвітність
Технічні стандарти ZT / SBOM	Упровадження архітектури Zero Trust; створення профілів SBOM у держзакупівлях; посилення шифрування й MFA в держсекторі	ЦК ↑ (цифрова компетентність), ІС ↑	Єдиний рівень кіберзахисту, уніфіковані вимоги
ISAC та обмін IoC	Формування галузевих ISAC (енергетика, транспорт, фінанси); інтеграція з CERT-UA та платформами обміну індикаторами компрометації (IoC)	ІС ↑, ІД ↑	Скоординоване реагування, колективна безпека
Кризові комунікації	Розроблення протоколів кризових повідомлень; ex-post	ІД ↑	Прозорість уряду,

	розсекречення технічних висновків; єдиний словник і канали брифінгів		підвищення довіри населення
Освітні траєкторії та антифішинг	Масові програми медіа- й кіберосвіти; кампанії проти фішингу; сертифікація держслужбовців із кібергігієни та DevSecOps	КС ↑ (когнітивна стійкість), ЦК ↑	Зміцнення соціального імунітету до дезінформації та шахрайства

* Джерело: розробка здобувача.

Послідовність етапів відображає логіку поступового нарощування стійкості: спочатку зміцнюються інституційні засади (ІД, ІС), далі – технічна й цифрова база (ЦК), а завершальним блоком стає розвиток когнітивних та просвітницьких компетенцій (КС). Отже, дорожня карта поєднує нормативну реформу, технологічну модернізацію й суспільну освіту в єдину стратегічну послідовність.

Індикаторна оцінка України за композитною моделлю (ІСІС = 0,25КС + 0,25ЦК + 0,25ІД + 0,25ІС) (табл. 5.4) свідчить про досягнення середнього рівня (0,70). Найвищі значення зафіксовано у сферах когнітивної стійкості (0,78) та інформаційної стабільності (0,68), що пояснюється високою мобілізацією суспільства й швидкістю відновлення цифрових сервісів після атак. Водночас інституційна довіра (0,60) та цифрова компетентність (0,72) залишаються зонами потенційного зростання. Наявність дисбалансу між довірою та технічною зрілістю є типовою рисою держав, які перебувають у стані трансформації.

Таблиця 5.4

Індикаторна оцінка України за композитною моделлю*

Індикатор	Значення (0–1)	Коротке обґрунтування
Когнітивна стійкість (КС)	0,78	Масова медіаграмотність унаслідок війни, фактчек-спільноти
Цифрова компетентність (ЦК)	0,72	Е-уряд, MFA / шифрування поширені, але ZT не всюди
Інституційна довіра (ІД)	0,60	Військові – високо; цивільний сектор – неоднорідно
Інформаційна стабільність (ІС)	0,68	Відновлюваність є; потрібні єдині правила інцидент-репортингу
ICIC (Україна)	0,70	Середній (верхній сегмент)

* Джерело: розробка здобувача.

Цільові орієнтири для України передбачають поступове підвищення інтегрального ICIC до рівня 0,79 протягом 36 місяців. Очікувані результати повинні ґрунтуватися на комплексному впровадженні дорожньої карти: підвищення когнітивної стійкості – через освітні програми й антифішингові кампанії; цифрової компетентності – через стандартизацію Zero Trust і використання SBOM у державних закупівлях; інституційної довіри – через протоколи кризових комунікацій і публічне розсекречення технічних звітів; інформаційної стабільності – через застосування норм, подібних до NIS2, і проведення національних стрес-тестів.

Отже, стратегічна траєкторія підвищення інформаційної стійкості України має ґрунтуватися на поєднанні нормативно-правової узгодженості, технічної стандартизації, міжінституційної координації та розвитку людського капіталу. Саме ця синергетична модель забезпечить перехід від реактивного

реагування до проактивного управління ризиками, зміцнить інформаційну безпеку держави й дасть змогу досягнути рівня високої стійкості до 2027 р.

У контексті глобальної цифровізації проблема інформаційної безпеки дедалі частіше виходить за межі суто технічного виміру, набуваючи чітко вираженого політичного та безпекового характеру. Інформаційна стійкість держави стає показником її спроможності функціонувати в середовищі гібридних загроз, де інформація застосовується як інструмент впливу, дестабілізації та підриву довіри до інститутів влади. Для України це питання має екзистенційне значення: починаючи з 2014 р., держава перебуває під постійним інформаційним тиском із боку Російської Федерації, що поєднує пропаганду, кібератаки, психологічні операції та маніпуляції в цифровому просторі (додаток З).

Порівняльний аналіз нормативно-інституційних моделей США, Європейського Союзу, Естонії, Франції й Норвегії дає змогу визначити універсальні принципи побудови ефективної інформаційної політики. До таких засад належать, по-перше, чітке правове регулювання у сфері кібер- та інформаційної безпеки, що відображає американську доктрину «захисту за замовчуванням» і передбачає проактивне управління ризиками; по-друге – інституційна координація, яку забезпечують агентства типу CISA чи ENISA, що інтегрують національні CERT-структури та створюють мережеву взаємодію між державою, бізнесом і науковими установами; по-третє – партнерство державного й приватного секторів у межах моделі «public–private resilience», яке передбачає спільну відповідальність за критичну інфраструктуру та обмін інформацією про загрози; по-четверте – розвиток цифрової грамотності населення як елемент суспільної безпеки; по-п’яте – системна протидія дезінформації шляхом підтримки незалежних фактчекінгових ініціатив і платформ моніторингу.

Україна поступово адаптує ці підходи у власній системі інформаційної безпеки. Зокрема, важливу роль відіграють діяльність CERT-UA, Центру стратегічних комунікацій та інформаційної безпеки, Служби безпеки України,

Міністерства цифрової трансформації. Однак, попри наявність позитивних тенденцій, поточна модель інформаційної стійкості залишається фрагментарною: простежено відсутність єдиної координаційної вертикалі, нестачу уніфікованих стандартів звітності про кіберінциденти, а також нерівномірний рівень цифрової компетентності серед державних інституцій і громадян. Ці чинники зумовлюють відносно низькі значення за окремими індикаторами інформаційної стійкості, зокрема в сегментах інституційної довіри та нормативної узгодженості.

Отже, підвищення інформаційної стійкості України потребує не лише технологічного вдосконалення, а й комплексної трансформації політико-інституційної архітектури – переходу від фрагментарних ініціатив до цілісної державної стратегії, що поєднує правове регулювання, міжвідомчу координацію, партнерство з приватним сектором і довготривалу інвестицію в людський капітал.

5.3. Роль інститутів громадянського суспільства у формуванні системи інформаційного захисту держави

Стратегія протидії російській пропаганді є неможливою без широкого залучення громадянського суспільства, зокрема неурядових організацій, аналітичних центрів, журналістських об’єднань і фактчекінгових платформ. Такі проєкти, як StopFake, Texty.org.ua, VoxUkraine, Detector Media, InformNapalm та інші, виконують важливу функцію виявлення та спростування дезінформації, підвищення медіаграмотності громадян, формування контрнаративів. Громадянський сектор не лише доповнює державні ініціативи, але й забезпечує гнучкість й оперативність реагування на нові форми загроз, зокрема використання deepfake, нейромереж і штучного інтелекту.

Із початком військової агресії Росії проти України в 2014 р. державні органи влади – СБУ, МВС, РНБО, МЗС, перші особи держави відразу ж почали

реагувати на інформаційні атаки та маніпуляції зі сторони ворожих медіа, спростовувати заяви й висловлювання російських офіційних осіб. Питання захисту інформаційного простору України, яке до того багато хто вважав відомчим, або вузькогалузевим, стало загальнонаціональним. Громадський сектор також одним із перших виступив на захист інформаційного простору України. Це сприяло напрацюванню нової нормативно-правової бази, створенню нових органів, служб, які реально займалися проблемами захисту національного простору України. Визначення ролі громадських організацій, які активно діють, контролюють інформаційний простір України щодо кіберзахисту, а саме блокування сайтів терористів, що вже давно відбувається за ініціативи окремих волонтерів, патріотично налаштованих власників та керівників українських провайдерів, постало нагальним питанням дослідження.

Сучасні події засвідчують, що в питанні інформаційного протистояння держава не завжди є гарантом захисту своїх громадян і критичних структур, тому особливе значення має діяльність громадських організацій – добровільних об’єднань фізичних осіб та/або юридичних осіб приватного права для здійснення й захисту прав і свобод, задоволення суспільних, зокрема економічних, соціальних, культурних, екологічних та інших інтересів [70].

За своєю суттю й призначенням будь-яке суспільне об’єднання / громадська організація є некомерційним, що не зорієнтоване, передусім, на отримання прибутку, а функціонує для зовсім інших цілей. До основних функцій громадських організацій належать:

– захист прав і свобод особистості, людини й громадянина;

– розвиток політичної активності та самодіяльності людей;

– залучення громадян до управління громадськими й державними справами.

Серед активних громадських організацій, які контролюють інформаційний простір України, треба згадати Центр комунікаційно-контентної безпеки, Партнерів цифрового правозахисту, Національну спілка

журналістів України, Донецький інститут інформації, Громадське телебачення Донбасу, Академію української преси, Інститут розвитку регіональної преси, Інтерньюз-Україна. Громадська організація «Інтерньюз-Україна» за підтримки Центру інформації та документації НАТО в Україні реалізовує проєкт «Розповсюдження українського досвіду протистояння гібридним загрозам» [254] й ін.

Ми зосередимо свою увагу на таких громадських організаціях, як НотаЄнота, Центр стратегічних комунікацій StratCom Ukraine, CAT-UA, Українські кібервійська, Детектор медіа, Інформаційний спротив, Інформаційний центр «Майдан Моніторинг», Українські кібервійська, InformNapalm, Лабораторія цифрової безпеки, StopFake, які, на нашу думку, є найефективнішими й дієвими в українському інформаційному просторі.

Одне з головних завдань російської пропаганди – створювати додаткове протистояння в Україні. Тому низка організацій, таких як Інститут масової інформації (1995 р.), «Internews» (1996 р.), Detector Media (2004 р.), проводять регулярні моніторинги достовірності та дотримання журналістських стандартів, визначають лідерів й аутсайдерів серед онлайнових медіа. ГО «Детектор медіа» публікує щорічні звіти-підсумки про наявність маніпуляцій у діяльність телевізійних каналів України [59]. Отже, можна спостерігати, що маніпуляції в інформаційному просторі нашої держави здійснюють не лише закордонні видання, а й вітчизняні медіаресурси, кінцевими власниками яких є відомі українські олігархи, які визначають їхню редакційну політику й підтримують певні політичні партії. Крім того, ГО «Детектор медіа» пояснює для української аудиторії, які новації, документи запроваджують країни світу для захисту свого інформаційного простору.

Громадська організація «Інформаційний центр “Майдан Моніторинг”» (2000 р.), ще в грудні 2013 р. наголошувала на важливості інформаційної війни в Україні, перша в лютому 2014 р. почала допомагати й учити людей, організації, установи організовувати протидію спеціальним інформаційним операціям для збереження їх цілісності. Організація взяла на себе завдання

спростування інформації, а також підготувала посібник із безпечної поведінки в сервісах соціальних мереж [252]. У його сатиричній версії викладено такі поради: «1. Ніколи не дивися на дату публікації, усі публікації в інтернеті створені хвилину тому й тому є актуальними! 2. Ніколи не дивися на джерело інформації. В Інтернеті не бреше ніхто, тому джерело неважливе, усі джерела – надійні! 3. Ніколи не перевіряй інформацію про людей. Якщо хтось пише про незнайому тобі людину, то він точно не бреше, тому треба сліпо вірити! 4. Побачив новий тест, обов'язково пройди його й покажи всім друзям, щоб ФСБ мало інформацію не тільки про тебе, а й про них!» [252].

Центр стратегічних комунікацій StratCom Ukraine – неурядова організація, яка працює над реформою комунікацій державних інституцій України, підвищенням професійного рівня комунікаторів і створенням сучасних підходів до публічної комунікації. Його місія – підтримати Українську державу в упровадженні ефективного управління комунікаціями та підвищенні професійних стандартів; зробити комунікації однією з ключових функцій державного управління. За даними офіційного сайту, НУО співпрацює з дев'ятьма країнами, має понад 500 медіаконтактів, 50 реалізованих проєктів, 45 партнерів, а також дев'ять років досвіду [238].

Основні напрями роботи – дизайн комунікаційних систем і процесів у державних організаціях через створення або реформування підрозділів комунікації, використання стратегічного підходу; розробка власних інформаційних кампаній, SMM, відео, фото контенту, медіааналізу, а також проєктів «Corruption in the army kills», конкурсу військової фотографії, «Army. Second Birth»; тренінги й навчання для державних і громадських комунікаторів, а саме медіатренінги, практикуми з комунікації з медіа, річне планування комунікацій.

Організація виникла як відповідь на потребу модернізації державних комунікацій (частково в контексті інформаційної війни) і поступово розширила масштаби від одного-двох проєктів до системного дизайну комунікаційних процесів. На сьогодні перспективними є зростання кількості

міжнародних партнерств (Велика Британія, США, країни Балтії), залучення досвіду з-за кордону, перехід від окремих кампаній до моделі «системних змін» у державному комунікаційному полі (трансформація підходів, структур комунікаційних підрозділів).

Проєкт «Corruption in the army kills» – інформаційна кампанія, спрямована на висвітлення наслідків корупції в армії (згадано на сайті); конкурс української військової фотографії – як інструмент комунікації армії, громадянського суспільства й медіа; тренінги-практикуми для комунікаторів держпідрозділів – підвищення спроможності реагувати на кризові й інформаційні виклики [238], усе це стало можливим завдяки сильним сторонам діяльності НУО, а саме орієнтації на державний сектор із великою зоною впливу (держоргани, армія, громадський сектор), здатності працювати на системному рівні – не лише кампанії, але зміна процесів, міжнародному досвіду й партнерству, що підсилюють кредибілітет.

Центр StratCom Ukraine відіграє важливу роль у модернізації України як комунікаційно-освіченої держави, особливо в умовах інформаційної війни та гібридних загроз. Робота на системному рівні, інтеграція міжнародного досвіду й фокус на держкомунікаціях роблять його цінним актором. Попереду – виклики забезпечення сталого впливу (вимірюваного, реального) й адаптації до постійних змін інформаційного середовища.

Серед українських громадських організацій, які також цілодобово протистоять Росії в кібервійні з Україною, є патріотично налаштовані вебфахівці, об'єднані в ініціативу «Українські кібервійська» («УКВ», 2014 р.). Операції «УКВ» у кіберпросторі є досить ефективними в реальному житті – блокування електронних рахунків і сайтів сепаратистів, отримання доказів із серверів державних й урядових органів РФ про присутність російських військових в Україні. «Українські кібервійська» провели декілька операцій – «Кіберштурм», «Кібераураган», «Заблоковані виродки». У серпні 2017 р. операція «Відплата» – блокували сайти терористів DoS-атаками, щоб вони не працювали: без-вести.рф, white-book.info, dnrpress.ru, bratstvo-lg.ru, ungu.org,

rv.org.ru, cik-lnr.info, cikdnr.ru, pravdatoday.info, voicedonbass.ru, bne.su, lvs-global.ru, slemtt.myjino.ru, molotpravdu.com, europeanfront.info, новорус.рф, novorossia.co, novorossia.tv, nol.su, dnrepublic.info, ukrnovosti.info, donetsk-gov.su, k61.donetsk.ua, ntribunal.mcdir.ru, ntribunal.su, batalyonmoskva.ru, icp.su, interbrigada.org, особистий кабінет платника податків ДНР, dokcpp.dn.ua, antiukrop.su, gazeta-dnr.ru, milion.kiev.ua, banner.dn.ua [230].

У перший рік агресії «УКВ» остаточно заблокували 40 сайтів загрозливого, фейкового контенту чи терористичного спрямування, зламали десятки сайтів терористів «ДНР» і «ЛНР», зокрема, «ЦВК ЛНР», узяли під контроль двісті вебкамер Донбасу, Криму та Москви, закрили 144 акаунтів у електронних платіжних системах. Організація склала список сотні сайтів терористів, які українські провайдери закривати не хочуть, вимагаючи рішення суду. Зломи сайтів пошти різних органів і серверів МВС РФ, партії «Єдина Росія» в різних областях, партій сепаратистів, дали змогу знайти докази участі російських військових у боях на Сході України [132]. «Кібервійська» виявили діяльність групи хакерів «Кіберберкут», «Novorussian Cyber Army», які вважаються проєктами ФСБ та проводять активну інформаційну війну проти України. У рамках окремої операції «Крим – це Україна» закрили десять кримських державних сайтів, які були захоплені терористами.

Навесні 2018 р. «УКВ» визначили географічні координати бази (ангару) в окупованому Луганську, де розміщено військову техніку бойовиків. Активісти передали дані про терористів СБУ і волонтерам, котрі працюють із ЗСУ. Хакери «УКВ» заблокували 445 рахунків, на яких збирали кошти для терористів з усього світу – на суму близько 19 млн доларів США [3].

Серед проблем діяльності «УКВ» – нестача досвідчених хакерів. Для блокування акаунта терориста в соціальній мережі Facebook чи Twitter, потрібно, щоб сотні тисяч людей написали на нього скаргу. Лише тоді буде реакція: на декілька прохань великі соціальні мережі станом на кінець 2021 р. реагували дуже повільно.

Міжнародна волонтерська розвідувальна спільнота «InformNapalm» (2014 р.) активно займається OSINT-розслідуваннями (англ. – *Open source intelligence* – розвідка з відкритих джерел), що ґрунтуються на аналізі інформації із загальнодоступних, відкритих джерел, у тому числі соціальних мереж. Варто зазначити, що організація має найбільші відкриті бази даних щодо російської військової агресії у світі. Результати досліджень використовуються світовими масмедія, матеріали презентують на сесіях у ПАРЄ, НАТО й ОБСЄ.

За чотири роки (2018–2021 рр.) представники «InformNapalm» значну увагу приділяли ситуації в Україні та її впливу на інформаційну безпеку країн світу. Улітку 2017 р. вони заявляли, що в армії РФ існує низка проблем і що її збройні сили перебувають у незадовільному моральному, фізичному і технічному стані, так це стало помітно під час участі росіян у військових кампаніях проти Грузії, Сирії й України [226].

Волонтери «InformNapalm» отримали фотодокази присутності на окупованих територіях Донецької та Луганської областей сучасних російських комплексів радіоелектронної боротьби (РЕБ), які терористи намагалися заховати під маскувальними сітками [39]. У листопаді 2019 р. розвідувальна спільнота опублікувала резонансне розслідування волонтерів про російську операцію захоплення українського Криму. Подробиці дослідження в студії UA.TV розповів речник «InformNapalm» М. Макарук, який у розмові згадав про пошту одного з високопоставлених офіцерів служби тилу Південного військового округу РФ, а також про документи, які чітко пов’язували відрядження великої кількості солдатів у невідомому напрямку.

Українські волонтери, узявши до уваги дані з відкритих джерел, почали поетапно ідентифікувати прізвища та встановили, хто саме захоплював Крим, яким чином російські військові потрапляли на півострів, визначили чотири шляхи: 1. Траса Сімферополь–Харків (військові були одягнені в цивільний одяг, приїжджали рейсовими автобусами, легковими авто); 2. Пором, на фото з якого були БТР-72У, які виготовляють тільки у РФ; 3. Траса Керч-Феодосія;

4. Російську військову техніку завозили на кораблях Балтійського, Північного та Чорноморського флотів [211].

Спільнота «InformNapalm» активно співпрацює з активістами кібервійни в Україні – Українським кіберальянсом, активістами хакерських груп «FalconsFlame», «Trinity», групою RUH8 та хактивістами групи «КіберХунта». Кіберактивісти передавали дані, добуті в результаті зламів ресурсів агресора, спільноті для аналізу й подальшого оприлюднення. Зважаючи на резонансну діяльність організації, яку телеканал «Аль-Арабія» порівняв із публікаціями «WikiLeaks», Федеральна служба РФ з нагляду у сфері масових комунікацій і зв'язку (Роскомнагляд) у липні 2019 р. заблокувала доступ до сайту «InformNapalm». Він став першим серед ресурсів OSINT-розслідувань, які досліджують участь РФ в агресії проти України [197].

StopFake – це ініціатива з фактчекінгу, заснована у 2014 р. як відповідь на сплеск дезінформації, зокрема в умовах анексії Криму та початку гібридної агресії з боку РФ; сайт, який виріс зі студентсько-викладацької групи НаУКМА (м. Київ) і журналістів. Місія – перевірка фактів, підвищення медіаграмотності, створення архіву пропаганди та фейків [515].

Основні напрями діяльності: фактчекінг – систематичне спростування дезінформації, переважно про Україну та її конфлікти («Fake: Ukraine Mines Western Border – Fox News»); медіаосвіта (навчальні поради для аудиторії «How to Identify a Fake»); моніторинг й аналіз пропаганди (архівування та дослідження пропагандистських наративів); міжнародна співпраця.

Реалізацію діяльності простежено через розгорнуті кейси-спростування (відео, яке стверджувало, що військові України розстріляли цивільного за відмову казати «Слава Україні»), великий перелік публікацій «Fake: …» на сайті; аналітичні публікації (дослідження механізмів дезінформації «A Year of Lies: Russia's Information War Against Ukraine») [355].

StopFake почався як волонтерський проєкт, але з часом став впливовим гравцем у сфері інформаційної безпеки. Завдяки своїй роботі, здобув визнання як в Україні, так і за кордоном – проєкт називали «золотим стандартом»

боротьби з дезінформацією. У контексті повномасштабного вторгнення РФ у 2022 р. діяльність StopFake стала ще більш критичною для інформаційної стійкості країни.

StopFake працює як один із ключових механізмів інформаційної оборони: він не замінює державну комунікацію, але допомагає створити середовище де-дезінформації, підвищити медіаграмотність громадян і збільшити прозорість інформаційного простору. В умовах гібридної війни проєкт відіграє роль «триксу» (перевірки) та «сигналу» (індикатора наративів, які треба відслідковувати).

Головним завданням групи «Інформаційний спротив» (2014 р.) є протидія зовнішнім загрозам в інформаційному полі, які виникли в Україні в воєнній, економічній, енергетичній, інформаційній сферах. Координаторами проєкту стали офіцери запасу, переважно колишні військові кореспонденти (Д. Тимчук і Ю. Карін). Він публікує аналітику, підготовлену власними експертами (ГО «Центр військово-політичних розслідувань»), так і запрошеними вітчизняними, іноземними експертами з неурядових структур та міжнародних організацій.

Члени групи постійно інформують громадськість про результати дослідження чи аналізу фактів і доказів на офіційних вебсторінках групи (українською, російською й англійською мовами), у мережі Facebook, на особистих сторінках членів групи в соціальних мережах. Аналізуючи найвідоміші розслідування групи, а саме «РПЦ – ФСБ – інструмент Кремля не лише на духовному фронті», «Гібридний український мир у соціальних мережах», зазначимо, що простежено готовність до подальшої активної співпраці з місією ОБСЄ на південному сході України й збір доказів щодо незаконної там присутності Збройних сил РФ, озброєння та військової техніки російсько-терористичних військ.

Широко відомий соціальний проєкт групи – «Пам’ятаємо. Пишаємося. Переможемо!» [2] (2015 р.), про історію двох поколінь українців – часів Другої світової війни і сучасних «кіборгів», спрямований проти російської

пропаганди й спекуляцій стосовно святкування Дня Перемоги, учасників, ветеранів і нагород Другої світової війни. Він набув широко резонансу, функціонує й досі, а також зібрав і низку «хейтерів».

Відома своєю діяльністю в українському інформаційному просторі громадська організація «Лабораторія цифрової безпеки» (2017 р.) [117], де спеціалісти з аналізу даних, юристи допомагають журналістам, громадським активістам, правозахисникам вирішувати проблеми цифрової безпеки, сприяють реалізації прав людини в Інтернеті через вплив на державну політику у сфері цифрових прав. На підставі досвіду проведення тренінгів й індивідуальних консультацій члени організації з'ясували, що користувачі через складність пристроїв, сервісів, захованість певних безпекових функцій в інтерфейсах, зазвичай не знають про їх існування, а тому не вміють їх самостійно налаштувати. Для розв'язання цієї проблеми вони створили сайт «Як» – проєкт реалізований за підтримки «Counterpart International». Ресурс містить покрокові поради з налаштування комп'ютерів, мобільних пристроїв та сервісів (Windows, MacOS, Android, iOS, Telegram, Twitter, Facebook, Gmail, WhatsApp. Сайт «Як»), дає змогу налаштувати двофакторну аутентифікацію, сповіщення про вхід, відновити обліковий запис, пояснює про фішинг, додатки, шифрування, антивірус, закриті сесії, секретні чати [251].

Однак траплялися випадки, коли громадські організації, які контролювали інформаційний простір України, перешкоджали його функціонуванню. У травні 2016 р. Центр Миротворець розпочав «повномасштабну бойову операцію з очищення інформаційного простору України від російської брехні, маніпуляцій, системної антиукраїнської діяльності в медіа. Проте 10–11 травня 2016 р. цей сайт опублікував списки журналістів, акредитованих у терористичній організації «ДНР» [210], що викликало негативну реакцію вітчизняної журналістської спільноти, організації «Репортери без кордонів». Адже журналістів CNN, BBC, Reuters, Assosiated Press звинуватили в «пособництві терористам» й після викладу персональних даних, номерів телефонів, електронних адрес їм почали

телефонувати та писати із погрозами, а від деяких українських політиків звучали заклики «вважати цих журналістів «ворогами України» і взагалі закрити їм можливість працювати» [26]. Таке ставлення до журналістів було грубим порушенням Конституції України, Закону України «Про захист персональних даних», порушенням Європейської конвенції прав людини.

У «Заяві журналістів щодо оприлюднення бази контактів сайтом «Миротворець», яку опублікувала головний редактор інтернет-видання «Українська правда» і під якою свої підписи поставили декілька десятків журналістів, зазначалося, що саме завдяки роботі українських і закордонних журналістів, акредитованих на окупованих територіях, суспільство дізналося «з кого складається батальйон «Восток», про злочини Мотороли, саме ці журналісти дали інформацію для якісного розслідування про падіння малазійського «Боїнга» влітку 2014 р., їх матеріали про керівний склад окупованих територій лягли в основу багатьох розслідувань та аналітичних матеріалів. Журналісти вимагали негайно видалити з вільного доступу інформацію про персональні дані відповідних журналістів [152]. Отже, рішення сайту «Миротворець» викликало протидію зі сторони інших громадських організацій, засвідчило різне розуміння інтересів і захисту інформаційного простору України.

ГО «НотаЄнота» громадська ініціатива, яка реалізовує освітній, просвітницький проєкт у формі антифейкової інтелектуальної гри з метою підвищення медіаграмотності та критичного мислення серед молоді (віком ~13–18 років) й освітян [7]. Основна ідея полягає в тому, щоб через гру навчити розпізнавати фейки, маніпуляції, впливи в інформаційному просторі, показати, як вони працюють, навчати використанню критичного мислення. Формат – командна гра (5–6 раундів, 90–110 хв) із завданнями-кейсами, фото, відео-каналами, логікою, ребусами. Авторкою стала Альона Романюк – фактчекерка, редакторка, викладачка журналістики, яка й вивела ініціативу на сучасний рівень, пройшовши етапи запуску (літо 2021 р. – початок 2022 р.) антифейкового квізу «НотаЄнота»; розширення формату, коли з одного квізу

перетворюється на серію раундів, із розробленими понад 1 250 завданнями та 30+ тематичними розділами, заявленими 70 000+ учасниками [212]; упровадження в освітню сферу з активним проведенням курсів для освітян, розробкою методичних матеріалів для шкіл, інтеграцією гри в навчальні заходи й, нарешті партнерства з коледжами, громадськими структурами, програмами підвищення кваліфікації педагогів і т.ін.

26 березня 2024 р. запустили, курс для освітян із проведення антифейкових ігор «НотаЄнота», де участь брали вчителі, бібліотекарі з кількох областей, курс уключає п’ять ігор, роздаткові матеріали та сертифікацію. 9 травня 2024 р. виходить друга гра проєкту «НотаЄнота»: тема «Історичні фейки і не тільки».

Перевагами є, власне, формат інтерактивної гри, який підвищує залучення учасників; орієнтація на реальні кейси й фейки, що значно підвищує актуальність у контексті інформаційної війни; освітня інтеграція. Щодо викликів, то треба зазначити підтримання актуальності матеріалів, оскільки інформаційне середовище швидко змінюється, тому потрібно оперативно оновлювати кейси, а також залучення достатньої кількості ресурсів (людей, фінансування) для охоплення більшої кількості шкіл/регіонів, щоб мати можливість подальшого розвитку й розробки онлайн-версії або мобільного додатка гри, що дасть змогу охопити більшу аудиторію (особливо під час дистанційного навчання).

CAT-UA – громадська організація, яка починалася як волонтерська аналітична група в перший день повномасштабного вторгнення (24 лютого 2022 р.) зі скануванням, моніторингом й аналізом медіа, соціальних мереж для підтримки військових і цивільних структур [305]. Місія – прозорі, сучасні принципи і формати комунікації в Україні, щодо нашої держави за кордоном; дослідження маніпуляцій, оманливого впливу й інформаційних спецоперацій. Напрями діяльності – моніторинг й аналіз медіа, соцмереж, а саме аналіз контенту, наративів, настроїв в соцмережах щодо війни, інформаційних кампаній; звіти, тобто регулярні публікації «зведень з

інформаційної війни», про те, що сталося, які меседжі домінують, які тренди у соцмережах; аналітичні дослідження – напрацювання теоретичних підходів (PR-Message Analysis) для аналізу комунікаційних кампаній; підтримка, консультації державних або громадських структур, надання їм аналітичної інформації, яка може бути використана в державній комунікації чи протидії маніпуляціям.

CAT-UA є важливим елементом сучасної інформаційної стійкості України: через аналіз соцмереж і наративів вони дають змогу розуміти, як формується громадська думка, як працює ворожа пропаганда, які меседжі мають ефект. Дослідження «National narrative: three visions of Ukraine» – оприлюднене 21 березня 2024 р. [265], де CAT-UA аналізує три різні наративні моделі, які існують в українському інформаційному просторі. Звіт від 27 вересня – 3 жовтня 2025 р. про аналіз соцмереж українців: «Українців сколихнула надія на «Томагавки»» тощо.

Активно функціонують групи й сторінки в соціальній мережі Facebook, які об'єднують радикально налаштованих проти українців поляків – (2018–2019 рр.) «Ukrainiec nie jest moim bratem» (66 тис. підписників), «Lwow jest polski» (39 тис.), «Pamietam Wolyn» (29 тис.) [151]. Завдяки роботі українських активістів «Кіберхунти» та «Українського кіберальянсу», до рук волонтерів «InformNapalm» потрапив скриншот пошти одного із «сірих кардиналів» російської зовнішньої політики в Європі О. Усовського. Цей громадянин Білорусі, прибічник «руского міра», активно займався організацією антиукраїнських акцій, провокацій у Польщі, країнах Східної Європи [145].

Після початку війни в Україні активного впливу російської пропаганди зазнають держави-сусіди, насамперед Республіка Польща. У 2014–2018 рр. польський блогер-розслідувач М. Рей вів блог «Російська п'ята колона у Польщі», який зібрав аудиторію понад 200 тис. підписників. Блог стосувався російського впливу на інформаційний простір Польщі та польську політику щодо українців та посилення ворожого ставлення [181]. Найбільше статей із відверто антиукраїнськими гаслами та закликами до ворожнечі між поляками

й українцями опубліковано в «SputnikNews» і Kresy.pl. Саме ці прокремлівські видання, маніпулювали твердженнями, що українці приїжджають та забирають у поляків роботу, гальмують зростання зарплати в Польщі, про «неймовірну злочинність» наших громадян [204]. У дописах Kresy.pl ішлося про теорію, що польський платник податків змушений буде із власної кишені утримувати українських заробітчан на пенсії в Польщі. Міністерство соціальної політики РП змушене було неодноразово спростовувати такі твердження [9].

Інформаційна безпека в Україні має багаторівневу громадську архітектуру, де поєднуються аналітичні центри національного рівня (м. Київ) й мережа локальних акторів, які працюють безпосередньо з громадами. Головним ресурсом є просвіта та критичне мислення. Більшість ініціатив (м. Чернівці, м. Рівне, м. Тернопіль, Волинь) спрямовані на навчання, розвиток медіаграмотності, формування «інформаційного імунітету». Основна проблема полягає в нерівномірності покриття населення та ресурсній обмеженості. Частина організацій не має сталих фінансових джерел або представництв у віддалених громадах, що знижує ефективність протидії дезінформації в сільських і прифронтових зонах. Позитивна тенденція закладена в поступовому зростанні мережевості. Регіональні ініціативи покроково інтегруються з національними структурами (ЦПД, StratCom, Detector Media), створюючи горизонтальні зв’язки й обмін практиками. Переважаючим ефектом є формування інформаційної стійкості. Завдяки діяльності громадського сектору відбувається зміцнення довіри, підвищення якості комунікації в громадах і поступове формування культури відповідального споживання інформації.

Зазначимо, що далеко не всі ГО в безпековій сфері (а особливо в інформаційній) активно комунікують свої результати або мають публічні кейси. Тому розглядаємо доступні. ГО «Інформаційна безпека» (м. Київ), яка активно функціонує на українському ринку з 2015 р. Основні напрями сучасної діяльності – розвиток незалежних медіа, підвищення стандартів

журналістики, стратегічні інформаційні кампанії [46]. Сильні її сторони включають національний масштаб, експертний потенціал, спроможна формувати інформаційні наративи, впливати на журналістів, готувати аналітику. Але при цьому є й низка обмежень, тому що не завжди може досягти глибин громад, особливо в районах із низькою інтернет-активністю; існує також ризик звинувачень в «упередженості».

ГО Інститут інформаційної безпеки (м. Київ). Основна місія – аналітика інформаційного простору, захист свободи слова, підтримка стратегічних комунікацій, нарративи, контрзаходи [79]. Має великий потенціал бути «мозковим центром» для регіональних партнерів, підготовки методичок, навчань. Наразі окреслено локаційну проблему, оскільки, щоб стати впливовою на рівні областей, потрібно мати регіональні представництва або партнерів на місцях/громадах.

Львівський медіафорум (LMF, м. Львів) – одна із найсильніших регіональних «опор» медіастійкості в Україні, що підтримує місцеві й національних медіа, навчання, дослідницькі проєкти, мережування журналістів; проводить щорічний форум, а також поширює освітні програми [250]. Цьогоріч відзначився активною міжнародною співпрацею й розширенням команди.

ГО «ДІІ-Україна» (Донбас). Л. Раковиця як голова ГО «ДІІ-Україна», активно працює з медіа Донбасу, працює над публікаціями, форумами, розвитком медіа на регіональному рівні. Надзвичайно важливо мати організацію, яка орієнтована саме на місцеві медіа, знання мовного, культурного контексту. Але натрапляє на виклики сучасності, коли повинна протидіяти тиску з боку окупаційної чи проросійської інформаційної машини, максимально забезпечувати безпеку журналістів, знаходити фінансування.

Клуб медіаграмотності (м. Чернівці). Його формат – це тематичні події для громади, молоді у сфері інформаційної безпеки, а саме протидії фейкам, розвитку критичного мислення. Він є хорошим стартом для мережування з університетом, школами. На продовження цьому в Чернівецькому

національному університеті імені Ю. Федьковича на кафедрі журналістики проводиться курс «Майстер-клас з медіаграмотності» [149], а також тренерські компетенції викладачів. Сильними сторонами є формальна освіта та можливість робити відкриті воркшопи для вчителів ліцеїв, громади.

Проєкт «Протидія дезінформації: інформаційна безпека громади» – навчання в громадах, створення мережі контактних осередків Центру протидії дезінформації (ЦПД) із метою долучення до регіональних ініціатив [189]. Це хороший приклад поширення «знизу вверх» і зміцнення стійкості населення через просвіту. Проблема реалізації полягає в тому, що ресурсно важко масштабувати, особливо в сільській місцевості або на тимчасово окупованих/перехідних територіях.

З ініціативи Волинської обласної державної адміністрації громади Волині пройшли навчання з кібергігієни, інструментів кібербезпеки в межах локальних тренінгів з кібербезпеки [51]. Це доволі актуальне й нагальне вирішення ситуації, що складається в державі задля підвищення «імунітету» громад до атак через інформаційні канали, слабкі паролі тощо.

Тернопільський пресклуб (м. Тернопіль) проводить тренінги з критичного мислення, фактчекінгу, дослідження про довіру до медіа та дезінформацію [4]. Серед переваг наголошуємо на тому, що це реальна платформа для системних навчань дорослих і молоді; свіжа аналітика аудиторних практик дає матеріал для планування кампаній у громадах.

ГО «Рівненська Горинь» (м. Рівне) – ініціативи з медіаграмотності у 2022–2024 рр. Цінність організації полягала в тому, що це локальний актор, спроможний працювати «на землі» спільно з бібліотеками, школами [195]. І, як наслідок – зародження ще одного систематичного проєкту «Безкоштовні курси медіаграмотності» (м. Рівне) від Рівненської обласної універсальної бібліотеки [227], де постійно відкритий простір для всіх вікових груп; регулярні набори.

Аналізуючи реальні приклади локальних або регіональних громадських / неурядових організацій в Україні, які працюють у сфері інформаційної

безпеки, протидії дезінформації, підвищення стійкості громад, робимо висновок, що необхідна систематичність, регулярність і мережа (перетворити разові лекції/курси на щомісячні клуби медіастійкості), запровадження комбо-підходу, де навчання проходить на рівні з відпрацюванням операційних навичок (воркшопи з OSINT, верифікації фото/відео, картування бот-мереж), створення регіональних «фейк-алертів», «фейк-стопів» (телеграм-каналів, розсилок) із короткими спростуваннями й порадами, підготовлені місцевими клубами та модераторами з університетів, ГО.

Громадські й волонтерські організації, професійні спілки, інформаційні агенції, не чекаючи закликів до участі державних органів, самі створили та використовують реальні інструменти в протистоянні російським інформаційно-маніпулятивним посяганням. Вони двадцять чотири години на добу стежать за безпекою інформаційного й кіберпростору України; за територіями ОРДЛО, записують відео, роблять відео з Луганська та Донецька – із військовою технікою й бойовиками, виявляють і спростовують фейки в медіа.

Активісти цих організацій змусили державу врегулювати певні питання функціонування й захисту інформаційних систем органів державної влади, поширили просвітницький рух про правильне користування соціальними мережами, інтернет. Вони взяли на себе пояснення та коментування механізмів створення, наповнення й поширення фейків, їх спростування та збір контраргументів; суттєво допомагають інформацією, виявленням відомостей про стан і переміщення військовослужбовців РФ Збройним силам, Службі безпеки України, пресцентру АТО.

Однією з проблем є неузгодженість повноважень у діяльності державних органів України, які повинні займатися захистом інформації, і їх співпрацею з громадянськими організаціями. А також комунікаційна робота української дипломатії в інших державах повинна бути оперативною й точковою – повідомлення, які діятимуть у Польщі, не спрацьовують в Італії, потрібно розкривати механізми впливу проросійських сил на європейське суспільство й

оприлюднювати результати досліджень із характерними ознаками двосторонніх чи міжнародних відносин. Проблемою є також бюджет більшості громадських організацій України, що обрали своєю діяльністю відстеження та захист інформаційного простору України, тому вони функціонують на власні кошти засновників і благодійні внески громадськості.

Проведений аналіз діяльності українських громадських організацій у сфері інформаційного захисту засвідчує, що саме громадянське суспільство стало одним із ключових стовпів у формуванні системи інформаційної безпеки в умовах гібридної війни. Із початку збройної агресії Російської Федерації проти України у 2014 р. громадські ініціативи відіграли критично важливу роль у протидії ворожим інформаційно-психологічним операціям, виявленні фейків, формуванні наративів, спрямованих на консолідацію українського суспільства. Своєю діяльністю ці організації не лише заповнили прогалини, залишені державними структурами, але й започаткували нові практики OSINT-розвідки, цифрового патрулювання, медіаграмотності й контрпропаганди. Створення потужних громадських інституцій, таких як «InformNapalm», «CAT-UA», «НотаЄнота», Центр стратегічних комунікацій StratCom Ukraine, «Українські кібервійська», «Детектор медіа», «Інформаційний спротив», «Лабораторія цифрової безпеки», а також ініціатив із фактчекінгу, таких як «StopFake», дали змогу забезпечити постійний громадський контроль за інформаційним простором, а також оперативне реагування на інформаційні загрози. Ці організації довели свою ефективність у знешкодженні фейкових наративів, викритті російських військових в окупованих територіях, протидії пропагандистським кампаніям через соціальні мережі, а також у розбудові системи цифрової безпеки для журналістів, активістів і правозахисників. Їхня діяльність стала джерелом експертної інформації для українських державних структур, міжнародних організацій, а також іноземних партнерів України.

Водночас, функціонування громадських ініціатив у сфері інформаційної безпеки не позбавлене викликів. Найгострішими серед них є фрагментарність

координації з боку держави; нестача сталого фінансування; брак спеціалізованих кадрів у сфері кіберзахисту та OSINT; надмірна залежність від донорської підтримки. Окремі випадки, як-от публікація персональних даних журналістів у базі «Миротворець», засвідчують необхідність упровадження чітких етичних стандартів і правових рамок у діяльність деяких ініціатив для уникнення порушень прав людини. Досвід українських ГО також підтверджує, що сучасна інформаційна безпека неможлива без активної участі громадянського суспільства. Добровольчі ініціативи в цифровій сфері, незалежна журналістика, просвітницька діяльність, розвиток критичного мислення й інформаційної гігієни серед населення повинні стати основою стійкого суспільного імунітету до маніпуляцій, пропаганди й дезінформації.

У перспективі державі треба поглибити співпрацю з громадськими структурами, забезпечити їм правовий захист, інституційну підтримку, сприяти формуванню національної мережі цифрової безпеки, інтегрованої в загальноєвропейську систему захисту від гібридних загроз. Водночас актуалізується потреба у виробленні єдиної стратегії взаємодії державних і громадських інституцій у сфері інформаційного захисту – із чітким розподілом повноважень, зобов'язань та зон відповідальності. Отже, громадянське суспільство України довело свою ефективність як потужний агент інформаційного спротиву. Утвердження їхньої ролі в системі національної безпеки є не лише проявом демократичної зрілості, а й запорукою виживання держави в умовах тривалого гібридного конфлікту.

Український досвід протидії інформаційному тероризму в умовах повномасштабної гібридної агресії набуває особливої ваги для міжнародної безпекової спільноти. Він демонструє, як держава, зазнаючи систематичного зовнішнього інформаційного тиску, може успішно поєднувати інституційні механізми, технологічні інновації, громадську ініціативу та міжнародну солідарність для зменшення шкоди від інформаційного терору. Значення цього досвіду полягає в кількох вимірах. По-перше, Україна стала першою державою, яка фактично створила цілісну модель реагування на інформаційні

загрози в реальному часі під тиском постійних атак. По-друге, вона запропонувала нові інструменти інформаційного спротиву: цифрову дипломатію, алгоритмічну відповідь на фейки, мобілізацію цифрового суспільства (зокрема волонтерських ініціатив, кіберпартизанських рухів). По-третє, український кейс доводить важливість розвитку національної медіаграмотності та критичного мислення громадян як фундаменту стійкості до інформаційних маніпуляцій. Цей досвід уже частково інтегрується в політики безпеки Європейського Союзу, НАТО, окремих держав-партнерів. Україна є не лише об'єктом допомоги, а й джерелом практичних знань, які можуть бути масштабовані й адаптовані для інших регіонів світу, що стикаються з інформаційними загрозами. На цьому тлі актуалізується потреба у формалізації міжнародно-правових механізмів протидії інформаційному тероризму, у розробці глобальних стратегій цифрової безпеки, у яких український досвід слугуватиме одним із ключових орієнтирів.

Розвиток демократичної держави неможливий без активної участі громадянського суспільства у формуванні політик безпеки, зокрема у сфері протидії інформаційним загрозам і тероризму. В умовах гібридної війни проти України саме інститути громадянського суспільства стали одним із найважливіших чинників інформаційної стійкості, поєднуючи моніторингову, освітню, аналітичну й комунікаційну функції. Нормативно-правові механізми, що регулюють боротьбу з тероризмом, повинні враховувати цю роль і забезпечувати правові підстави для залучення неурядових суб'єктів до системи національної безпеки.

Попри значний прогрес у розвитку законодавства у сфері боротьби з тероризмом (Закон України «Про боротьбу з тероризмом», 2003 р.), його положення залишаються зорієнтованими переважно на силові структури та державні органи. Громадянське суспільство в цьому контексті розглядається пасивно – як об'єкт захисту, а не активний суб'єкт протидії. Водночас нові форми терористичної діяльності – інформаційний та кібертероризм, інформаційно-психологічні операції, маніпуляції в медіа й соціальних

мережах – потребують розширення кола суб'єктів безпеки, уключаючи аналітичні центри, журналістські ініціативи, волонтерські мережі OSINT та фактчекінгові спільноти (додаток И).

Громадянське суспільство відіграє провідну роль у створенні механізмів раннього попередження інформаційних атак, у викритті дезінформаційних кампаній і підвищенні рівня медіаграмотності населення. Такі ініціативи, як *StopFake, Detector Media, Інститут масової інформації, Texty.org.ua, OSINT-Ukraine*, фактично виконують функцію недержавних індикаторів інформаційної стійкості. Їхня діяльність має не лише соціальне, а й безпекове значення, оскільки сприяє формуванню критичного мислення, зниженню рівня паніки та підвищенню довіри до достовірних джерел.

З огляду на це, законодавча модернізація повинна передбачати інтеграцію громадянського суспільства до системи забезпечення інформаційної безпеки. Доцільно закріпити в Законі України «Про боротьбу з тероризмом» низку норм, що визначають правовий статус неурядових суб'єктів у сфері інформаційного захисту. Зокрема, пропонується:

1. Визнати громадянське суспільство співсуб'єктом протидії інформаційному тероризму, який бере участь у моніторингу, верифікації інформації, аналітиці та громадському контролі за діяльністю державних структур;

2. Запровадити інститут громадських рад із питань інформаційної безпеки при ключових органах державної влади – СБУ, Міністерстві цифрової трансформації, Міністерстві оборони, Центрі стратегічних комунікацій. Такі ради можуть виконувати консультативно-дорадчу функцію, сприяти комунікації між державою й суспільством;

3. Передбачити можливість залучення неурядових організацій до програм кіберосвіти, інформаційної просвіти та фактчекінгу в межах державних і регіональних стратегій;

4. Закріпити принцип партнерства в протидії інформаційному тероризму, який передбачає відкритий обмін даними між державними структурами, громадськими ініціативами та міжнародними партнерами.

Такі зміни не лише розширюють інституційний склад системи інформаційної безпеки, але й сприяють формуванню моделі колективної стійкості – у якій держава, суспільство й бізнес діють як взаємодоповнювальні елементи єдиної системи реагування на інформаційні загрози.

На особливу уваги заслуговує освітньо-просвітницький аспект діяльності громадянського суспільства, що має бути нормативно підтриманий. Програми медіаосвіти, тренінги з кібергігієни, інформаційна грамотність для держслужбовців і молоді – це не лише соціальні ініціативи, а й ефективний превентивний інструмент протидії інформаційному тероризму. Уключення таких заходів до законодавчих актів про боротьбу з тероризмом відповідатиме принципу «безпека через освіту», який нині визнається провідними міжнародними інституціями, зокрема ЄС і НАТО. Міжнародний досвід свідчить, що в розвинених демократіях саме неурядові організації забезпечують гнучкість та інноваційність у сфері інформаційного захисту, діючи швидше й адаптивніше за бюрократичні структури. В Україні ця тенденція також набуває системного характеру – волонтерські об’єднання й незалежні журналістські ініціативи часто першими реагують на дезінформаційні кампанії, зокрема російського походження.

Отже, громадянське суспільство стає невід’ємним елементом національної системи інформаційної стійкості. Його нормативне визнання в контексті антитерористичної політики забезпечить баланс між державною монополією на безпеку та демократичними принципами участі. Це дасть змогу перейти від вертикальної моделі управління інформаційною безпекою до мережевої, багаторівневої системи, у якій держава, суспільство й міжнародні партнери є взаємопов’язаними суб’єктами спільного інформаційного захисту. Отже, зміцнення інформаційної стійкості України в контексті протидії тероризму потребує не лише оновлення законодавчої бази, а й

інституціоналізації партнерства з громадянським суспільством. Саме через поєднання нормативного регулювання, відкритості комунікацій та активності неурядових акторів можливо забезпечити комплексну, демократично легітимну модель інформаційної безпеки, що стане фундаментом для сталого розвитку держави в умовах гібридних викликів.

ВИСНОВКИ ДО РОЗДІЛУ 5

Інформаційна агресія Російської Федерації проти України, що триває вже понад два десятиліття, є однією з ключових складових частин сучасної гібридної війни. Починаючи з етапу формування проросійських медіанаративів у 2004–2013 рр., і до відкритої інформаційної кампанії після 2014 р., РФ системно використовує інформаційний простір як поле стратегічного впливу. Змістовна еволюція цієї агресії засвідчує її комплексний характер: вона охоплює не лише традиційні медіа, але й цифрові платформи, соціальні мережі, кіберінфраструктуру, освітню та культурну сфери.

Метою інформаційних операцій Кремля є дестабілізація внутрішньополітичної ситуації в Україні, делегітимізація її державних інституцій, підрив довіри до Збройних сил, формування образу України як «failed state», а також перешкоджання її європейській та євроатлантичній інтеграції. Основні інструменти цього впливу включають масове поширення дезінформації, маніпуляцію фактами, активізацію бот-мереж і фейкових акаунтів, просування токсичних наративів у соціальних медіа, легітимізацію пропаганди через псевдоаналітичні платформи й так звані «новинні фабрики».

У відповідь на ці виклики Україна реалізовує багаторівневу систему протидії. Вона охоплює:

– нормативно-правові механізми: ухвалення закону «Про медіа», запровадження санкцій, блокування ворожих ресурсів;

– інституційну інфраструктуру: Рада національної безпеки і оборони України, Національна рада з питань телебачення і радіомовлення, Центр стратегічних комунікацій;

– громадянські ініціативи: фактчекінгові платформи StopFake, VoxUkraine, Detector Media, Texty.org.ua;

– міжнародне партнерство: взаємодія з EUvsDisinfo, NATO StratCom COE, East StratCom Task Force та іншими міжнародними ініціативами.

Водночас ефективність цієї протидії стримується низкою критичних факторів. Серед них – недостатній рівень медіаграмотності, особливо у віддалених регіонах; повільна реакція державних інституцій на нові загрози, зокрема на deepfakes та генеративний штучний інтелект; олігархізація медіапростору й політична залежність окремих медіа; зростання впливу анонімних Telegram-каналів; нерівномірний доступ населення до якісного інформаційного контенту.

В умовах триваючої російської агресії інформаційна безпека України має бути пріоритетом національної безпекової політики. Це не лише питання оборонного потенціалу в інформаційній сфері, а й потреба в стратегічному плануванні, медіаосвіті, розвитку цифрової дипломатії та комунікаційної культури. Державна політика повинна орієнтуватися не лише на реагування, а й на попередження загроз, формування системи стратегічних контрнаративів і посилення координації з міжнародними партнерами.

Як результат, російська інформаційна агресія суттєво трансформувала підходи до інформаційної політики в Україні, актуалізувавши питання етичної журналістики, зміцнення цифрової грамотності, підвищення стійкості медіаінфраструктури. Формування національної інформаційної екосистеми, спроможної ефективно реагувати на виклики гібридної війни, є одним із ключових завдань держави, громадянського суспільства й міжнародної спільноти в найближчій перспективі.

Аналіз функціонування громадянського суспільства у сфері інформаційного захисту України засвідчує його унікальну роль як активного

суб’єкта протидії інформаційним загрозам у контексті гібридної війни. Із 2014 р. низка громадських організацій, зокрема «InformNapalm», «Українські кібервійська», «Детектор медіа», «Інформаційний спротив», «Майдан Моніторинг», «Лабораторія цифрової безпеки», – це рушій формування інформаційної стійкості держави, розробки контрнаративів, упровадження технологій OSINT, медіаграмотності, цифрового захисту й дослідницької діяльності у сфері виявлення фейків і ворожих наративів.

Незалежна діяльність цих ініціатив не лише компенсувала дефіцит державної спроможності на початкових етапах конфлікту, але й стала каталізатором інституціоналізації інформаційної безпеки. Громадські об’єднання взяли на себе критично важливі функції – від цифрової розвідки й боротьби з дезінформацією до міжнародної комунікації результатів OSINT-розслідувань. Їхня діяльність сприяла формуванню прозорих механізмів контролю за інформаційним простором, розбудові горизонтальних комунікацій між державою, медіа та суспільством, формуванню демократичного інформаційного середовища.

Попри значні досягнення, актуальними залишаються проблеми фрагментованості взаємодії з державними структурами, обмеженості фінансування, нестачі кваліфікованих кадрів і правового врегулювання їхньої діяльності. Інциденти на кшталт ситуації із сайтом «Миротворець» засвідчили потребу в етичних стандартах і балансі між захистом національної безпеки та прав людини.

ВИСНОВКИ

Концепт тероризму в контексті теорії міжнародних відносин постає як надзвичайно складне, багатовимірне й водночас політично чутливе явище, яке має не лише безпековий, а й глибокий соціальний, інформаційний та ідеологічний виміри. Відсутність універсального визначення тероризму обумовлюється як об'єктивною складністю феномену, так і політичними інтерпретаціями, що впливають на концептуалізацію самого поняття. Тероризм трансформувався від державного інструменту терору до інструменту недержавних та транскордонних акторів, ставши формою асиметричної боротьби за політичні, ідеологічні або релігійні цілі. У сучасних умовах його механізми охоплюють не лише фізичне насильство, а й системні інформаційні кампанії, що формують атмосферу страху, недовіри та нестабільності. Окрім того, зростання ролі кіберпростору, мас-медіа й соціальних мереж значно підсилило спроможність терористичних організацій впливати на глобальні процеси. Теоретичні парадигми міжнародних відносин – неореалізм, неолібералізм, конструктивізм – по-різному інтерпретують тероризм: як засіб впливу у світі анархії; як загрозу, що потребує міжнародної координації, або як соціальний конструкт, що формується під впливом дискурсивних практик. Такий міждисциплінарний підхід дає змогу більш комплексно оцінювати природу тероризму, зокрема його еволюцію, типологію, механізми функціонування та способи легітимації. Загалом, концепт тероризму повинен розглядатися як динамічне поняття, що розвивається у відповідь на трансформації міжнародного безпекового середовища, соціальних конфліктів й інформаційних технологій. Його аналіз є необхідною передумовою для формування ефективної національної та глобальної стратегій протидії терористичним загрозам і посилення архітектури міжнародної безпеки.

Міжнародний тероризм у сучасному світі є не лише загрозою безпеці, а й складним глобалізаційним феноменом, що виявляє глибокі суперечності між

цивілізаціями, політичними системами та соціальними устроями. Його витоки й еволюція значною мірою зумовлені асиметрією глобального розвитку, геополітичними імперативами провідних держав, спробами збереження домінування західної моделі, а також ігноруванням культурної ідентичності «інших» світів. Водночас тероризм є реакцією на виклики сучасної глобалізації, у якій не всі учасники мають рівні можливості доступу до ресурсів, розвитку й самореалізації. Тож для подолання тероризму потрібне не лише вдосконалення силових і безпекових механізмів, а й нова парадигма глобальної взаємодії, заснована на повазі до цивілізаційного плюралізму, справедливості, інклюзивності й етичної відповідальності глобальних лідерів.

Інформаційний тероризм став невід'ємною та надзвичайно небезпечною складовою частиною міжнародного тероризму в умовах цифрової доби. Його вплив поширюється не лише на інфраструктуру, а й на свідомість суспільства, використовуючи інструменти масових маніпуляцій, кіберзлочинів і спеціальних інформаційних операцій. Як показав аналіз наукових підходів, це явище охоплює низку форм – від психологічного тиску й дезінформації до кібернападів на критичні об'єкти держав. Небезпека інформаційного тероризму полягає в його невидимості, швидкості поширення та здатності руйнувати довіру до влади, інституцій і цінностей. У сучасному світі, де межа між війною й миром розмита, інформаційна зброя часто є не менш потужною, ніж фізична. Тому боротьба з інформаційним тероризмом повинна стати пріоритетом як для національної безпеки, так і для міжнародного співробітництва, що потребує оновлення правових механізмів, розвитку цифрової стійкості, створення ефективної системи реагування на інформаційні загрози.

Комплексний міждисциплінарний аналіз феномену міжнародного тероризму свідчить про його виняткову складність, динамічність і здатність до трансформації у відповідь на зміни глобального безпекового середовища. Незважаючи на помітні інтелектуальні зусилля, спрямовані на осмислення причин та форм прояву тероризму, наукове забезпечення боротьби з цим

явищем і досі не відповідає рівню його загрози. Ізольовані або одновимірні підходи до подолання терористичних викликів виявляються неефективними. Водночас, як свідчить аналіз праць провідних аналітиків (В. Лакер, К. Гіршман, В. Парсі, А. Конте), серед причин і рушіїв терористичної активності домінують соціально-економічна поляризація, релігійний фанатизм, ідеологічний радикалізм, прагнення до самовизначення та глибокі міжцивілізаційні розломи.

Особливу тривогу викликає поява так званого технологічного тероризму, заснованого на використанні зброї масового ураження, кіберінструментів і «сурогатних» воєн. Усе це посилюється процесами глобалізації, які, з одного боку, сприяють поширенню екстремістських ідеологій, а з іншого – ускладнюють механізми правової кваліфікації та міжнародного реагування. Змінюється й природа суб'єктів терористичної діяльності: до традиційних угруповань додаються транснаціональні структури, мережеві організації та гібридні утворення з ознаками квазідержав. У зв'язку з цим потребує переосмислення концепт як війни, так і самої безпеки, де терористичні акти дедалі більше набувають ознак воєнного інструментарію як за масштабами наслідків, так і за політичними цілями.

Проблема тероризму сьогодні виходить за межі питань безпеки і стає індикатором структурних вад світового порядку. Досвід подій 11 вересня 2001 р., подальших збройних операцій та міжнародних санкційних механізмів свідчить про обмежену дієвість переважно силових або суто правових підходів. Навпаки, боротьба з тероризмом повинна здійснюватися не лише через нейтралізацію його безпосередніх носіїв, а й шляхом ліквідації причин – бідності, соціального відчуження, релігійної нетерпимості, викривленої глобалізації й нерівності доступу до ресурсів.

Усе це обумовлює необхідність переходу від концепту «реакції» до концепту «упередження», що передбачає синергію зусиль національних держав, міжнародних організацій, громадянського суспільства та наукової спільноти. Без цього говорити про реальну протидію терористичній загрозі –

лише ілюзія. Тероризм не є окремим злом, а радше – симптомом глибших хвороб сучасної цивілізації. Отже, стратегія боротьби з ним повинна бути частиною ширшої доктрини глобальної безпеки, справедливості та стійкого розвитку.

Теракти 11 вересня 2001 р. стали поворотним моментом у переосмисленні міжнародної безпеки, ролі держав у боротьбі з новими загрозами й засад глобального порядку. Уперше одній із найпотужніших країн світу – США – було завдано удару зсередини, що продемонструвало асиметричний характер терористичних загроз у глобалізованому світі. У відповідь США ініціювали воєнну кампанію в Афганістані та Іраку, що викликала міжнародну критику через порушення принципів колективної безпеки й підміну їх концепцією «превентивної війни». Події спричинили геостратегічні зрушення, зокрема посилення американського впливу в Центральній Азії та активізацію інформаційних і пропагандистських практик. Риторика «світової боротьби з тероризмом» часто слугувала виправданням політичних та воєнних дій, що нехтували соціальними й культурними коренями самого явища тероризму.

Сучасна епоха характеризується стрімкою еволюцією форм воєнних дій, що виходять за межі традиційної «гарячої» війни та охоплюють широкий спектр асиметричних, інформаційних, медійних і проксі-конфліктів. Війна четвертого покоління, гібридна війна, iWar, медіавійна, асиметричні та посередницькі війни дедалі частіше використовуються як ефективні інструменти впливу в умовах, коли відкриті бойові дії стають політично й економічно невигідними для глобальних акторів. Ці форми конфліктів орієнтовані не лише на військове послаблення противника, а й на підрив його внутрішньої стабільності, ідентичності, економіки, легітимності влади та морального духу населення.

Інформаційна війна в умовах сучасного глобального протистояння перетворилася з допоміжного інструменту на стратегічну вісь гібридної агресії. Вона охоплює широке коло цілей – від дезорганізації комунікацій, підриву інформаційної інфраструктури, впливу на психіку населення до

створення альтернативної реальності в масовій свідомості. Такі війни ведуться не лише державами, а й транснаціональними структурами, терористичними угрупованнями, хактивістами та приватними суб'єктами.

Сучасні інформаційні конфлікти не обмежуються межами кіберпростору – вони інтегруються в політичну, економічну, культурну сфери життя, вражаючи і структури влади, і масову свідомість, і економіку. Особливо небезпечними є новітні форми мережево-центричної війни, які поєднують інформаційний, психологічний та економічний впливи в єдиний інструмент стратегічного тиску. Така війна не потребує фізичної окупації території – вона спрямована на руйнування довіри, ідентичності, морального духу населення, що створює передумови для внутрішньої дестабілізації.

Отже, у XXI ст. саме інформаційна війна визначає нову парадигму глобального конфлікту, і країни, які не готові до активної інформаційної самооборони та стратегічних комунікацій, ризикують утратити не лише контроль над власним інформаційним простором, а й суверенітет. Ефективна протидія цим загрозам потребує національної інформаційної доктрини, розвитку цифрового опору, критичного мислення громадян і тісної міжнародної кооперації.

Інформаційна зброя стала одним із ключових інструментів сучасного конфлікту, спроможним завдавати значної шкоди державам без фізичного втручання. Її специфіка полягає у використанні дезінформації, маніпулятивних наративів, кібероперацій, психологічного впливу, фейків і спеціальних інформаційних операцій, які спрямовані на підрив морального духу, дестабілізацію політичної ситуації, ослаблення державного управління та ерозію суспільної довіри. У контексті гібридної війни росії проти України інформаційна зброя стала стратегічним засобом впливу: зокрема, через поширення пропаганди, підрив довіри до державних інституцій, делегітимацію збройних сил, а також стимулювання паніки, зневіри й розколу всередині суспільства. Такий тип зброї не потребує значних матеріальних витрат, але має високий рівень ефективності завдяки цифровим технологіям,

соціальним мережам і глобальному інформаційному простору. Використання інформаційної зброї також змінює традиційні уявлення про воєнні конфлікти – стирається межа між миром та війною, цивільним і військовим, обороною й нападом. У цих умовах держави повинні розвивати спроможність до ідентифікації, нейтралізації та попередження інформаційних атак, зміцнювати цифрову стійкість, стратегічні комунікації й навички інформаційної гігієни громадян. Отже, інформаційна зброя становить загрозу національній безпеці на рівні, зіставному із застосуванням традиційних форм збройної сили, що потребує адекватних заходів реагування як у внутрішній, так і в міжнародній політиці безпеки.

У сучасному цифровому середовищі інформаційна стійкість перетворюється на ключовий інструмент протидії інформаційному тероризму, який ускладнює безпекову ситуацію, підриває демократичні інституції та порушує суспільну згуртованість. Комплексний аналіз показав, що загроза інформаційного тероризму проявляється не лише через кібернапади чи фейки, а й через деструктивний вплив на політичну культуру, громадянську активність і довіру до державних інституцій.

Інформаційна стійкість охоплює широкий спектр заходів – від розвитку стратегічних комунікацій і медіаграмотності до забезпечення цифрової безпеки й інституційного контролю за дотриманням інформаційних прав. Центральним елементом у протидії деструктивним впливам є синергія між державними структурами, громадянським суспільством і технічними інструментами, спрямованими на виявлення, блокування й нейтралізацію інформаційних атак.

Особливу роль у зміцненні інформаційної стійкості відіграють медіаосвіта та критичне мислення, що формують у громадян здатність розпізнавати маніпуляції й фейки; інституційна спроможність держави, уключаючи роль омбудсмена або інформаційного комісара, у захисті інформаційних прав; інструменти ЄС (Hybrid Toolbox, Cyber Diplomacy Toolbox тощо), які слугують ефективною моделлю багаторівневої протидії

гібридним загрозам; цифрова безпека та нормативне регулювання, що забезпечують технологічний і правовий захист національної інформаційної інфраструктури.

Досвід України та країн ЄС підтверджує ефективність комплексного підходу, що поєднує превентивні, просвітницькі, нормативні й технічні засоби. У цьому контексті створення незалежного інституту Інформаційного комісара в Україні є логічним кроком до конституційного закріплення інформаційної демократії та адаптації до європейських стандартів. Отже, інформаційна стійкість повинна розглядатися як стратегічна категорія національної безпеки, що забезпечує спроможність суспільства й держави протистояти інформаційним загрозам, зберігати соціальну згуртованість, посилювати громадянську відповідальність і формувати безпечне інформаційне середовище в умовах гібридної війни та цифрових трансформацій.

У XXI ст. інформаційні технології стали основою глобальної взаємодії, економічної діяльності й державного управління. Водночас цифровізація зумовила зростання кіберзагроз, що ставить під сумнів безпечність і стійкість національних інформаційних інфраструктур. Аналіз міжнародного досвіду свідчить, що успішна інформаційна політика потребує поєднання кількох ключових елементів: ефективного нормативно-правового регулювання, належної організації системи управління, розвитку цифрової грамотності населення та впровадження інструментів кіберстрахування.

Росія, Китай, а також недержавні актори, зокрема терористичні угруповання, активно адаптують ці моделі до власних стратегічних цілей, що створює серйозні виклики для традиційної системи міжнародного права та безпеки. Такі війни часто залишаються нижче порога офіційного оголошення конфлікту, що ускладнює міжнародне реагування й відкриває простір для правового нігілізму. Водночас західні демократії, з огляду на високу вразливість до втручання у свої відкриті суспільства, змушені шукати нові

моделі стійкості – від реформування інформаційної політики до запровадження систем протидії кіберзагрозам і гібридним операціям.

Поширення таких форм війни свідчить про глибоку трансформацію безпекового середовища XXI ст., у якому ключову роль відіграють не лише військові ресурси, а й технологічна перевага, інформаційний контроль, психологічний вплив та здатність до адаптивного мислення. Це потребує оновлення концепцій національної та міжнародної безпеки, міжвідомчої координації, стратегічних комунікацій і консолідації зусиль демократичного світу задля ефективного реагування на новітні виклики та загрози. США демонструють системний підхід до інформаційної безпеки, зокрема завдяки ухваленню стратегій кіберзахисту, створенню спеціалізованих державних інституцій (CERT, DHS, C3), розвитку цифрової освіти й співпраці з приватним сектором. Суттєве значення має також баланс між захистом персональних даних і забезпеченням інформаційної безпеки в межах загальнодержавної стратегії. Європейський Союз формує комплексну політику кібербезпеки через директиви, мережі CERT, агенцію ENISA, а також заохочення міждержавної кооперації у сфері кіберзлочинності. Успішні приклади Естонії, Франції та Норвегії демонструють ефективність поєднання правового регулювання, інституційної стійкості й стратегічного планування.

У результаті дослідження зроблено висновок, що ключовими чинниками ефективної інформаційної безпеки є наявність чіткої законодавчої бази та стратегій кіберзахисту; інтеграція державних, приватних і міжнародних зусиль; розвиток цифрової грамотності населення; створення спеціалізованих органів реагування на кіберінциденти; посилення міжнародного співробітництва в межах глобальної цифрової екосистеми. Зважаючи на гібридні загрози, що постійно еволюціонують, та зростаючу інтенсивність кібератак, забезпечення інформаційної безпеки стає не лише технічним викликом, а й пріоритетом державної політики й міжнародної співпраці.

У контексті зростання ролі цифрових технологій і кіберпростору як рушія соціально-економічного розвитку, проблема інформаційної безпеки набула

глобального значення та стала предметом стратегічної уваги держав. Аналіз практик Японії, Китаю й Індії дає підставу зробити низку важливих висновків щодо закономірностей та особливостей національних підходів до забезпечення інформаційної безпеки.

По-перше, у Японії простежено розвинену нормативно-інституційну модель, що ґрунтується на принципах соціальної відповідальності, сервісного підходу до кіберзахисту та широкого використання механізмів аутсорсингу. Водночас система характеризується високим рівнем державного впливу на інформаційний обіг, уключаючи механізми неформального контролю й саморегулювання медіа. Незважаючи на значні досягнення в галузі інформатизації, нормативне забезпечення інформаційних прав громадян залишається обмеженим фрагментарністю правової бази та дефіцитом доктринального осмислення.

По-друге, Китай демонструє стратегічне використання кібербезпеки як елементу зовнішньої політики. Ініціатива «Цифрового шовкового шляху» в рамках BRI передбачає не лише експорт цифрової інфраструктури, а й експорт моделі кіберсуверенітету. Залучення кібербезпечних компаній, тісно пов’язаних із державними органами безпеки, свідчить про використання приватного сектору в інтересах політичного впливу та просування специфічного бачення інтернет-врядування. Такий підхід викликає занепокоєння щодо прозорості, дотримання прав людини та потенційних механізмів цифрового контролю.

По-третє, Індія, маючи статус одного з лідерів у сфері інформаційних технологій, активно розвиває інституційний потенціал у сфері кібербезпеки. Національна політика кібербезпеки, створення галузевих органів (зокрема DSCI), а також зростання державного й приватного інвестування свідчать про прагнення до посилення стійкості у цифровому середовищі. Водночас країна залишається вразливою до кіберзагроз через фрагментарність регулювання, обмежений доступ до якісних IT-рішень і нерівномірність цифрового розвитку.

Загалом, досвід цих країн засвідчує необхідність формування багаторівневої, адаптивної системи інформаційної безпеки, що враховує комплексність регуляторних механізмів; баланс між безпекою, правами людини й свободою інформації; стратегічне бачення цифрового суверенітету; ефективну координацію між державним, приватним і громадянським секторами; міжнародну співпрацю в галузі цифрової безпеки. Для України ці напрацювання становлять значну цінність у процесі розбудови національної системи інформаційної безпеки. Вивчення підходів Японії, Китаю та Індії дає змогу виокремити ефективні практики, уникнути системних ризиків і сформулювати стратегію цифрової стійкості, що відповідатиме як вимогам національної безпеки, так і цінностям демократичного врядування.

Аналіз підходів країн Латинської Америки до забезпечення інформаційної безпеки засвідчив наявність спільних викликів, серед яких – фрагментарність нормативно-правової бази, нестача координації між інституціями, обмежені технічні ресурси та вразливість до кіберзлочинності. Водночас кожна держава демонструє власну модель реагування на цифрові загрози, яка формується під впливом політичного контексту, рівня цифровізації й наявності інституційної спроможності. Мексика характеризується спробами інституційного оформлення кібербезпеки, однак її політика залишається декларативною через брак міжвідомчої координації, відсутність центрального органу та обмежене впровадження стратегії. Бразилія демонструє децентралізовану, але активну політику з акцентом на цифрові права, свободу інтернету й публічно-приватне партнерство. Водночас ефективність обмежується регіональною фрагментованістю. Аргентина зробила кроки до посилення кіберзахисту через створення спеціалізованих структур, однак страждає на відсутність інтегрованої стратегії та сталого міжінституційного управління. Колумбія виділяється порівняно системним підходом до формування кіберполітики, активною участю в міжнародному співробітництві й розбудовою інституцій, проте стикається з нестачею ресурсів та нерівномірним упровадженням політик.

Урешті, ефективне забезпечення інформаційної безпеки в регіоні потребує створення національних координуючих центрів; уніфікації законодавства відповідно до міжнародних стандартів; розвитку цифрової освіти та обізнаності населення; зміцнення міжнародного співробітництва в межах Латинської Америки; поєднання технічних, правових й організаційних механізмів кіберзахисту. Для України досвід країн Латинської Америки може слугувати джерелом важливих уроків щодо побудови стійкої цифрової інфраструктури в умовах політичної нестабільності, обмежених ресурсів і зростаючих гібридних загроз.

Аналіз особливостей поширення та протидії інформаційному тероризму в африканських країнах засвідчує, що континент перебуває у фазі швидкої цифрової трансформації, яка поряд із можливостями економічного та соціального розвитку супроводжується суттєвим зростанням інформаційних загроз. Інформаційний тероризм і кіберзлочинність стають системними викликами для держав, бізнесу та громадян, що зумовлено низьким рівнем цифрової грамотності, недостатнім розвитком правових й інституційних механізмів реагування, а також слабкою координацією між державами регіону. Попри наявність окремих позитивних прикладів – створення спеціалізованих міністерств (як у Зімбабве), ухвалення стратегій кібербезпеки (Єгипет) та розвиток національних політик ІКТ (ПАР, Кенія, Танзанія), – загалом африканські країни залишаються вразливими до інформаційного тероризму. Кіберзагрози в регіоні САДК і поза ним характеризуються динамічним зростанням, технічною складністю й масштабністю атак, що часто спричиняє значні економічні втрати.

Отже, ключовими завданнями для африканських держав є формування узгодженої регіональної політики кібербезпеки, адаптація національного законодавства до сучасних типів кіберзлочинів, зміцнення кадрового та інституційного потенціалу силових структур, розвиток цифрової культури населення, а також активізація міжнародної співпраці у сфері протидії інформаційному тероризму. Тільки комплексний і скоординований підхід

дасть змогу ефективно протистояти зростаючій загрозі інформаційного тероризму та забезпечити безпечний розвиток цифрового простору Африки.

Інформаційна стійкість є політичним та інституційним маркером зрілості держави, що визначає її спроможність протидіяти інформаційному тероризму без руйнування демократичних засад. Високі значення ICIC корелюють із рівнем відкритості, правової культури та суспільної довіри; натомість низькі – із режимним контролем або структурною слабкістю. Порівняльний аналіз підтверджує: інформаційна стійкість має три моделі – демократичну, режимно-центричну та транзитивну; лише перша забезпечує сталу безпеку й легітимність. Для України релевантним є комбінований підхід, який поєднує технологічну модернізацію, розвиток критичного мислення, медіаосвіту та інституційну координацію з партнерами ЄС і НАТО.

Інформаційна агресія російської федерації проти України є системною, комплексною та стратегічно вмотивованою формою гібридної війни, що поєднує пропаганду, дезінформацію, кібероперації, інформаційно-психологічні впливи й маніпулятивні кампанії в цифровому середовищі. Її мета – підірвати політичну стабільність, делегітимізувати державні інститути, ослабити національну єдність і знизити міжнародну підтримку України.

Аналіз засобів та механізмів, що використовуються РФ, свідчить про високу технологічність, адаптивність і мімікрію під демократичні цінності, зокрема свободу слова, плюралізм та відкритість інформаційного простору. В умовах триваючої війни особливо небезпечною є здатність ІПсО формувати викривлену реальність, деморалізувати населення й впливати на громадську думку як в Україні, так і за її межами.

Незважаючи на значні зусилля Української держави у сфері протидії – від нормативно-інституційних ініціатив до блокування проросійських ресурсів, зміцнення стратегічних комунікацій і співпраці з міжнародними партнерами, – Україна залишається вразливою до інформаційних атак. Серед її ключових проблем – низький рівень цифрової освіти, обмеженість незалежних медіа,

поширення анонімного деструктивного контенту та повільна реакція на новітні загрози, зокрема з боку генеративного ШІ.

У цьому контексті забезпечення інформаційної безпеки повинно стати постійним елементом національної безпекової політики. Протидія інформаційно-маніпулятивному впливу РФ мусить спиратися на такі стратегічні підходи, як підвищення цифрової та медіаграмотності громадян, формування культури критичного мислення, розвиток незалежних медіа, розширення міжнародної співпраці в межах системи інформаційної безпеки й створення ефективної державної політики з превентивного захисту інформаційного простору. Лише в умовах поєднання інституційної спроможності, громадянської активності та міжнародної солідарності можливе стримування російської інформаційної експансії й збереження інформаційного суверенітету України.

Громадянське суспільство стало одним із ключових чинників забезпечення інформаційної безпеки України в умовах гібридної війни. Із початку агресії РФ у 2014 р. численні неурядові організації, журналістські ініціативи, OSINT-спільноти та волонтерські об’єднання, зокрема StopFake, Detector Media, InformNapalm, українські кібервійська, Лабораторія цифрової безпеки, узяли на себе функції моніторингу, спростування дезінформації, цифрового патрулювання й формування контрнаративів. Ці організації оперативно реагують на інформаційні загрози, посилюють спроможності держави, розбудовують цифрову грамотність суспільства, створюють нові стандарти кіберзахисту та сприяють міжнародному визнанню українського досвіду. Участь громадськості дала змогу не лише компенсувати інституційну нестачу державної відповіді, але й запровадити нові практики – від верифікації фактів до мобілізації цифрових волонтерів.

Водночас діяльність громадянського сектору стикається з низкою викликів: фрагментарна координація з державою, нестача фінансування, правова неврегульованість, а також необхідність дотримання етичних і правових норм, особливо щодо питань публікації персональних даних. Окремі

приклади, як-от випадок із «Миротворцем», засвідчують ризики відсутності чітких рамок співпраці між державними й недержавними суб'єктами. У сучасних умовах захист інформаційного простору потребує скоординованої взаємодії держави та громадських ініціатив. Необхідним є формування національної стратегії співпраці, розвиток правових гарантій для громадських організацій і розбудова загальнонаціональної мережі цифрової безпеки. Український досвід протидії інформаційному тероризму вже інтегрується в європейські й натівські стратегії безпеки та може бути адаптований іншими державами, які стикаються з подібними загрозами.

Отже, українське громадянське суспільство довело свою ефективність як потужний суб'єкт інформаційного спротиву. Його подальше інституціональне укріплення та міжнародна підтримка повинні стати пріоритетом у побудові сталої моделі інформаційної стійкості України. У роботі також обґрунтовано роль громадянського суспільства як співсуб'єкта національної інформаційної стійкості в системі протидії тероризму. Доведено, що неурядові актори (аналітичні центри, фактчекінгові ініціативи, OSINT-спільноти) виконують моніторингові, аналітичні та освітні функції, підсилюючи державну політику інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «Асиметрична» або «гібридна» війна? (Щодо нових змістів у концептах епохи постмодерну). URL: http://stratcom.co.ua/asimetrichna-abo-gibridna-vijna-shhodo-novih-zmistiv-u-kontseptah-epohi-postmodernu/ (дата звернення: 12.06.2025).

2. «Пам'ятаємо. Пишаємось. Переможемо»: серія тематичних постерів. URL: http://www.volynpost.com/news/50424-pamiataiemo-pyshaiemos-per emozhemo-seriia-tematychnyh-posteriv-foto (дата звернення: 13.07.2025).

3. «Українські кібервійська» заблокували 445 рахунків, на яких збирали кошти для терористів. URL: https://www.5.ua/suspilstvo/ukrainski-kiberviiska-zablokuvaly-445-rakhunkiv-na-iakykh-zbyraly-koshty-dlia-terorystiv-145669.html (дата звернення: 13.07.2025).

4. 29–30 березня у прес-клубі практичний тренінг «Критичне мислення та фактчекінг в умовах війни». URL: https://pressclub.te.ua/novyny/29-30-bereznya-u-pres-klubi-praktychnyj-trening-krytychne-myslennya-ta-faktcheking-v-umovah-vijny/ (дата звернення: 15.08.2025).

5. Абакумов В. М. Суб'єкти інформаційних війн: поняття та види. *Форум права*. 2009. № 2. С. 6–12.

6. Антипенко В. Ф. Тероризм: кримінологічна та кримінально-правова характеристика. Київ: НБУВ, 1999. 53 с.

7. Антифейкова інтелектуальна гра НотаЄнота. URL: https://notaenota.com/ (дата звернення:12.08.2025).

8. Артеменко Д. Проблеми розмежування диверсії і тероризму. URL: https://molodyivchenyi.ua/index.php/journal/article/view/4500/4424 (дата звернення: 11.05.2025).

9. Банахевич Ю. Українська міграція до Польщі: якою вона стане? URL: http://www.ukrinform.ua/rubric-world/2381161-ukrainska-migracia-do-polski-akou-vona-stane.html (дата звернення: 12.07.2025).

10. Банк Р. О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект. *Інформація і право*. 2016. № 1(16). С. 110–116. URL: http://ippi.org.ua/sites/default/files/17.pdf (дата звернення:).

11. Баранов О. А., Брижко В. М. Захист персональних даних в сфері Інтернет речей. *Інформація і право*. 2016. № 2. С. 85–91. URL: http://nbuv.gov.ua/UJRN/Infpr_2016_2_11 (дата звернення: 12.05.2025).

12. Бекеша О., Матюшок В., Вознюк Є. Розвиток кібербезпеки Бразилії на сучасному етапі. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2020. № 2 (406). С. 52−58.

13. Бізнес Саміт Шовкового шляху. URL: http://www.uc-fa.com/ua/novini-ta-podii/biznessamit-shovkovogo-shljahu-u-siani_-veresen-2017.htm (дата звернення: 27.08.2025).

14. Білецька Т. Медіа-тероризм як один із проявів сучасного тероризму. *Проблеми історії країн Центральної та Східної Європи.* Вип. 4. 2015. С. 210–218. URL: http://nbuv.gov.ua/UJRN/Pikctse_2015_4_19 (дата звернення: 11.07.2025).

15. Білорус О. Г. Глобалізація і національна стратегія України. Броди: Просвіта, 2001. С. 31.

16. Бойченко О. В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці. *Інтегровані інтелектуальні робототехнічні комплекси (ПРТК-2009)*: друга Міжнар. наук.-практ. конф. (25–28 трав. 2009 р.). Київ: НАУ, 2009. С. 230–232.

17. Бондар Ю. В. Свобода слова як чинник інформаційної безпеки. *Актуальні проблеми міжнародних відносин. Міжнародна інформаційна безпека: сучасні концепції і практика*. Вип. 102 (Ч. І). Київ, 2011. С. 127−129.

18. Борисова Т. М. Тенденції змін та перспективи розвитку підприємств вітчизняної некомерційної сфери. *Вісник Львівського університету*. 2013. Вип. 50. С. 3–12.

19. Боротьба з тероризмом. Київ: Знання України, 2002. С. 253.

20. Боти і бот-мережі – найнебезпечніша загроза в Інтернеті? URL: https://rmrf.tech/uk_UA/blog/rmrf-1/post/17 (дата звернення: 11.07.2025).

21. Бурячок В. Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства. *Сучасна спеціальна техніка*. 2011. № 3 (26). С. 104−114.

22. Бурячок В. Л., Киричок Р. В., Складанний П. М. Основи інформаційної та кібернетичної безпеки. Київ: КУБГ, 2019. 320 с.

23. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект. Київ: ДУТ, 2015. 288 с.

24. В Україні одна законна Церква – УПЦ: Синод Грузинської Православної Церкви висловився щодо автокефалії. URL: http://news.church.ua/2018/06/24/v-ukrajini-odna-zakonna-cerkva-upc-sinod-gruzinskoji-pravoslavnoji-cerkvi-vislovivsya-shhodo-avtokefaliji/ (дата звернення: 27.07.2025).

25. Васюта О. «iWar». Глосарій: навч. енцикл. слов.-довід. з питань інформ. безпеки / за заг. ред. д-ра. політ. наук, проф. А. М. Шуляк. Київ: МПБП «Гордон», 2019. 580 с. С.116−122.

26. Від сайту «Миротворець» вимагають видалити персональні дані журналістів. URL: https://www.pravda.com.ua/news/2016/05/11/7108087/ (дата звернення: 17.08.2025).

27. Відкриття Центру реагування на кіберзагрози. URL: https://cert.gov.ua/ news/25. 2019.04.09 (дата звернення: 15.08.2025).

28. Війна і тероризм. URL: https://www.coe.int/uk/web/compass/war-and-terrorism (дата звернення: 16.08.2025).

29. Вознюк В. С. Міжнародний тероризм в сучасних глобалізаційних стратегіях: дис. на здобуття наук. ступеня канд. політ. наук за 23.00.04 – політичні проблеми міжнародних систем та глобального розвитку. Луцьк, 2005. 192 с.

30. Вознюк Є. SWOT-аналіз стану інформаційної безпеки України. *Науковий часопис НПУ імені М. П. Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін*. 2021. 22(30). С. 116−124. DOI: 10.31392/pnspd.v22i30.1147.

31. Вознюк Є. В Інформаційна війна. Глосарій: навч. енцикл. слов.-довід. з питань інформ. безпеки / за заг. ред. д-ра. політ. наук, проф. А. М. Шуляк. Київ: МПБП «Гордон», 2019. 580 с. С. 135−138.

32. Вознюк Є. В. Гібридні загрози. Глосарій: навч. енцикл. слов.-довід. з питань інформ. безпеки / за заг. ред. д-ра. політ. наук, проф. А. М. Шуляк. Київ: МПБП «Гордон», 2019. 580 с. С. 54−56.

33. Вознюк Є. Громадські об'єднання на захисті інформаційного простору України. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2021. № 3 (11). С. 48−61.

34. Вознюк Є. Особливості поширення російських фейків в Україні. *Історико-політичні проблеми сучасного світу:* зб. наук. ст. Чернівці: Чернівец. нац. уні-т, 2021. Т. 44. С. 52−63.

35. Вознюк Є. Поширення впливу мексиканських картелів засобами інформаційних технологій і пропаганди. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини.* 2019. № 8 (392). С. 35–41.

36. Вознюк Є. Романцов Д., Рошко І. Кібербезпека в умовах російської агресії. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2020. № 2 (406). С. 58−66.

37. Вознюк Є., Андрюхіна В. Порівняльний аналіз кібербезпеки Європейського Союзу. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2025. № 2 (22). С. 161−180.

38. Вокс Україна. Офіційний сайт. URL: https://voxukraine.org/ (дата звернення: 24.07.2025).

39. Волонтери InformNapalm показали новітні російські комплекси РЕБ на Донбасі. URL: https://glavcom.ua/news/rozvidniki-informnapalm-

pokazali-novitni-rosiyski-kompleksi-reb-na-donbasi-646147.html (дата звернення: 12.08.2025).

40. Волтер Л. Витоки. Насильство, влада, терор. *Незалежний культурологічний часопис «Ї»*. 2002. № 25. С. 26–77.

41. Воронкова В. Г., Нікітенков О. Філософія цифрової людини і цифрового суспільства: теорія і практика: монографія. Львів, Торунь: Liha-Pres, 2022. 460 с.

42. Геополітичний синдром антитероризму. Київ: Політ. думка, 2003. С. 121.

43. Герасименко К. С. Сучасні ознаки загроз «інформаційного тероризму». *Форум права*. 2009. № 3. С. 162–166.

44. Геращенко О. С. Кібертероризм як фактор загрози національній безпеці України: генеза поняття та шляхи протидії. *Південноукраїнський правничий часопис*. 2016. № 3–4. С. 39–42.

45. Гетьманчук М. П. Гібридна війна Росії проти України: інформаційний аспект. *Військово-науковий вісник*. 2017. Вип. 27. С. 296–307.

46. ГО «Інформаційна безпека». URL: http://inform-security.com/ua (дата звернення: 14.07.2025).

47. Голова СБУ відкрив Ситуаційний центр забезпечення кібернетичної безпеки. URL: https://ssu.gov.ua/ua/news/1/category/ 21/view/4318.O4n8C7Vl.dp bs.2019.13.08 (дата звернення: 26.08.2025).

48. Горбенко І. Д., Долгов В. І., Гріненко Т. О. Інформаційна війна – сутність, методи та засоби ведення. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні:* матеріали ювілейної наук.-техн. конф. Київ, 1998. С. 11–15.

49. Горєвой Д. Нова інформаційна атака щодо Томосу: прийоми та маніпуляції. URL: https://prm.ua/nova-informatsiyna-ataka-shhodo-tomosu-priyomi-ta-manipulyatsiyi/ (дата звернення: 12.06.2025).

50. Грицун О. Питання міжнародно-правового регулювання інформаційного тероризму. 2014. URL: http://kul.kiev.ua/images/chasop/2014_4/CHAS14_4.pdf (дата звернення: 29.05.2025).

51. Громади Волині навчалися основ кібербезпеки. URL: https://voladm.gov.ua/new/gromadi-volini-navchalisya-osnov-kiberbezpeki/ (дата звернення: 16.08.2025).

52. Губерський Л. В., Макаренко Є. А., Камінський Є. Є. [та ін.]. Інформаційна політика України: європейський контекст: монографія. Київ: Либідь, 2007. 358 с.

53. Гхош М. Індія: розставляючи крапки над «і». Посольство Індії в Україні. Київ: [б.в], 2002. С. 2.

54. Данченко О. Рухати країну вперед повинні саме інформаційно-комунікаційні технології. URL: https://www.golos.com.ua/article/253964 (дата звернення: 24.07.2025).

55. Дерев'янко С. М. Гібридна війна: інформаційно-безпековий вимір. *Вісник Прикарпатського університету. Серія: Політологія* / Прикарпат. нац. ун-т ім. Василя Стефаника. Одеса: Гельветика, 2024. Вип. 18. С. 101–113. DOI: 10.32782/2312-1815/2024-18-11.

56. Дерев'янко С. Народовладдя у безпековому вимірі. *Актуальні проблеми політики, інформації та безпеки*: монографія / [за ред. Марчука В. В.]; Прикарпат. нац. ун-т ім. В. Стефаника; Ф-т іст., політол. і міжнар. відносин. Івано-Франківськ: Ярина, 2022. С. 4–29.

57. Держави-жертви кібератак у 2013 році. URL: http://telecomblogs.in/blog/2013//what-you-should-know-about-nettraveler-attack/ (дата звернення: 13.07.2025).

58. Доброжанська О. Л., Демцов А. А. Кібербезпека як феномен міжнародних відносин на прикладі Федеративної Республіки Німеччини. *Актуальні проблеми міжнародних відносин*. 2011. №102. С. 111–116.

59. Довженко М. Маніпуляції року або рік маніпуляцій. *Підсумки огляду телетижневиків 2019 року*.

URL: https://detector.media/teletizhneviki/article/173617/2019-12-30-manipulyatsii-roku-abo-rik-manipulyatsii-pidsumki-oglyadu-teletizhnevikiv-2019-roku/ (дата звернення: 11.08.2025).

60. Довженко О. Фейковий Бойко як тест на адекватність журналістів. URL: https://detector.media/infospace/article/143389/2018-12-16-feikovii-boiko-yak-test-na-adekva tnist-zhurnalistiv/ (дата звернення: 25.07.2025).

61. Доктрина информационной безопасности Российской Федерации. URL: www.russianenterpricesolutions.com/help/dib.html (дата звернення: 18.09.2019).

62. Дорошкевич А. С. Гібридна війна в інформаційному суспільстві *Вісник національного ун-ту «Юридична академія України ім. Ярослава Мудрого». Серія: Філософія, філософія права, політологія, соціологія.* 2015. № 2. С. 21–28.

63. Дослідження USAID «Disinformation Primer for Democracy Assistance». 2021. URL: https://www.echocommunity.org/resources/319e91d9–41ef–4fd7–aff3–d429b5774801 (дата звернення: 20.07.2025).

64. Дубов Д. В. Стратегічні комунікації: проблеми концептуалізації та практичної реалізації. *Стратегічні пріоритети.* № 4 (41). 2016. С. 12.

65. Дуцик Д., Плис А., Сичова А. [та ін.]. Як функціонують та завойовують аудиторію неінституціоналізовані новинні телеграм-канали українського сегменту. *Аналітичний звіт*. Київ: ГО «Укр. ін-т медіа та комунікації», 2023. 68 с. URL: https://ekmair.ukma.edu.ua/items/889ea882-7c83-4515-8878-e7727cdf8e9a (дата звернення: 11.07.2025).

66. Ємельянов В. П. Злочини терористичної спрямованості. Харків: Рубікон, 1997. 160 с.

67. Жайворонок О. Причини і джерела ескалації інформаційного тероризму в Україні та світі. *Міжнародне право*. 2019. №10. С. 218–223. DOI: 10.32849/2663-5313/2019.10.38.

68. Жителів Донбасу очікує насильницьке переселення «до Львова на перевиховання». URL: https://www.stopfake.org/uk/fejk-zhiteliv-donbasu-

ochikuye-nasilnitske-pereselennya-do-lvova-na-perevihovannya/ (дата звернення: 15.07.2025).

69. Зайцев Г. В., Коломієць Н. В. Диверсія та терористичний акт, проблеми кваліфікації. *Аналітично-порівняльне правознавство*. С. 573. URL: http://journal–app.uzhnu.edu.ua/article/view/294809. (дата звернення: 17.06.2025).

70. Закон України «Про громадські об'єднання». *Відомості Верховної Ради України (ВВР)*. 2013. № 1. Ст. 1. URL: https://zakon.rada.gov. ua/laws/show/4572-17#Text (дата звернення: 12.07.2025).

71. Закон України «Про національну безпеку України». URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 12.07.2025).

72. Закон України «Про основи національної безпеки України». URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355 (дата звернення: 12.07.2025).

73. Збитки WannaCry. URL: https://www.epravda.com.ua/news/ 2017/05/25/625286 (дата звернення: 28.06.2025).

74. Зелений і безпечний Європейський Союз: монографія / [А. О. Бояр (кер. авт. кол.), І. В. Кицюк, Н. І. Романюк та ін.]; за ред. А. О. Бояра, В. Й. Лажніка. Луцьк: Вежа-Друк, 2023. С. 82–84.

75. Зубар Н. Інформаційна безпека в реалі в епоху інформаційної війни. URL: https://maidan.org.ua/da/2014/02/natalka-zubar-informatsijna-bezpeka-v-reali-v-epohu-informatsijnoji-vijny/ (дата звернення: 12.07.2025).

76. Ілляшенко А. В., Кіяшко Ю. М. Інформаційний тероризм як злочинна діяльність міжнародного масштабу. *Журнал східноєвропейського права*. 2016. № 27. С. 94–100. URL: https://tinyurl.com/yu632jp7 (дата звернення: 21.07.2025).

77. Ільницька У. В. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним

впливам. *Гуманітарні візії*: наук. журн. Львів: Вид-во НУ «Львівська політехніка», 2016. Вип. № 3. С. 27–33.

78. Інститут демократії імені Пилипа Орлика. Інформаційний простір України: нагальні виклики. URL: https://www.slideshare.net/UkraineCrisisMediaCenter/ss-54338467 (дата звернення: 17.05.2025).

79. Інститут інформаційної безпеки. URL: https://www.infosecurity.institute/ (дата звернення: 25.07.2025).

80. Інформаційна система Національного агентства із забезпечення якості вищої освіти. URL: NAQA.Svr (дата звернення:13.06.2025).

81. Інформаційний комісар чи сильний омбудсман: хто захистить право на інформацію? 8 Вересня 2020. URL: https://dostup.org.ua/explainers/publications/informatsiinyi-komisar-chy-sylnyi-ombudsman-khto-zakhystyt-pravo-na-informatsiiu (дата звернення: 15.07.2025).

82. Інформаційний комісар: хто захищатиме доступ до інформації. 2017. URL: https://dostup.pravda.com.ua/stories/publications/informatsiinyi-komisar-khto-zakhyshchatyme-dostup-do-informatsii (дата звернення: 13.06.2025).

83. Канцелярук Б. Геополітичний синдром антитероризму. Київ: Політ. думка, 2003. С. 7.

84. Канцелярук Б. І. Кризовість як інгредієнт поступу. *Дослідження світової політики*: зб. наук. праць. Київ, 2000. Вип. 9. С. 3–7.

85. Канцелярук Б. І. Наукове пізнання у «викликах» часу. *Дослідження світової політики*: зб. наук. праць. Київ, 2003. Вип. 24. С. 11.

86. Капітоненко М. Г. Системний підхід в дослідженні міжнародного конфлікту. *Дослідження світової політики*. Вип. 20. Київ: ІСЕМВ НАНУ, 2002. С. 186–194.

87. Карпчук Н. П. Посередницька війна. Глосарій: навч. енцикл. слов.-довід. із питань інформ. безпеки / за заг. ред. д-ра. політ. наук, проф. А. М. Шуляк. Київ: МПБП «Гордон», 2019. 580 с. С. 363–366.

88. Карпчук Н. П. Фейкова інформація. Глосарій: навч. енцикл. слов.-довід. із питань інформ. безпеки / за заг. ред. д–ра. політ. наук, проф. А. М. Шуляк. Київ: МПБП «Гордон», 2019. 580 с. С. 519–523.

89. Карпчук Н., Юськів Б., Пелех О. Структура стратегічних комунікацій як основа ефективного комунікаційного менеджменту України в умовах війни. *Міжнародні відносини, суспільні комунікації та регіональні студії*. № 2 (16). 2023. URL: https://relint.vnu.edu.ua/index.php/relint/article/view/318 (дата звернення: 28.07.2025).

90. Качинська Н. О. Хактивізм: соціально-політичний протест онлайн. URL: http://istfak.org.ua/tendentsiirozvytku-suchasnoi-systemy-mizhnarodnykh-vidnosyn-ta-svitovho-politychnoho-protsesu/188 (дата звернення: 24.07.2025).

91. Кібератаки проти Естонії. URL: https://uk.wikipedia.org/wiki97_(2007) (дата звернення: 11.08.2025).

92. Кібербезпека. URL: http://start.karazin.ua/programs/5/7/125/31 (дата звернення: 11.08.2025).

93. Кіпа О. О. Правопорушення в мережі Інтернет. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/23673/83-Kipa.pdf?sequence=1 (дата звернення: 17.05.2025).

94. Класифікація заходів із забезпечення інформаційної безпеки регіону. URL: https://journals.khnu.km.ua/vestnik/pdf/ekon/2010_1_2/pdf/251-254.pdf (дата звернення: 11.08.2025).

95. Климосюк А. С. Співвідношення диверсії (ст. 113 КК України) і терористичного акту (ст. 258 КК України). URL: https://dspace.nlu.edu.ua/handle/123456789/14854 (дата звернення:13.05.2025).

96. Комплексний підхід до боротьби з кіберзлочинністю в Європі. URL: http://dspace. oduvs.edu.ua/bitstream/20.pdf (дата звернення: 20.08.2025).

97. Конах В. К. Загрози та виклики національним інтересам України в інформаційній сфері в умовах глобалізації. *Стратегічні пріоритети*. 2014. № 2. С. 73–78.

98. Кондратова В. Донбасс – бандеровцам, или Спасти пропагандистку Скабееву. Фейк месяца с #Медиагигиена. URL: https://www.liga.net/politics/articles/donbass-banderovtsam-ili-spasti-propagandistku-skabeevu-feyk-mesyatsa-s-mediagigiena (дата звернення: 12.08.2025).

99. Конфіденційність та захист даних. Європейський парламент. URL: https://tinyurl.com/y365zzjz (дата звернення: 16.08.2025).

100. Кончаковська В. В., Кравчук А. С. Тероризм як злочинне явище: еволюція та заходи запобігання. URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/19042/Konchakovskaya_Kravchuk.pdf;jsessionid=A1BA841A6C18AE0BA6982ABABF7E00F3?sequence=1 (дата звернення: 26.07.2025).

101. Кормич Б. А. Інформаційна безпека: організаційно-правові основи. Київ: Кондор, 2004. 384 с.

102. Кормич Б. А. Класифікація видів інформаційної безпеки. *Митна справа*. 2004. № 5. С. 39–44.

103. Кормич Б. А. Компетенція держави у сфері інформаційної безпеки. *Митна справа*. 2005. № 1. С. 72–80.

104. Коршунов В. О. Політичний тероризм: інформаційні методи боротьби: автореф. дис. на здобуття наук. ступеня канд. політ. наук: спец. 23.00.02. Дніпропетровськ, 2008. 18 с.

105. Косовська криза і міжнародне втручання: уроки для Європи. *Дослідження світової політики*: зб. наук. праць. Київ, 2001. Вип. 17. С. 69–75.

106. Коцур В. Тероризм і засоби масової інформації: межа об’єктивності і мас-медіального продовження терактів. *Політичний менеджмент*. 2009. No 6. С. 167–172.

107. Криза «подвійного стримання»: американська політична думка про політику США в Перській затоці (кінець 90–х рр. XX ст.). *Дослідження світової політики*: зб. наук. праць. Київ, 2001. Вип. 18. С.

108. Кримінальний кодекс України. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 12.05.2025).

109. Кримський С. Б. Цивілізаційні виміри сучасності. Київ: Либідь, 1999. 304 с.

110. Кудінов С. С., Рижов І. М., Романов М. С. Основи терорології: навч. посіб. Острог: Нац. ун-т «Острозька академія», 2020. 234 с. С. 22.

111. Кулеба Д. Війна за реальність: як перемагати у світі фейків, правд і спільнот. Київ: Книголав, 2019. С. 70.

112. Кулик С., Вознюк Є. Фейк російської пропаганди: Олена Підгрушна – снайпер АТО. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2021. № 1 (9). С. 83−101.

113. Курбан О. Сучасна гібридна війна: нові форми агресії. URL: http://ua.racurs.ua/1063-suchasna-gibrydna-viyna-ta-yiyi-vidobrajennya-u-virtualniy-realnosti-chastyna-2 (дата звернення: 15.08.2025).

114. Кушніренко В. Ісламське суспільство та його вестернізація. *Політичний менеджмент*. 2003. № 1. С. 136.

115. Лабенко Л. В. Інформаційний тероризм: поняття та ознаки. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/11e0462a-321d-4751-ba49-9038f5effd6b/content (дата звернення: 11.06.2025).

116. Лабенко Н. В. Інформаційний тероризм як форма сучасної агресії: теоретичний і прикладний аспекти. *Політичне життя.* 2020. № 3. С. 57–64.

117. Лабораторія цифрової безпеки. Офіційний сайт. URL: https://dslua.org. (дата звернення: 25.08.2025).

118. Лебедєва О., Шепелева А. Росія очолила світовий рейтинг кіберзлочинності. URL: https://www.dw.com/uk/rosia-ocolila-svitovij-rejting-kiberzlocinnosti-z-vidrivom-za-neu-ukraina/a-68792554 (дата звернення: 11.04.2024).

119. Левада-Центр. Массовые представления о дружественных и недружественных странах, отношение к некоторым странам.

URL: https://www.levada.ru/2024/06/14/massovye-predstavleniya-o-druzhestvennyh-i-nedruzhestvennyh-stranah-otnoshenie-k-nekotorym-stranam/ (дата звернення: 16.07.2025).

120. Лисько Т. Д., Клімук О. О., Лисянська Д. В. Інформаційний тероризм як загроза національній безпеці та спосіб інформаційної війни. DOI: 10.32782/2524-0374/2022-10/143 (дата звернення: 21.07.2025).

121. Ліпкан В. А. Тероризм і національна безпека України. Київ: Знання, 2000. С. 182 с.

122. Ліпкан В. А. Інформаційна безпека як складова національної безпеки України. *«Інформаційні технології в економіці, менеджменті і бізнесі: Проблеми науки, практики і освіти»:* зб. наук. праць VIII Міжнар. наук.-практ. конф. Ч. 2. К.: Вид-во Європ. у-ту, 2003. С. 443–453.

123. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції. Київ: КНТ, 2006.

124. Ліпкан В. А., Никифорчук Д. Й., Руденко М. М. Боротьба з тероризмом. Київ: Знання України, 2002. С. 29–44. С. 227.

125. Ліпкан В. Поняття та структура стратегічних комунікацій на сучасному етапі державотворення URL: https://www.lipkan.com/ponyattya-ta-struktura-strategichnih-komunikatsij-na-suchasnomu-etapi-derzhavotvorennya/ (дата звернення: 12.08.2025).

126. Лук'янчикова В. Ю. Кіберпростір: загрози для міжнародних відносин та глобальної безпеки. *Гілея: науковий вісник.* 2013. № 72. С. 793–796.

127. Луць В. Медіавійна (медіапротистояння). *Новітня політична лексика (неологізми, оказіоналізми та інші новотвори)*. Львів: Новий світ-2000. 2015. С. 214–215.

128. Мазур П. «Ісламський глобальний медіа-фронт (GIMF)». *Глосарій:* навч. енцикл. слов.-довід. із питань інформ. безпеки / за заг. ред. д-ра. політ. наук, проф. А. М. Шуляк. Київ: МПБП «Гордон», 2019. 580 с. С. 190–192.

129. Макаренко Є. А., Рижиков М. М, Ожеван М. А. [та ін.]. Міжнародна інформаційна безпека: сучасні виклики та загрози. Київ: Центр вільної преси. 2006. 916 с.

130. Максим Х. Феномен інформаційної агресії в умовах повномасштабної війни Росії проти України. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки»*. 2023. № 2 (38). С. 72–78.

131. Малик Я. Й. Інформаційна війна і Україна. *Демократичне врядування*. 2015. Вип. 15. URL: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3 (дата звернення: 22.12.2020).

132. Малинка В. Очільник «Українських кібервійськ»: «Україна – одна з найбільш легковажних країн у питанні кібербезпеки». URL: https://dt.ua/personalities/ochilnik-ukrayinskih-kiberviysk-ukrayina-odna-z-nay bilsh-legkovazhnih-krayin-u-pitanni-kiberbezpeki-html (дата звернення: 17.08.2025).

133. Малинка В. Топ-10: фейки 2018 року. URL: https://ms.detector.media/ethics/standards/pobrekhenki_roku_dobirka_sokovitikh_feykiv_2018go/ (дата звернення: 08.06.2025).

134. Малігонов М. Обережно! Боти серед нас. Як врятуватися? URL: http://idecide.com.ua/botofermal (дата звернення: 13.08.2025).

135. Маркова М. В. Інформаційно-психологічна війна як нова загроза здоров'ю населення України: реальність небезпеки та напрями протидії. URL: https://health-ua.com/article/5219-nformatcjnopsihologchna-vjna-yak-nova-zagroza-zdorovyu-naselennya-ukrani-re (дата звернення: 24.07.2025).

136. Маруненко О. Зовнішні і внутрішні інформаційні війни у медійному просторі України. *Освіта регіону. Політологія, психологія, комунікації. Український науковий журнал*. 2011. № 4. С. 92.

137. Марунченко О. П. Інформаційна війна у сучасному політичному просторі: автореф. дис. на здобуття наук. ступеня канд. політ. наук. Одеса, 2013. 20 с.

138. Марущак А. І. Вплив міжнародних процесів регулювання штучного інтелекту на інформаційне право України. URL: http://il.ippi.org.ua/article/view/291582 (дата звернення: 17.07.2025).

139. Марущак А. І. Передумови для формування правових механізмів протидії дезінформації в соціальних медіа у контексті національної безпеки: постановка проблеми. URL: http://il.ippi.org.ua/article/view/254345 (дата звернення: 16.07.2025).

140. Марущак А. І., Петров С. Г. Правові механізми ЄС та США для виявлення і блокування російської дезінформації у соціальних мережах. URL: http://il.ippi.org.ua/article/view/317797 (дата звернення: 11.08.2025).

141. Матвіїшин І. Мемократія: як соцмережі впливають на політику в Україні. URL: https://rubryka.com/article/yak-sotsmerezhi-vplyvayut-na-polityku-v-ukrayini (дата звернення: 29.07.2025).

142. Матула М. М. Феномен інформаційного тероризму як загрози національній та міжнародній безпеці. URL: http://naub.oa.edu.ua/2014/fenomen-informatsijnoho-teroryzmu-yakzahrozy-natsionalnij-ta-mizhnarodnij-bezpetsi/ (дата звернення: 08.08.2025).

143. Медіаграмотність – основа інформаційної безпеки. URL: https://www.golos.com.ua/article/374808 (дата звернення: 14.06.2025).

144. Медіаграмотність та інформаційна гігієна: що це і навіщо? URL: https://ukr-day.com/media-literacy-information-hygiene-what-it/ (дата звернення: 14.06.2025).

145. Мефодієв К. За антиукраїнськими акціями у Польщі стоїть Кремль – аналіз викритого листування. URL https://informnapalm.org/ua/za-antyukrayinskymy-aktsiyamy-v-polshhi-stoyit-kreml/ (дата звернення: 17.08.2025).

146. Мирянин В. Информационные манипуляции «ПЦУ». URL: https://spzh.news/ru/socseti/66930-informacionnyje-manipulyacii-pcu (дата звернення: 04.06.2025).

147. Митко А., Кольцова І. Інформаційна безпека в контексті введення інституту інформаційного комісара (омбудсмена) в Україні. *Медіафорум.* 2018. 6. С. 116.

148. Михайлин І. Л. Основи журналістики. Київ: ЦУЛ. 2002. С. 21.

149. Міжнародна діяльність кафедри журналістики. URL: https://journalism.chnu.edu.ua/spivpratsia/ (дата звернення: 12.05.2025).

150. Мова ворожнечі в друкованих ЗМІ Донбасу по обидві сторони лінії фронту: дослідження. URL: http://dii.dn.ua/analytics/125-mova-vorozhnechi-v-drukovanykh-zmi-donbasu-poobydvi-storony-linii-frontu (дата звернення: 30.06.2017).

151. Моренчук А., Марчук А. Антиукраїнські протести в Польщі: польський націоналізм чи російська пропаганда? *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2019. № 1. С. 115–123.

152. Мусаєва-Боровик С. Заява журналістів щодо оприлюднення бази контактів сайтом «Миротворець». URL: https://blogs.pravda.com.ua/ authors/musaieva/5732e403bdf48/ (дата звернення: 13.07.2025).

153. Нагорна К. Г. Розмежування диверсії і терористичного акту (ст. 113 і ст. 258 КК України). *Всеукраїнський саміт приватних детективів*: матеріали доп. (м. Дніпро, 30 лист. 2017 р.). Дніпро: ДДУВС, 2018. С. 145–151.

154. Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз: нац. доп. / ред. кол. С. І. Пирожков, О. М. Майборода, Н. В. Хамітов, Є. І. Головаха, С. С. Дембіцький, В. А. Смолій, О. В. Скрипнюк, С. В. Стоєцький / Ін-т політ. і етнонац. дослідж. ім. І. Ф. Кураса НАН України. Київ, 2022. 552 с.

155. Національний інститут стратегічних досліджень. Оцінка терористичних ризиків для України в умовах гібридної війни. 2022. URL: https://niss.gov.ua (дата звернення: 16.07.2025).

156. Нестеренко О. Інформаційний омбудсман в механізмі забезпечення прав людини і основоположних свобод. *Права людини.* 2008. URL: http://khpg.org/index.php?id=1216383271 (дата звернення: 28.05.2025).

157. Ничипорчук Н., Вознюк Є. Секрет успіху США у сфері інформаційної безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2018. № 1(3). С. 66−71.

158. Ніколаєнко Н. Інформаційний фронт російсько-української гібридної війни. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2022. № 4(12). С. 109–114.

159. Ніколаєнко Н. О. Загрози українським державним інтересам у Чорноморському регіоні: історико-політичний аспект. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2023. № 2 (16). С. 86–91.

160. Ніколаєнко Н. О. Маніпулятивний характер російських засобів масової комунікації в умовах російсько-української гібридної війни. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2020. № 1(7). С. 93–104.

161. Ніколаєнко Н. О., Шуляк С. О. Основні тенденції процесу трансформації державних та політичних інститутів в Україні в умовах російсько-української війни. *Acta Securitatae Volynienses*. 2024. № 4. С. 24–31.

162. Ніколаєнко Н., Макаренко Л. Міжнародні відносини та політичні процеси в країнах Чорноморського регіону в контексті російсько-української війни. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2022. № 4(12). С. 5–16.

163. Німецька кіберзлочинність. URL: http://www.dw.com/uk/%D1%838C/a-3855519 (дата звернення: 11.07.2025).

164. Новий час. URL: https://nv.ua/ukr/techno/it-industry/eksperti-vijavili-virus-jakij-fizichnoposhkodzhuje-smartfoni-dobuvajuchi-kriptovaljuta-2409883.html (дата звернення: 19.07.2025).

165. НотаЄнота. Офіційний сайт. URL: https://notaenota.com/ (дата звернення: 12.08.2025).

166. Омельчук В. А. Роль держави у забезпеченні інформаційної безпеки в умовах глобалізації: реалії і перспективи. *Інформаційна безпека людини, суспільства, держави*. 2012. № 3. С. 6–10.

167. Організація Американських держав. URL: https://mfa.gov.ua/ua/about-ukraine/international-organizations%D0% BE%D0%B0s (дата звернення: 19.05.2025).

168. Остроухов В. В., Рижов І. М. Філософське підґрунтя соціально-інформаційних концепцій профілактики тероризму. *Інформаційна безпека людини, суспільства, держави*. 2013. № 2. С. 13–19.

169. Офіційний маніфест із вимогами «жовтих» жилетів виявився фейком – розслідування «Української правди». URL: https://ms.detector.media/ethics/manipulation/ofitsyniy_manifest_iz_vimogami_zhovtikh_zhiletiv_viyavivsya_feykom_rozsliduvannya_ukrainskoi_pravdi/ (дата звернення: 19.08.2025).

170. Парфенюк І. М. Псевдоподії в інформаційних війнах. «*Комунікаційно-контентна безпека в умовах гібридно-месіанських агресій путінської Росії*»: тези доп. Міжнар. форуму з кризових комунікацій / за заг. ред. В. Балабіна. Київ: ВІКНУ, 2016. С. 78.

171. Патрико З. В. Теорія масової інформації та комунікації: навч. посіб. Львів: Афіша. 2008. С. 18.

172. Паш Б. В. Складові інформаційної безпеки держави: постановка питання. URL: https://dspace.uzhnu.edu.ua/server/api/core/bitstreams/6202e934-9175-4f84-8b89-455da60a1d84/content (дата звернення: 17.06.2025).

173. Пелещак О. Р. Деякі аспекти кримінально-правової характеристики кібердиверсій. *Соціально-правові студії*. 2020. Вип. 3 (9). С. 26–33. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://sls-journal.com.ua/web/uploads/pdf/S&LS_2020_Vol.%203,%20No.%203_26-33.pdf (дата звернення: 17.07.2025).

174. Перший канал видав білоруса за розчарованого Євромайданом українця. URL: https://ms.detector.media/ethics/manipulation/pervyy_kanal_

vidav_bilorusa_za_rozchrovanogo_evromaydanom_ukraintssya/ (дата звернення: 12.07.2025).

175. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. Київ, 2009. № 5. С. 122–134.

176. Піпченко Н. Дипломатія в епоху штучного інтелекту. *Україна дипломатична*. 2024. № 25. С. 805–811.

177. Піпченко Н. Трансформація зовнішньополітичної комунікації ЄС, Німеччини та України. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2022. № 2 (13). С. 91–101.

178. Піпченко Н., Лепеха Я. Підтримка зовнішньополітичної діяльності Німеччини інструментами стратегічних комунікацій. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2023. № 1 (15). С. 75–90.

179. Погорецький М. А., Шеломенцев В. П. Поняття кіберпростору як середовища вчинення злочину. *Інформаційна безпека людини, суспільства, держави.* 2009. № 2 (2). С. 80.

180. Покальчук О. Проксі-війна і інформаційні операції. URL: https://ukr.lb.ua/society/2017/12/13/384643_proksiviyna_i_informatsiyni.html (дата звернення: 16.08.2025).

181. Польща потерпає від російської пропаганди після початку війни в Україні – Марчін Рей. URL: https://hromadske.radio/podcasts/dno/z-pochatkom-revolyuciyi-gidnosti-ta-viyny-u-polshchi-vidbuvsya-splesk-dezinformaciyi-ta-propagandy-vid-rf-marchin-rey (дата звернення: 11.08.2025).

182. Постанова Верховної Ради України «Про Концепцію (основи державної політики) національної безпеки України». *Голос України*. 1997. № 3/97 ВР. URL: https://zakononline.ua/documents/show/184875___642945 (дата звернення: 07.07.2025).

183. Почепцов Г. Війна четвертого покоління – це війна культур. URL: https://www.ar25.org/article/viyna-chetvertogo-pokolinnya-ce-viyna-kultur.html (дата звернення: 18.08.2025).

184. Почепцов Г. Інформаційний простір як ключовий для розвитку країни. URL: https://ms.detector.media/ethics/manipulation/informatsiyniy_prostir_yak_klyuchoviy_dlya_rozvitku_kraini/undefined/undefined/undefined/ (дата звернення: 13.07.2025).

185. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/main/685/2021 (дата звернення: 10.07.2025).

186. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/main/96/2016 (дата звернення: 10.07.2025).

187. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». *УКАЗ ПРЕЗИДЕНТА УКРАЇНИ* № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення: 10.07.2025).

188. Пропозиція ЄС щодо нормативно-правового врегулювання питання щодо штучного інтелекту. URL: https://www.nrada.gov.ua/propozytsiya-yesshhodo-normatyvno-pravovogo-vregulyuvannya-pytannya-shhodo-shtuchnogointelektu/ (дата звернення: 17.06.2025).

189. Протидія дезінформації: інформаційна безпека громади. URL: https://ndu.kr.ua/562-protidiya-dezinformatsiji-informatsijna-bezpeka-gromadi (дата звернення: 19.07.2025).

190. Радутний О. Е. Поняття та ознаки інформаційної агресії на законодавчому рівні в кримінально-правовій сфері. DOI: 10.37750/2616-6798.2015.2(14).272668. (дата звернення: 12.08.2025).

191. Резнікова О. О., Місюра А. О., Дрьомов С. В., Войтовський К. Є. Актуальні питання протидії тероризму у світі та в Україні: аналіт. доп. Київ: НІСД, 2017. 60 с.

192. Результати інформаційно-просвітницької кампанії з протидії дезінформації. URL: https://cedem.org.ua/news/rezultaty-informatsijno-

prosvitnytskoyi-kampaniyi-z-protydiyi-dezinformatsiyi/ (дата звернення: 28.08.2025).

193. Рєзнікова О. О. Національна стійкість в умовах мінливого безпекового середовища: монографія. Київ: НІСД, 2022. 532 с.

194. Робота із соціальними мережами: посіб. з питань використання соц. мереж, розроблений Департаментом преси і публічної інформ. Консультативної місії ЄС в Україні. Київ, 2020. URL: https://www.euam-ukraine.eu/wp-content/uploads/2020/09/Working-with-Social-Media-Compendium-UKRAINIAN-AUGUST-2020-FOR-PUBLICATION.pdf (дата звернення: 24.07.2025).

195. Розвиток медіаграмотності на Рівненщині як засобу протидії пропаганді протягом 2022–2024 років. URL: https://itvmg.com/news/rozvitok-mediahramotnosti-na-rivnenshchini-yak-zasobu-protidii-propahandi-protyahom-2022-2024-rokiv-106148 (дата звернення: 17.08.2025).

196. Романюк В. С. Дискредитація української армії як наратив російської пропаганди. *Комунікаційно-контентна безпека в умовах гібридно-месіанських агресій путінської Росії:* тези доп. Міжнар. форуму з кризових комунікацій / за заг. ред. В. Балабіна. Київ: ВІКНУ, 2016. С. 133.

197. Роскомнагляд заблокував доступ до сайта InformNapalm. URL: https://detector.media/infospace/article/170075/2019-08-22-roskomnaglyad-zabl okuvav-dostup-do-saita-informnapalm/ (дата звернення: 24.07.2025).

198. Рудич Ф. Політична наука в Україні: стан і перспективи. *Політичний менеджмент*. 2003. № 1. С. 14.

199. Рудник Л. І. Соціальні мережі як засіб здійснення терористичних актів. URL: https://goal-int.org/socialni-merezhi-yak-zasib-zdijsnennya-teroristichnixaktiv (дата звернення: 12.08.2025).

200. Савчук Т. Індустрія маніпуляцій: скільки коштує вплив на вашу думку в соцмережі (недорого). URL: https://foreignpolicy.com.ua/suspilstvo/industriia-manipuliatsii-skilky-koshtuie-vplyv-na-vashu-dumku-v-sotsmerezhi-

nedoroho/?fbclid=IwAR0-pAx44OEojRY27Ky-S3bdqhx17GhFpLtKr8hrilRzIKORVB8zu6l7soo (дата звернення: 16.08.2025).

201. Саган О. В. Протидія медіаінформаційному тероризму як питання національної безпеки України: дис. на здобуття наук. ступеня канд. політ. наук: 21.01.01. Київ, 2021. 224 с.

202. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. URL: http://search.ukr.net/?go=http%3A%2F%2Fjourn.univ.kiev.ua%2Ftrk%2Fpublikacii%2Fsatshuk_publ.php (дата звернення: 13.07.2025).

203. СБУ ліквідувала мережу ботоферм у дев'ятьох областях із 200-тисячною аудиторією. URL: https://detector.media/infospace/article/210853/2023-05-04-sbu-likviduvala-merezhu-botoferm-u-devyatokh-oblastyakh-iz-200-tysyachnoyu-audytoriieyu/ (дата звернення: 03.08.2025).

204. Світ проти кремлівської пропаганди: Mythbusters, бойкот RT та «антиколорадські» наклейки. URL: http://tyzden.ua/News/135174 (дата звернення: 16.07.2025).

205. Семен Н. Ф. Соціальні мережі як один з найефективніших засобів протидії інформаційній агресії в українському інтернет-просторі. URL: http://ena.lp.edu.ua:8080/xmlui/handle/ntb/43011 (дата звернення:12.07.2025).

206. Семенець О., Суботін К. Завдяки стратегії «аутсорсінгу». *Політика і час*. 2004. № 1. С. 35–40.

207. Сенченко М. Невидимі інформаційні війни нового покоління: Теорія мережецентричної війни на практиці. *Вісник Книжкової палати.* 2011. № 11. С. 3–6.

208. Сливка С. С. Філософія міжнародного тероризму: правовий вимір. Спеціальність 12.00.12 – філософія права: дис. на здобуття наук. ступеня д-ра юрид. наук. Львів, 2011. С. 453.

209. Спецпроєкт Фільтра про ТОП-10 найбільш медіаграмотних країн Європи. URL: https://filter.mkip.gov.ua/speczproyekt-filtra-pro-top-10-najbilsh mediagramotnyh-krayin-yevropy/ (дата звернення: 12.07.2025).

210. Список журналістів, акредитованих в терористичній організації «ДНР». URL: https://myrotvorets.news/spysok-zhurnalystov-akkredytovannyh-terrorystycheskoj-organyzatsyej-dnr/ (дата звернення: 16.08.2025).

211. Список-1097: спікер InformNapalm розповів, які військові РФ захоплювали. URL: https://uatv.ua/spysok-1097-spiker-informnapalm-rozpo viv-yaki-vijskovi-rf-zahoplyuvaly-krym-video/ (дата звернення: 16.08.2025).

212. Стартує курс для освітян із проведення антифейкових ігор «НотаЄнота» для учнів та молоді. URL: https://pon.org.ua/novyny/11022-startuie-kurs-dlia-osvitian-iz-provedennia-antyfeikovykh-igor-notayenota-dlia-uchniv-ta-molodi.html (дата звернення: 20.08.2025).

213. Степанова Ю. П. Спільність і відмінність об'єктивних ознак терористичного акту та диверсії. URL: https://univd.edu.ua/general/publishing/konf/18_04_2019/pdf/88.pdf (дата звернення: 12.05.2025).

214. Стичинська А. Б. Інформаційна агресія Російської Федерації: виклики та подолання. URL: file:///C:/Users/user/Downloads/15019-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-29886-1-10-20240219%20(1).pdf (дата звернення: 16.07.2025).

215. Стратегічні комунікації ЄС: протидія деструктивним впливам: кол. моногр. / за заг. ред. д-ра політ. наук, проф. Н. Карпчук. Луцьк: Вежа-Друк, 2023. 308 с.

216. Суслов А. Інформаційні маніпуляції УПЦ (МП): чи справді Грузинська Церква проти автокефалії? URL: https://spa.ukma.edu.ua/info_manipulations_uoc_mp_georgia/ (дата звернення: 27.07.2025).

217. Суслова І. Хто захистить наше право на інформацію? 2017. URL: http://blog.liga.net/user/isuslova/article/25691 (дата звернення: 20.05.2018).

218. Телешун С. Електронний інформаційний простір і публічна політика. URL: https://ipiend.gov.ua/wp-content/uploads/2018/08/teleshun_elektronnyi.pdf (дата звернення: 05.07.2025).

219. Телешун С. О., Рейтерович І. В. Моніторинг джерел інформації в системі державного управління; за заг. ред. проф. С. О. Телешун. Київ: НАДУ, 2009. 36 с.

220. Телешун С. О. Сучасний тероризм – українські реалії. *Політичний менеджмент*. 2005. № 1. С. 166.

221. Тероризм: кримінологічна детермінація і кримінально-правова протидія: монографія / В. В. Середа, І. Р. Серкевич; за заг. ред. В. С. Канціра. Львів: ЛьвДУВС, 2016. 188 с.

222. Тихомирова Є. Б. «StopFake.org». Боротьба з неправдивими відомостями. *Глосарій:* навч. енцикл. слов.-довід. із питань інформ. безпеки / за заг. ред. д-ра політ. наук, проф. А. М. Шуляк. Київ: МПБП «Гордон», 2019. 480 с. С. 462.

223. Токаревський Г. «Собаки пекла» повертаються. *Політичний менеджмент*. 2003. № 1. С. 128–135.

224. Токарюк О. Росія «закріплюється» в Киргизстані. *Газета «День».* № 191. 2003. URL: https://day.kyiv.ua/article/panorama-dnya/rosiya-zakriplyuyetsya-v-kyrhyzstani (дата звернення: 06.07.2025).

225. Требін М. П. Феномен інформаційної війни у світі, що глобалізується. *Вісник національного університету юридичної академії України ім. Ярослава Мудрого*. 2013. Вип. 2. С.188–198.

226. У InformNapalm вказали на слабкість російської армії. URL: https://www.segodnya.ua/ua/world/russia/v-informnapalm-ukazali-na-slabost-rossiyskoy-armii-1051699.html (дата звернення: 17.07.2025).

227. У Рівному почнуться безкоштовні курси медіаграмотності. Як записатися. URL: https://ogo.ua/u-rivnomu-pochnutsya-bezkoshtovni-kursy-mediahramotnosti-yak-zapysatysya/ (дата звернення: 20.08.2025).

228. Український інститут медіа та комунікації. Офіційний сайт. URL: https://www.jta.com.ua/pro-ho-ukrainskyy-instytut-media-ta-komunikatsii/ (дата звернення: 16.08.2025).

229. Український кейс (2022–2024). Звіт Центру стратегічних комунікацій при МКІП. URL: https://mcsc.gov.ua/wp-content/uploads/2025/01/zvit-shhodo-vykonannya-planu-zahodiv-z-realizacziyi-strategiyi-informaczijnoyi-bezpeky-za-2023-rik.pdf (дата звернення: 25.08.2025).

230. Українські кібервійська заявили, що «поклали» 187 сайтів терористичних організацій. URL: https://gordonua.com/ukr/news/society/-ukrajinski-kibervijska-zajavili-shcho-poklali-187-sajtiv-teroristichnih-organizat sij-203364.html (дата звернення: 13.07.2025).

231. Українські кібервійська. Офіційний сайт. URL: https://armyinform.com.ua/ tag/kibervijska-ukrayiny/ (дата звернення: 13.07.2025).

232. Українські медіа поширили фейк про продавчиню, яка проколювала презервативи для покращення генофонду. URL: https://ms.detector.media/ethics/standards/ukrainski_media_poshsrili_feyk_pro_prodavchinyu_v_rosii_yaka_prokolyuvala_prezervativi_dlya_pokraschennya_genefondu/ (дата звернення: 24.07.2025).

233. Фурашев В. М. Інформаційна безпека: індикатори. *Інформація і право.* 2013. № 1 (17). С. 143–150.

234. Харамурза Д. Інформаційний тероризм як інструмент гібридної війни та фактор руйнації медіапростору. *Інтегровані комунікації*. 2023. № 2 (16). С. 29−37. DOI: 10.28925/2524-2644.2023.163.

235. Хенді Н. Соціальні медіа – новий ключовий інструмент продажу книг. *Журнал «Поети та письменники»*. 2011. № 3. С. 71–75.

236. Хорошко В. О. Основи інформаційної безпеки. Київ: ДУІКТ, 2008. 186 с.

237. Центр дослідження армії, конверсії та роззброєння. Аналітичні матеріали щодо загроз гібридного тероризму. 2022. URL: https://cacds.org.ua (дата звернення: 14.06.2025).

238. Центр стратегічних комунікацій. Офіційний сайт. URL: https://spravdi. gov.ua/ (дата звернення: 17.07.2025).

239. Черній А. Л. Детермінуюча роль кризових явищ. *Дослідження світової політики*: зб. наук. праць. Київ. 2003. Вип. № 22. С. 196−205.

240. Чупіс А. Д. Вепонізація інформації як технологія російсько-української війни. «*ПОЛІТИКУС*: наук. журн. 2024. Вип. 2. С. 181−187.

241. Шаблінський І. Розуміння сили. *Політичний менеджмент*. 2003. № 1. С. 126.

242. Шварц Д., Сулима Р. Bitkom: У Німеччині зростає кількість кібератак з РФ і Китаю. URL: https://www.dw.com/uk/bitkom-u-nimeccini-zrostae-kilkist-kiberatak-z-rosii-ta-kitau/a-69068691 (дата звернення: 13.05.2024).

243. Шевчук О. М. Інформаційний тероризм як загроза національній безпеці України під час воєнного стану. DOI: 10.36059/978-966-397-287-9-83.

244. Шкода В. Україна – не Росія. Але Росія – не Америка. *День*. 2003. 1 лист. С. 5.

245. Шматковська Т., Дзямулич М., Стащук О. Особливості моделювання бізнес-процесів в умовах формування цифрової економіки. URL: https://economyandsociety.in.ua/index.php/journal/article/view/375 (дата звернення: 21.08.2025).

246. Шуляк А. М. Медіатехнології під час моделювання образу «іншого» в ідеології «руского міра». *Науковий вісник Східноєвропейського національного університету імені Лесі Українки*. 2020. № 2 (406). Луцьк: Вежа-Друк. С. 110.

247. Шуляк Н., Шуляк А. Інформаційна гігієна в еру цифрових загроз: від пропаганди до гібридних атак. *Вісник Маріупольського державного університету. Серія: Історія. Політологія*. 2024. № 40. С.185−195.

248. Шуляк Н., Шуляк А. Стратегічні комунікації та інформаційна гігієна: національна безпека в умовах глобальних викликів: монографія. Луцьк: Вежа-Друк, 2025. 250 с.

249. Що таке інформаційна війна. URL: my.elvisti.com/sergandr/iv.html (дата звернення: 12.07.2025).

250. Що таке Львівський медіафорум. URL: https://lvivmediaforum.com/about-us (дата звернення: 25.08.2025).

251. Як «Лабораторія цифрової безпеки» запустила сайт з порадами. URL: https://www.prostir.ua/?news=yak-laboratoriya-tsyfrovoji-bezpeky-zapustyla-vlasnyj-sajt (дата звернення: 25.08.2025).

252. Як забруднити інформаційний простір і мізки друзів в соцмережах. URL: https://maidan.org.ua/2019/09/yak-zabrudnyty-informatsiynyy-prostir-i-mizky-druziv-v-sotsmerezhakh-posibnyk/ (дата звернення: 25.08.2025).

253. Як упізнати тролів або рік маніпуляцій. Підсумки огляду телетижневиків 2019 року. URL: https://detector.media/teletizhneviki/article/173617/2019-12-30-manipulyatsii-roku-abo-rik-manipulyatsii-pidsumki-oglyadu-teletizhnevikiv-2019-roku/ (дата звернення: 25.08.2025).

254. Як упізнати тролів та знайти їх мережу. URL: https://netfreedom.org.ua/article/yak-upiznati-troliv-ta-znajti-yih-merezhu (дата звернення: 25.08.2025).

255. Яцик Т. П. Особливості інформаційного тероризму як одного із способів інформаційної війни. *Науковий вісник Національного університету державної податкової служби України (економіка, право)*. 2014. № 2. С. 55– 60.

256. (Why) Is Misinformation a Problem? URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC10623619/ (дата звернення: 15.06.2025).

257. «A Terrible Idea»: Experts Blast Trump’s Plan to Label Mexican Drug Cartels «Terrorists». URL: https://www.vox.com/2019/11/27/20985392/trump-mexico-drug-cartel-oreilly-terrorist (дата звернення: 11.05.2025).

258. 20 Media Ownership and Concentration in Brazil. URL: https://academic.oup.com/book/27756/chapter-abstract/197972498 (дата звернення: 05.05.2025).

259. 8 a Cada 10 Executivos já Enfrentaram Fraudes Cibernéticas. URL: https://itforum365.com.br/8-cada-10-executivos-ja-enfrentaram-fraudes-ciberneticas/ (дата звернення: 10.06.2025).

260. A Strategic Compass for Security and Defence For a European Union that Protects its Citizens, Values and Interests and Contributes to International Peace and Security. 2022. URL: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf (дата звернення: 07.06.2025).

261. About NorCERT, the Norwegian National Cyber Security Centre. URL: https://nsm.stat.no/norcert/norcert-eng/ (дата звернення: 02.05.2025).

262. Act on the Protection of Personal Information (Act No. 57 of 2003). URL: https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en (дата звернення: 12.08.2025).

263. Act on the Protection of Personal Information. URL: https://www.ppc.go.jp/en/legal/ (дата звернення: 12.08.2025).

264. Advancing School Mental Health Conference.The Masks of Manipulation. URL: https://www.schoolmentalhealth.org/media/som/microsites/ncsmh/documents/archives/CS-1.12_The-Masks-of-Manipulation.pdf (дата звернення: 11.05.2025).

265. Advantages of the Connective Strategic Narrative During the Russian–Ukrainian War. URL: https://www.frontiersin.org/journals/political-science/articles/10.3389/fpos.2025.1434240/full (дата звернення: 05.08.2025).

266. Africa Cyberthreat Landscape Repor. URL: https://content.kaspersky-labs.com/se/media/en/africa-cyberthreat-landscape-report-2025.pdf (дата звернення: 11.08.2025).

267. Africa top target for cyber attacks – Check Point report. URL: https://www.itweb.co.za/article/africa-top-target-for-cyber-attacks-check-point-report/mYZRXM9gkWNvOgA8 (дата звернення: 13.07.202).

268. American Foreign Policy Since World War. Washington: CQ Press, 2000. P. 429.

269. Amos C. Fox On Proxy War: A Multipurpose Tool for a Multipolar World. URL: file:///C:/Users/user/Downloads/On_proxy_war_A_multipurpose_tool_for_a_multipolar_world.pdf (дата звернення: 15.06.2025).

270. An Information Policy Handbook for Southern Africa / ed. T. James. Canada: International Development Research Centre, 2001. 245 p.

271. Andrejevic M. iSpy: Surveillance and Power in the Interactive Era. Lawrence, KS: University Press of Kansas, 2007. P. 325.

272. Andress J. The Basics of Information Security. URL: http://www.sciencedirect.com/science/article/pii/B9781597496537000013. (дата звернення: 18.08.2025).

273. Arafat and the Uses of Terror. *Commentary.* 1997. Vol. 103. № 5. P. 32.

274. Archetti C. Understanding Terrorism in the Age of Global Media A Communication Approach. URL: https://link.springer.com/book/10.1057/9781137291387 (дата звернення: 12.07.2025).

275. Atran S. Psychology of Transnational Terrorism and Extreme Political Conflict. *Annual Review of Psychology*. 2021. Vol. 72. P. 471–501. DOI: 10.1146/annurev-psych-010419-050800 (дата звернення: 18.07.2025).

276. Bairak S., Buslenko V., Vozniuk Ye. State policy in the field of information security providing in Ukraine. *Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate.* 2024. 14(1). P. 107–117. DOI: 10.24917/26578549.14.1.6. URL: https://studiadesecuritate.uken.krakow.pl/wp-content/uploads/sites/43/2025/04/6.-Serhii-Bairak.pdf (дата звернення: 23.08.2025).

277. Banking Phishing: The Case of Brazil. URL: https://hstalks.com/article/2199/banking-phishing-the-case-of-brazil/ (дата звернення: 12.05.2025).

278. Beijing's Global Media Influence. 2022. URL: https://freedomhouse.org/report/beijing-global-media-influence/2022/authoritarian-expansion-power-democratic-resilience (дата звернення: 07.06.2025).

279. Bellacqua Ja. Black and White and Red All Over: China's Improving Foreign-Directed Media. URL: https://www.cna.org/reports/2020/08/DRM-2020-U-027331-1Rev.pdf (дата звернення: 11.05.202).

280. Biliusov Ye., Chyzhov D., Osaulenko A. (et al.). International Institution in the Mechanism for the Protection of Human Rights and Freedoms in the National Security Context. *Revista Cuestiones Políticas.* 2022. Vol. 40. N. 73. Julio–Diciembre. P. 108–127. DOI: 10.46398/cuestpol.4073.05.

281. Britannica. Propaganda. URL: https://www.britannica.com /topic/propaganda (дата звернення: 05.08.2025).

282. Britannica. Terrorism. URL: https://www.britannica.com/topic/terrorism#ref217761 (дата звернення: 07.08.2025).

283. CAT-UA. Official website. URL: https://cat-ua.org/ (дата звернення: 03.08.2025).

284. Cederberg A., Eronen P. How can Societies Be Defended against Hybrid Threats? *Strategic Security Analysis. Sept*. 2015. No 9. URL: http://www.defenddemocracy.org/content/uploads/documents/GCSP_Strategic_Security_Analysis_How_can_Societies_be_Defended_against_Hybrid_Threats.pdf/ (дата звернення: 04.05.2025).

285. CERT-UA. Official website. URL: https://cert.gov.ua (дата звернення: 07.08.2025).

286. Chaliand G., Blin A. The History of Terrorism: From Antiquity to al Qaeda. 2007. 484 p. URL: http://www.orgsites.com/va/asis151/HistoryofTerrorism-FromAntiquitytoalQaeda (Ucla2007).pdf (дата звернення: 11.05.2025).

287. Chambet P. Le cyber-terrorisme. URL: http://www.chambet.com/publications/Cyberterrorisme.pdf (дата звернення: 11.02.2018).

288. Check Point Software Technologies. URL: https://www.checkpoint.com/ (дата звернення: 05.05.2025).

289. China Data Protection and Cybersecurity: Annual Review of 2024 and Outlook for 2025 (I). URL: https://www.twobirds.com/en/insights/2025/china/chin

a-data-protection-and-cybersecurity-annual-review-of-2024-and-outlook-for-2025-%28i%29 (дата звернення: 08.08.2025).

290. China Finalizes Generative AI Regulation. URL: https://www.hoganlovells.com/en/publications/china-finalizes-generative-ai-regulation (дата звернення: 03.05.2025).

291. China is Targeting U.S. Voters and Taiwan With AI-Powered Disinformation. URL: https://www.wsj.com/politics/national-security/china-is-targeting-u-s-voters-and-taiwan-with-ai-powered-disinformation-34f59e21 (дата звернення: 03.05.2025).

292. China. *Key Developments*, June 1. 2023 – May 31. 2024. URL: https://freedomhouse.org/country/china/freedom-net/2024 (дата звернення: 02.06.2025).

293. China: How Mass Surveillance Works in Xinjiang. URL: https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass (дата звернення: 29.05.2019).

294. China's Cybersecurity Law Amendments: Key Changes in the Second Draft. URL: https://www.china-briefing.com/news/china-cybersecurity-law-amendments-2025/ (дата звернення: 08.08.2025).

295. China's Digital Silk Road. URL: https://www.csis.org/analysis/chinas-digital-silk-road (дата звернення: 08.08.2025).

296. China's Great Cannon. URL: https://citizenlab.ca/2015/04/chinas-great-cannon (дата звернення: 09.08.2025).

297. China's Legal Framework and Measures for Counterterrorism. URL: https://newyork.china-consulate.gov.cn/eng/xw/202401/t20240124_11231838.htm (дата звернення: 08.08.2025).

298. China's Revised and More Stringent State Secrets Law Takes Effect. URL: https://www.reuters.com/legal/legalindustry/chinas-revised-more-stringent-state-secrets-law-takes-effect-2024-05-07 (дата звернення: 07.08.2025).

299. China's cabinet passes draft regulations on data security management. URL: https://www.reuters.com/world/china/chinas-cabinet-passes-draft-regulations-data-security-management-2024-08-30/?utm_source=chatgpt.com (дата звернення: 07.08.2025).

300. Chinese People's Association for Friendship with Foreign Countries, the P.R.C. URL: http://en.cpaffc.org.cn/ (дата звернення: 08.06.2025).

301. Cingranelli D., Mark S., Gibney M. [et al.]. Human Rights Violations and Violent Internal Conflict. *Social Sciences*. 2019. Vol. 8(2). P. 41. DOI: 10.3390/socsci8020041 (дата звернення: 06.08.2025).

302. Cisco «2014 Midyear Security Report». URL: https://www.cisco.com/c/dam/m/en_emear/internet-of-everything-ioe/iac/assets/ pdfs/security/securityreport_cisco_v4.pdf (дата звернення: 01.08.2025).

303. Civil Georgia. URL: https://civil.ge/ru/archives/273751 (дата звернення: 03.06.2025).

304. Commitment to a Free, Fair and Secure Cyberspace. URL: https://www.nisc.go.jp/eng/index.html (дата звернення: 01.08.2025).

305. Communication Analysis Team – Ukraine. URL: https://cat-ua.org/en/homepage/ (дата звернення: 24.05.2025).

306. Communication from the Commission on Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. *COM*. 2009. P. 149. URL: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm. (дата звернення: 11.08.2025).

307. Conte A. The cost of terror. *New Zeland law j*. Wellington. 2001. № 11. P. 412.

308. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Amendment to Convention ETS No. 108 allowing the European Communities to accede. Strasbourg.

URL: http://www.convention.coe.int/treaty/en/Treaties/Html/108.htm (дата звернення: 28.01.2018).

309. Cotta A. L'age du terrorisme. *Commentaire*. Paris, 2000–2001. Vol. 23. № 92. P. 819–822.

310. Countering Hybrid Threats: EU-NATO Cooperation. March. 2017. URL: http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf. (дата звернення: 24.05.2025).

311. Counter-Terrorism Law (as amended in 2018). URL: https://www.chinalawtranslate.com/en/counter-terrorism-law-2015 (дата звернення: 28.07.2025).

312. CSO. United States. URL: https://www.csoonline.com/article/3387981/stakes-of-security-especially-high-in-pharmaceutical-industry.html (дата звернення: 23.05.2025).

313. Cyber Intelligence Sharing and Protection Act. URL: https://www.congress.gov/bill/112th-congress/house-bill/3523 (дата звернення: 17.07.2025).

314. Cyber Security Strategy. Japan. 2013. URL: https://www.nisc.go.jp/eng/pdf/CyberSecurityStrategy.pdf (дата звернення: 01.07.2025).

315. Cyber Space Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure. URL: https://epic.org/wp-content/uploads/privacy/cybersecurity/Cyberspace_Policy_Review_final.pdf (дата звернення: 25.05.2025).

316. Cyber Swachhta Kendra. URL: https://www.csk.gov.in/ (дата звернення: 04.05.2025).

317. Cyberattack. *Collins English Dictionary*. 2017. URL: https://goo.gl/iE7gea (дата звернення: 11.12.2017).

318. Cyberattacks on Egypt's infrastructure in 2024. URL: https://global.ptsecurity.com/en/research/analytics/cyberattacks-on-egypt-s-infrastructure-in-2024 (дата звернення: 25.05.2025).

319. Cybersecurity Laws and Regulations India 2025. URL: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india (дата звернення: 28.08.2025).

320. Cybersecurity in Mexico. URL: https://www.lexology.com/library/detail.aspx?g=927a9204-7b94-419c-8a47-57e3ffceddf5 (дата звернення: 08.08.2025).

321. Cyberspace and Information Operations Study Center, Air University, U.S. Air Force. URL: http://www.au.af.mil/info-ops/ (дата звернення: 27.08.2025).

322. Data Protection Laws in China. URL: https://www.dlapiperdataprotection.com/index.html?c=CN (дата звернення: 17.05.2025).

323. Data Protection Laws in India. URL: https://www.dlapiperdataprotection.com/?t=law&c=IN (дата звернення: 16.06.2025).

324. Data Protection Officer. URL: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/data-protection-officer_en#:~:text=The%20Data%20Protection%20Officer%20(DPO,the%20Commission%20involving%20personal%20data (дата звернення: 14.08.2025).

325. Data Security Council of India. URL: https://www.dsci.in/content/about-us#about_section (дата звернення: 16.16.2025).

326. Deterrence and Influence in Counterterrorism: a Component in the War on Al Kajeda. (Qaeda). 2002. URL: https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1619.pdf (дата звернення: 16.08.2025).

327. Deutsch K. The Nerves of Government. *Free Press.* 1964. 316 p.

328. DeWitt M. R. Understanding the Origins of Terrorism. *The Web Approach to Terrorism: Connecting the Dots.* San Francisco, 2004. August 14th–16th. URL: www.peacefromharmony.org/?cat=en_c&key=15 (дата звернення: 06.06.2025).

329. Digital Agency. URL: https://www.digital.go.jp/en/policies/security (дата звернення: 27.05.2025).

330. Digital Literacy in 2015: America's Complicated Relationship with the Internet. URL: http://www.rasmussen.edu/resources/digital-literacy-in-america (дата звернення: 27.05.2025).

331. Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. EUR-Lex. 2017. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32017L0541&from=EN (дата звернення: 13.06.2025).

332. Disambiguating Disinformation: Extending Beyond the Veracity of Online Content. URL: https://arxiv.org/abs/2206.12915 (дата звернення: 02.08.2025).

333. Disrupting Malicious Uses of our Models: an update. February 2025. URL: https://cdn.openai.com/threat-intelligence-reports/disrupting-malicious-uses-of-our-models-february-2025-update.pdf (дата звернення: 07.05.2025).

334. Drive: Resisting Radicalization Through Inclusionю Universiteit Leiden, The Netherland. 2021. URL: https://www.driveproject.eu/ (дата звернення: 06.07.2025).

335. DSCI Excellence Awards 2025. URL: https://www.dsci.in/content/dsci-excellence-awards-2025 (дата звернення: 26.08.2025).

336. DSCI Promoting Data Protection. URL: https://www.dsci.in/ (дата звернення: 03.06.2025).

337. Dubov D. V. Cyberspace as a New Dimension of Geopolitical Rivalry: a monograph. Kyiv: NISD, 2014. 328 p.

338. Dubov D. V., Ozhevan M. A. Cyber Security: Global Trends and Challenges for Ukraine: analytical Report. Kyiv, Ukraine: NISD, 2011. 31 p.

339. Ellul J. Propaganda: The Formation of Men's Attitudes. Vintage, 1965. 320 p.

340. Estratégia Nacional de Segurança Cibernética. URL: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm (дата звернення: 18.06.2025).

341. EU Action Plan on Human Rights and Democracy 2020–2024. *Council of the European Union.* Brussels. 18 November 2020. URL: https://www.consilium.europa.eu/media/46838/st12848-en20.pdf (дата звернення: 03.05.2025).

342. EU Counter-Terrorism Strategy, 2005. *Council of the European Union.* 2005. URL: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014469%202005%20REV%204 (дата звернення: 07.06.2025).

343. EU Cybersecurity Dashboard. URL: http://cybersecurity.bsa.org/countries.html (дата звернення: 24.08.2025).

344. EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002F0475 (дата звернення: 04.06.2025).

345. European Agenda on Security, 2015. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Home Affairs.* 2015. URL: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/elibrary/documents/basic-documents/docs/eu_agenda_on_security_en.pdf (дата звернення: 04.05.2025).

346. European Centre of Excellence. URL: https://www.hybridcoe.fi/about-us (дата звернення: 08.08.2025).

347. European Convention on the Suppression of Terrorism. URL: https://rm.coe.int/16800771b2 (дата звернення: 10.08.2025).

348. European Data Protection Supervisor. URL: https://edps.europa.eu/_en (дата звернення: 08.08.2025).

349. Executive Order 14028 – Improving the Nation’s Cybersecurity. May 12. 2021. URL: https://www.govinfo.gov/content/pkg/DCPD-202100401/pdf/DCPD-202100401.pdf (дата звернення: 06.06.2025).

350. Executive Order on Improving the Nation's Cybersecurity. URL: https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity (дата звернення: 24.05.2025).

351. Fake News. Misinformation & Disinformation. URL: https://guides.temple.edu/fakenews (дата звернення: 01.08.2025).

352. Farinelli Francesco. EU action on radicalization needs to be targeted at grassroots level. *The Parliament Magazine.* March 19. 2019. URL: https://www.theparliamentmagazine.eu/articles/partner_article/european-foundation-democracy/euaction-radicalisation-needs-be-targeted (дата звернення: 25.05.2025).

353. FBI. Terrorism. URL: https://www.fbi.gov/investigate/terrorism (дата звернення: 11.08.2025).

354. Fedoniuk S., Karpchuk N. Dynamics of the EU Strategic Communications Regarding the European Integration of Ukraine. No. 45. 2024. *Online Journal Modelling the New Europe*. URL: https://www.researchgate.net/profile/Nataliia-Karpchuk/publication/384922411_DYNAMICS_OF_THE_EU_STRATEGIC_COMMUNICATIONS_REGARDING_THE_EUROPEAN_INTEGRATION_OF_UKRAINE/links/67174441035917754c1467e5/DYNAMICS-OF-THE-EU-STRATEGIC-COMMUNICATIONS-REGARDING-THE-EUROPEAN-INTEGRATION-OF-UKRAINE.pdf (дата звернення: 16.06.2025).

355. Fighting Disinformation in Central Europe: StopFake's Best Practices. URL: https://www.stopfake.org/en/fighting-disinformation-in-central-europe-stopfake-s-best-practices/ (дата звернення: 15.08.2025).

356. Financial Times «Nations are Chasing the Illusion of Sovereignty». 6 July 2013. URL: http://www.ft.com/intl/cms/s/0/d1dcdb6a-cddb-11e2-a13e00144feab7de.html#axzz2WqqIiyJz (дата звернення: 26.05.2025).

357. FindLaw. URL: https://codes.findlaw.com/us/title-18-crimes-and-criminal-procedure/18-usc-sect-2331/ (дата звернення: 27.05.2025).

358. *Foreign Affairs*. 1966. Sept.-Oct. P. 24.

359. *Foreign Affairs*. 1974. № 1. P. 14.

360. Foreign Information Manipulation Interference (FIMI) and Cybersecurity – Threat Landscape. *ENISA.* URL: https://www.enisa.europa.eu/publications/foreign-information-manipulationinterference-fimi-and-cybersecurity-threat-landscape (дата звернення: 13.08.2025).

361. Foreign Policy and Domestic Scandal. *American Foreing Policy* 00/01. 2000.

362. Frameworks, Modeling and Simulations of Misinformation and Disinformation: A Systematic Literature Review. URL: https://arxiv.org/abs/2406.09343 (дата звернення: 11.07.2025).

363. Freedom House – Freedom in the World Report 2023. URL: https://freedomhouse.org/sites/default/files/2023-03/FIW_World_2023_Digtal-PDF.pdf (дата звернення: 11.07.2025).

364. Gady F. Africa's Cyber WMD *Foreign Policy*. 24.03.2010. URL: https://goo.gl/6Q7sEN (дата звернення: 11.12.2017).

365. Garfinkle A. Liening on Saddam. *The Washington Quarterly*. *Summer*. 1998. Vol. 21. № 3. P. 15–18. URL: https://www.tandfonline.com/doi/abs/10.1080/01636609809550326 (дата звернення: 11.07.2025).

366. Gartner. Official website. URL: https://www.gartner.com/en/about (дата звернення: 14.07.2025).

367. Gertz B. IWar: War and Peace in the Information Age. The Institute of World Politics. Simon & Schuster, Reprint edition. Washington, 2017. URL: https://www.opendemocracy.net/article/iwar_pirates_states_and_the_internet (дата звернення: 11.08.2025).

368. Giles C., Allen K. Financial Times «Southeastern Shift: The New Leaders of Global Economic Growth». June 4. 2013. URL: https://www.ft.com/content/b0bd38b0-ccfc-11e2-9efe-00144feab7de (дата звернення: 27.05.2025).

369. Global Cybersecurity Index (GCI). 2017. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017.pdf (дата звернення: 07.08.2025).

370. Global Civil Society. Oxford, 2001. 348 p.

371. Grobler M., Vuuren van J. Collaboration as Proactive Measure against Cyber Warfare in South Africa. *African Security Review*. 2012. Vol. 21 (2). P. 61– 73.

372. Hacsek Z. Global Jihadist Terrorism. Terrorist Groups, Zones of Armed Conflict and National Counter-Terrorism Strategies. *Behavioral Sciences of Terrorism and Political Aggression.* 2022. Vol. 1–4. P. 338. DOI: 10.1080/19434472.2022.2098361.

373. Han R. Manufacturing Consent in Cyberspace: China's «Fifty-Cent Army». *Journal of Current Chinese Affairs*. 2015. № 44 (2). P. 105–134. DOI: 10.1177/186810261504400205.

374. Handbook of Terrorism Prevention and Preparedness. URL: https://icct.nl/handbook-terrorism-prevention-and-preparedness (дата звернення: 13.08.2025).

375. Hauner M. What is Asia to Us?: Russian's Asian Heartland Yesterday & Today. London; New York: Routlenge, 1992. P. 75–115.

376. High-Level Commission Expert Group on Radicalisation (HLCEG-R) Final Report. Home Affairs. 2018. URL: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-wedo/policies/european-agenda-security/20180613_final-report-radicalisation.pdf (дата звернення: 27.06.2025).

377. Hirschmann K. Terrorismus in Neuen Dimensionen Hintergruede und Schlussfolgerungen. *Aus Politik u. Zeitgeschichte*. Bonn, 2001. № 51. P. 7–15.

378. Hirschmann K. The Changing Face of Terrorism. *Intern. Politik u. Ges*. Bonn, 2000. № 3. P. 299.

379. Hoffman B. Inside Terrorism. Columbia University Press, 2006. P. 528.

380. How can you spot fake news? *BBC*. URL: https://www.youtube.com/watch?v=qet-0mfK5b0 (дата звернення: 17.08.2025).

381. How Japan Is Modernizing Its Cybersecurity Policy. URL: https://www.stimson.org/2023/japan-cybersecurity-policy/ (дата звернення: 24.08.2025).

382. How the Sinaloa Cartel Bested the Mexican Army. URL: https://time.com/5705358/sinaloa-cartel-mexico-culiacan/ (дата звернення: 18.07.2025).

383. How to Recognize a Fake News Story. 9 helpful tips to stop yourself from sharing false information. URL: https://www.huffpost.com/entry/fake-news-guide-facebook_n_5831c6aae4b058ce7aaba169 (дата звернення: 16.06.2025).

384. Hrynchuk V., Vozniuk E. Information Security of India. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2018. № 1 (374). P. 15–20.

385. Human Trafficking into and within the United States: a Review of the Literature. URL: https://aspe.hhs.gov/system/files/pdf/75891/index.pdf (дата звернення: 11.05.2025).

386. Hybrid War – A New Security Challenge for Europe. URL: http://www.parleu2015.lv/files/cfsp-csdp/wg3-hybrid-war-background-notes-en.pdf (дата звернення: 18.08.2025).

387. Hybrid war – does it even exist? URL: https://www.nato.int/docu/review/2015/also-in-2015/hybrid-modern-future-warfare-russia-ukraine/en/index.htm (дата звернення: 17.08.2025).

388. Hybrid Warfare and Challenges. URL: https://smallwarsjournal.com/documents/jfqhoffman.pdf. (дата звернення: 20.08.2025).

389. Hych I., Vozniuk E. The Threats and Opportunities of Crisis on Ukraine’s Accession to the EU. *Науковий вісник Східноєвропейського*

національного університету імені Лесі Українки. Серія: Міжнародні відносини. 2017. № 6 (355). P. 12–16.

390. IFSEC India. URL: https://www.ifsec.events/india/ (дата звернення: 14.08.2025).

391. IMARC Group. URL: https://www.imarcgroup.com/ (дата звернення: 14.08.2025).

392. India Cyber Security Market Size & Outlook. 2024–2030. URL: https://www.grandviewresearch.com/horizon/outlook/cyber-security-market/india (дата звернення: 13.08.2025).

393. India's Cybercrime Problems Grow as Nation Digitizes. URL: https://www.darkreading.com/cyber-risk/indias-cybercrime-problems-nation-digitizes (дата звернення: 13.08.2025).

394. Indian Cybercrime Coordination Centre (I4C). URL: https://i4c.mha.gov.in (дата звернення: 13.08.2025).

395. Indian Government Releases National Cyber Security Policy. 2013. URL: https://www.huntonprivacyblog.com/2013/07/03/indian-government-releases-national-cyber-security-policy-2013/ (дата звернення: 15.08.2025).

396. Information Safety of Ukraine: Integral Assessment and Taxonomic Analysis. URL: https://www.growingscience.com/ijds/Vol5/ijdns_2021_11.pdf (дата звернення: 25.08.2025).

397. Information Security Policies in Japan. Towards a Safe and Secure Network Infrastructure. URL: http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/070522_1.pdf (дата звернення: 14.08.2025).

398. Information Securitys Pendingin Indiatogrow 12 % to $1,5 billion: Gartner. URL: https://economictimes indiatimes.com/tech/software/information-security-spending-in-india-to-grow-12-to-1-5-billiongartner/articleshow/60278990.cms (дата звернення: 14.06.2025).

399. InformNapalm. Official website. URL: https://informnapalm.org/ua/ (дата звернення: 24.08.2025).

400. International Convention for the Suppression of the Financing of Terrorism. URL: https://treaties.un.org/doc/db/Terrorism/english-18-11.pdf (дата звернення: 01.08.2025).

401. International Security. URL: https://www.eolss.net/sample-chapters/c14/E1-35-04-02.pdf (дата звернення: 15.08.2025).

402. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (дата звернення: 11.08.2025).

403. International Terrorism: The Other World War. *International Terrorism. Characteristics, Causes, Controls*. University of South Carolina, 1990. 280 p.

404. Internet Organised Crime Threat Assessment. *European Cyber crime Centre*. 2018. URL: https://www.europol.europa.eu/sites/default/files-/documents/iocta2018.pdf (дата звернення: 13.07.2025).

405. Interpol Africa Cyberthreat Assessment Report. 2025. URL: file:///C:/Users/user/Downloads/25COM009248%20-%20Cybercrime_Africa%20Cyberthreat%20Assessment%20Report_Design_2025-05%20v11.pdf (дата звернення: 16.08.2025).

406. Japan and Information Security. URL: http://www.sciencedirect.com/science/article/pii/S0960259305800576?via%3Dihub (дата звернення: 11.07.2025).

407. Japan Cyber Threat Landscape. 2024. URL: https://gftn.co/insights/japan-cyber-threat-landscape (дата звернення: 12.07.2025).

408. Japan Cybersecurity. URL: https://www.trade.gov/market-intelligence/japan-cybersecurity (дата звернення: 08.08.2025).

409. Japan: A Cybersecurity Market in Full Swing. URL: https://incyber.org/en/article/japan-a-cybersecurity-market-in-full-swing/ (дата звернення: 08.08.2025).

410. Japan’s Cybersecurity Strategy. 2021. URL: https://dig.watch/resource/japans-cybersecurity-strategy-2021 (дата звернення: 08.08.2025).

411. Japan’s Information Security Initiatives. OECD: Better Policies for Better Lives. URL: http://www.oecd.org/japan/japansinformationsecurityinitiatives.htm (дата звернення: 07.08.2025).

412. Japan’s New Active Cyber Defense Law: A Strategic Evolution in National Cybersecurity. URL: https://www.centerforcybersecuritypolicy.org/insights-and-research/japans-new-active-cyber-defense-law-a-strategic-evolution-in-national-cybersecurity (дата звернення: 06.08.2025).

413. Jenkins B. International Terrorism: The Other World War. *International Terrorism. Characteristics, Causes, Controls*. University of South Carolina, 1990. P. 27.

414. Jenkins B. The Study of Terrorism: Definitional Problems. RAND, 1980. 10 p. URL: https://www.rand.org/content/dam/rand/pubs/papers/2006-/P6563.pdf (дата звернення: 11.06.2025).

415. Jerrold M. From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism. NATO Library at: *Terrorism_and_political_violence*. Vol. 12. № 2. Summer 2000. P. 97–122.

416. Joint Managing Mis/Disinformation Working Group. URL: https://www.cisa.gov/resources-tools/groups/joint-managing-misdisinformation-working-group (дата звернення: 13.05.2025).

417. Jonasson S. Understanding the Processes of Asymmetric Warfare. The Plight of the Strong: Actors, Dynamics and Strategy. URL: https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=1316742&fileOId=1316743 (дата звернення: 16.06.2025).

418. Jowett G. S., O’Donnell V. Propaganda & Persuasion Sixth Edition 2015. URL: https://csmeyns.github.io/propaganda-everyday/pdf/odonnell-jowett-2018-what-is-propaganda.pdf (дата звернення: 06.07.2025).

419. Kachkovska L., Blahovirna N., Vozniuk Ye. [et. al]. Documentary-information communication in public administration: legal aspects and digital

transformation. *International Journal of Basic and Applied Sciences*. 2025. 14 (3). P. 42–47. DOI: 10.14419/v1jmq034. URL: www.sciencepubco.com/index.php/IJBAS (дата звернення: 23.08.2025).

420. Khoma N., Vozniuk Ye. Evolution from the Concept «Zero Problems with Neighbors» to the Practice «Zero Neighbors Without Problems»: The Role of Neo-Ottomanism. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2020. № 2 (8). P. 46–56.

421. Khoma N., Vozniuk Ye. Turkey's Middle East Policy: Vectors, Aims and Results Studia Politica. *Romanian Political Science Review*. 2021. Vol. XXI. № 2. P. 577−601. URL: https://tinyurl.com/25zu7k7r. (дата звернення: 23.08.2025).

422. Kigen P. M., Muchai C., Kimani K. and others. Kenya Cyber Security Report. *Serianu*. 2015. URL: https://goo.gl/DHX4Yv (дата звернення: 11.12.2017).

423. Kiyuna A., Conyers L. Cyberwarfare Sourcebook. Lulu.com, 2015. P. 312.

424. Kormych L., Zavhorodnia Y. The Concept of Modern Political Confrontation in Cyber Space. *Cybersecurity*. Oxford, 2023. P. 1–7.

425. Kotsan N., Kopachinska G., Vozniuk Ye., Kotsan R. Basic models of protection and functioning of the Ukrainian border in modern geopolitical realities: a view from Ukraine. *European Spatial Research and Policy*. 2022. Vol. 29. № 1. P. 79–95. DOI: 10.18778/1231-1952.29.1.04. URL: https://czasopisma.uni.lodz.pl/esrap/article/view/9908 (дата звернення: 23.08.2025).

426. Kotsan R., Kotsan N., Kopachinska G., Vozniuk Ye. Transformations of Ukrainian-Polish Border Regions Transformation: Experience of Ukraine. *Forum Geographic*. 2022. Vol. 21. Issue 1. P. 92−101. DOI: 10.5775/fg.2022.071.i. URL: http://forumgeografic.ro/wp-content/uploads/2022/1/Kopachinska.pdf. (дата звернення: 23.08.2025).

427. Kryva L., Anisimovych-Shevchuk O., Toma M., Kutsepal S. & Derevianko S. Effectiveness of International Cooperation of the Lublin Triangle Countries in Addressing Terrorist Threats. *Pakistan Journal of Criminology*. 2024. Vol. 16. № 03. July–September. P. 835–850. DOI: 10.62271/PJC.16.3.835.850.

428. Larson S. The Hacks that Left Us Exposed in 2017. URL: http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/ index.html (дата звернення: 15.05.2025).

429. Law of Ukraine «On the Fundamentals of National Security of Ukraine». URL: http://cis-legislation.com/document.fwx?rgn=17928 (дата звернення: 19.01.2018).

430. Lebid A., Vashyst K., Nazarov M. Information Resilience as a Means of Countering the Socio-Psychological Strategies of Information Wars. *International Journal of Media and Information Literacy*. № 7(1). Bratislava, 2022. P. 157–166. DOI: 10.13187/ijmil.2022.1.158.

431. Levada-Center. Official website. URL: http://www.levada.ru/en/category/publications/ (дата звернення: 22.01.2018).

432. Lin Lauren Yu-Hsin, Milhaupt Curtis J. China's Corporate Social Credit System: The Dawn of Surveillance State Capitalism? *The China Quarterly*, Vol. 256. December 2023. P. 835–853. DOI: 10.1017/S030574102300067X.

433. Lind W. S. Understanding Fourth Generation War. URL: http://www.au.af.mil/au/awc/awcgate/milreview/lind.pdf (дата звернення: 14.06.2025).

434. Lind W. S., Nightengale K., Schmitt J. F., Sutton J. W., & Wilson G. I. The Changing Face of War: Into the Fourth Generation. *Marine Corps Gazette*. 1989. P. 8.

435. Lipkan V. The Necessity of Formation of the National Security System. 2003. P. 23–24. URL: file:///C:/Users/User/Desktop/Pib_2003_2_2_7.pdf (дата звернення: 11.08.2025).

436. Mack A. Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflic. *World Politics*. 1975. Vol. 27. № 2. P. 175–200.

437. Manipulating Uncertainty: Cybersecurity Politics in Egypt. URL: https://academic.oup.com/cybersecurity/article/7/1/tyaa026/6137887 (дата звернення: 11.08.2025).

438. Manipulation. Cambridge Dictionary. *Cambridge Universit Press*. URL: https://dictionary.cambridge.org/us/dictionary/english/manipulation (дата звернення: 03.05.2025).

439. Mazur P., Wasiuta O., Wasiuta S. Państwo Islamskie ISIS: nowa twarz ekstremizmu, Difin. Warszawa, 2018. P. 267.

440. McIntosh L. D., White W., Hudson C. Vitale Unveiling Deception: Establishing a Taxonomic Framework for Disinformation within Scientific Discourse. URL: https://arxiv.org/abs/2311.11344 (дата звернення: 16.07.2025).

441. Media in Brazil: Government, Politics and Regulation. URL: https://journalismresearch.org/2024/11/media-in-brazil-government-politics-and-regulation/ (дата звернення: 16.05.2025).

442. Mediating Scandal in Contemporary Japan. URL: https://www.frenchjournalformediaresearch.com/lodel-1.0/main/docannexe/file/1145 prusa_pdf.pdf (дата звернення: 11.05.2025).

443. METI Minister of Economy, Trade and Industry. URL: https://www.meti.go.jp/english/index.html (дата звернення: 13.05.2025).

444. Mexico: National Cybersecurity Strategy and Awareness Campaign. URL: https://www.coe.int/en/web/cybercrime/-/mexico-national-cybersecurity-strategy-and-awareness-campaign (дата звернення: 06.06.2025).

445. Mexico: Organized Crime and Drug Trafficking Organizations. December 20. 2019. URL: https://fas.org/sgp/crs/row/R41576.pdf (дата звернення: 29.06.2025).

446. Mexico’s New Drug War may be Worse than Old One. URL: https://apnews.com/9231894fd9bf451e92a6ba64e3c68dc2 (дата звернення: 29.06.2025).

447. Misinformation and Disinformation. URL: https://www.apa.org/topics/journalism-facts/misinformation-disinformation (дата звернення: 11.07.2025).

448. Misinformation, Disinformation & Malinformation: A Guide. URL: https://princetonlibrary.org/guides/misinformation-disinformation-malinformation-a-guide (дата звернення: 27.07.2025).

449. Modeling and Governance of the Country's Energy Security: The Example of Ukraine. URL: https://www.econjournals.com/index.php/ijeep/article/view/13397 (дата звернення: 11.06.2025).

450. Morenchuk A., Vozniuk Ye., Morenchuk A. junior Sources of Russian Policy Aggressiveness. *Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate.* 2024. 14(1). P. 91–105. DOI: 10.24917/26578549.14.1.5. URL: https://studiadesecuritate.uken.krakow.pl/wp-content/uploads/sites/43/2025/04/5.-Andriy-Morenchuk.pdf. (дата звернення: 12.08.2025).

451. Morgenthau Hans J. Politics Among Nations: The Struggle for Power and Peace / 3rd ed. New York: Alfred A. Knopf, 1960. 387 p.

452. Morin E., Kern A.-B. Terre-Patrie. Paris: Éditions du Seuil, 1993. 222 p.

453. Mumford A. Proxy Warfare and the Future of Conflic. URL: https://www.tandfonline.com/doi/full/10.1080/03071847.2013.787733 (дата звернення: 13.05.2025).

454. National Critical Information Infrastructure Protection Centre. URL: nciipc.gov.in (дата звернення: 15.08.2025).

455. National Cyber Strategy of the United States of America. September. 2018. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата звернення: 15.08.2025).

456. National Cybersecurity Strategy March 2023. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (дата звернення: 16.07.2025).

457. National Security versus Global Security. URL: https://www.un.org/en/chronicle/article/national-security-versus-global-security (дата звернення: 16.07.2025).

458. NATO StratCom COE. *iWar: The Changing Nature of Warfare*. 2016. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/586600/EPRS_BRI%282016%29586600_EN.pdf (дата звернення: 16.07.2025).

459. NATO StratCom COE. *Звіти про вплив російських ІПСО на вибори у Східній Європі (Україна, Литва, Словаччина).* 2020–2023. URL: https://mcsc.gov.ua/wp-content/uploads/2025/01/zvit-shhodo-vykonannya-planu-zahodiv-z-realizacziyi-strategiyi-informaczijnoyi-bezpeky-za-2023-rik.pdf. (дата звернення: 16.07.2025).

460. NATO Strategic Concept (2010). *Active Engagement, Modern Defence*. URL: https://www.nato.int/cps/en/natohq/topics_82705.htm (дата звернення: 16.07.2025).

461. NATO. Official website. URL: https://www.nato.int/docu/review/2018 (дата звернення: 16.07.2025).

462. NCIIPC Explained: Safeguarding India's Critical Infrastructure. URL: https://www.upguard.com/blog/nciipc-explained (дата звернення: 17.07.2025).

463. New INTERPOL report warns of sharp rise in cybercrime in Africa. URL: https://www.interpol.int/en/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa (дата звернення: 16.06.2025).

464. Nikolayenko N. Communication Component of the Russian-Ukrainian Hybrid War / Intercultural Communication in the Context of Globalization Dialogue: development strategies. *Monographic series «European Science». Book 4.* Part 8. 2021. P. 11–20. URL: file:///C:/Users/USER/Downloads/%D0%BA%D0%BD%D0%B8%D0%B3%D0%B0-8%20(3).pdf (дата звернення: 15.07.2025).

465. Nikolayenko N. Russian Aggression as a Challenge in the Sphere of Ukraine's National Security. *Міжнародні відносини, суспільні комунікації та*

регіональні студії. 2021. № 1(9). P. 86–93. DOI: 10.29038/2524-2679-2021-01-273-283.

466. Norms for International Peace and Security: the Normative Frameworks of International Cyber Cooperation. URL: https://ict4peace.org/wp-content/uploads/2020/05/ 16496284.pdf (дата звернення: 07.06.2025).

467. Norton Cyber Security Insights Report 2017 United States Result. URL: http://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-US.pdf (дата звернення: 15.08.2025).

468. Novak O., Vozniuk Ye. The Influence of the Information Society Development on Political Ideologies. *Studia de Securitate.* 2021. 11(1). P. 19–26. DOI: 10.24917/26578549.11.1.2. URL: https://studiadesecuritate.uken.krakow.pl/wp-content/uploads/sites/43/2021/06/2_Novak_Vozniuk.pdf (дата звернення: 23.08.2025).

469. Only 7 % of Organisations in India Ready gor Cyber Threats: Cisco report. URL: https://economictimes.indiatimes.com/tech/technology/only-7-of-organisations-in-india-ready-for-cyber-threats-cisco-report/articleshow/121291935.cms (дата звернення: 16.07.2025).

470. Orakhelashvili A. Legal Aspects of Global and Regional International Security – The Institutional Background. URL: https://www.nato.int/acad/fellow/98-00/orakhelashvili.pdf (дата звернення: 14.07.2025).

471. Organisation of the Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT). URL: https://www.oic-cert.org/en/index.html (дата звернення: 13.06.2025).

472. Ozhohan A., Derevianko S., Karchevska O. [et al.]. Language as a political manipulation tool. *Amazonia Investiga*. 2023. 12(64). P. 237–248. DOI: 10.34069/AI/2023.64.04.23.

473. Parsi V. E. Nuove Guerre e Antiehe Fraturre. *Vita e pensiero*. Milano, 2001. A. 84. № 5. P. 413.

474. Parvar Hamid Ziaei. Soft War (2): *Media War, Tehran: Tehran International Studies & Research Institute (TISRI).* September 2004. 303 p.

475. Patterns of International Terrorism: 1980. *Central Intelligence Agency*. PA 81 – 10163 U. 1981. June. 120 p.

476. Petrovic S. Tracing Individual Perceptions of Media Credibility in Post-3.11 Japan. May 15. 2020. URL: https://apjjf.org/2020/10/petrovic (дата звернення: 15.07.2025).

477. Pew Research Center. *Опитування в 19 країнах Європи: 72 % респондентів вважають, що соцмережі «ослаблюють демократію».* 2022. URL: https://www.pewresearch.org/ (дата звернення: 15.07.2025).

478. Pipchenko N. Public Discourse in the European Neighbour States of Ukraine Concerning the Russian Invasion. *Actual problems of international relations*. 2023. Issue 154. P. 34–52. DOI: 10.17721/apmv.2023.154.1.34-52.

479. Pipchenko N., Darnytskyi A. Public Diplomacy of Ukraine under Martial Law. *Actual problems of International Relations.* 2024. Vol. 1. No. 160. URL: http://apir.iir.edu.ua/index.php/apmv/article/view/3914 (дата звернення: 15.08.2025).

480. Pipchenko N., Makarenko I., Ryzhkov M., Zaitseva M. The Policy of European and Euro-Atlantic Integration as a Key Factor for Ukraine's Transformation. June 2021. *European Spatial Research and Policy.* 2021. № 28(1). P. 265–285. DOI: 10.18778/1231-1952.28.1.14.

481. Pipchenko N., Yurii A. Media Literacy and Psychological Resilience: the Swedish Approach to Countering Disinformation. *Actual Problems of International Relations.* 2025. Vol. 1. № 162. DOI: 10.17721/apmv.2025.162.1.16-23.

482. Pipes D. The Event of Our Era: Former Soviet Muslim Republics Change the Middle East. *Central Asia and the World* / ed. by M. Mandelbaum. New York: Counsil of Foreign Relations Books, 1994. P. 47–90.

483. Podhoretz N. Oslo: The Peacemongers Return. *Commentary*. 2001. Vol. 112. № 3. 38 p.

484. Pötzsch H. The Emergence of iWar: Changing Practices and Perceptions of Military Engagement in a Digital Era. *New Media &Society*. 2015. Vol. 17(1). P. 78–95.

485. Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities. Brussels. 16.12.2020 COM(2020) 829 final. URL: https://ec.europa.eu/homeaffairs/sites/default/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf (дата звернення: 15.07.2025).

486. Pro-PRC DRAGONBRIDGE Influence Campaign Leverages New TTPs to Aggressively Target U.S. Interests, Including Midterm Elections. URL: https://cloud.google.com/blog/topics/threat-intelligence/prc-dragonbridge-influence-elections/ (дата звернення: 15.05.2025).

487. Provisions on the Management of Algorithmic Recommendations in Internet Information Services. URL: https://www.chinalawtranslate.com/en/algorithms (дата звернення: 13.07.2025).

488. RAND Corporation. Networked Terror: Beyond Conventional Warfare. 2004. URL: https://www.rand.org/pubs/monograph_reports/MR1382.html (дата звернення: 15.08.2025).

489. Rauta V. Framers, Founders, and R eformers: three generations of proxy war research. URL: https://centaur.reading.ac.uk/91906/3/28-Jul2020Rauta%20-%20Final.pdf (дата звернення: 13.07.2025).

490. Relatório da Segurança Digital no Brasil *DFNDR Lab*. 2018. URL: https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-2%C2%BA-trimestre-de-2018.pdf (дата звернення: 16.05.2025).

491. Relatório da Segurança Digital no Brasil Primeiro trimestre - 2018. URL: https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/05/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-Primeiro-trimestre-de-2018-1.pdf?utm_source=chatgpt.com (дата звернення: 16.05.2025).

492. Reporter ohne Grenzen. URL: www/reporter-ohne-grenzen.de (дата звернення: 23.07.2025).

493. Resolutions adopted by the Security Council in 1990. URL: https://main.un.org/securitycouncil/en/content/resolutions-adopted-security-council-1990 (дата звернення: 19.06.2025).

494. Right-wing violent extremism and terrorism in the European Union: discussion paper. *Council of the European Union*. 30 August. 2019. URL: http://www.statewatch.org/news/2019/sep/eu-councilctc-right-wing-11756-19.pdf (дата звернення: 16.07.2025).

495. Rogan H. Al-Qaeda's Online Media Strategies: From Abu Reuter to Irhabi 007. Oslo. Norwegian Defence Research Establishment (FFI). 1.12.2007. URL: https://scispace.com/pdf/from-abu-reuter-to-irhabi-007-al-qaeda-s-online-media-3jaypv9sie.pdf (дата звернення: 19.06.2025).

496. RSF urges Japan to stop pressuring the media on Fukushima-related topics. URL: https://rsf.org/en/rsf-urges-japan-stop-pressuring-media-fukushima-related-topics (дата звернення: 16.07.2025).

497. Ruiz Carlos Diaz Ruiz Disinformation on digital media platforms: A market-shaping approach. URL: https://journals.sagepub.com/doi/10.1177/14614448231207644 (дата звернення: 06.07.2025).

498. Ryan J. iWar: A new threat, its convenience and our increasing vulnerability. Analysis. *NATO Review*. Winter 2007. URL: https://www.nato.int/docu/review/2007/issue4/english/analysis2.html (дата звернення: 24.05.2025).

499. Ryan J. iWar: pirates, states and the internet. URL: https://www.opendemocracy.net/article/iwar_pirates_states_and_the_internet (дата звернення: 24.05.2025).

500. Sahu P. Where Are Weon Cybersecurity in India? URL: https://securityintelligence.com/where-are-we-oncybersecurity-in-india/ (дата звернення: 27.07.2025).

501. Saint, Knights and Crystal Meth; Mexico's Bizarre Cartel. URL: https://www.reuters.com/article/us-mexico-drugs-knights/saint-knights-and-

crystal-meth-mexicos-bizarre-cartel-idUSBRE86H0WB20120718 (дата звернення:16.06.2025).

502. Sectoral Privacy Project. URL: https://www.dsci.in/sectoral-privacy-project/ (дата звернення: 03.05.2025).

503. Sheridan S. Why Writers Must Embrace Social Media, no Matter the Genre. *The Guardian*. URL: https://www.theguardian.com/edinburgh/2011/apr/14/edinburgh-sara-sheridan-digital-rights (дата звернення: 13.05.2024).

504. Shimuleni M. S., Vozniuk E. Regional Integration and Development: a Theoretical Review of the SADC Region. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2017. № 10 (359). P. 111–116.

505. Shuliak A., Sydoruk T., Pavliuk V. Russia's war against Ukraine and the transformation of the Euro-Atlantic security architecture. *Politics in Central Europe*. 2023. Vol. 19, No. 2. P. 305-323. DOI: 10.2478/pce-2023-0014.

506. Shuliak A., Vozniuk Ye., Patlashynska I. [et. al]. The Impact of the 4.0 Technological Revolution on the Hybrid War of the russian federation in Ukraine. *AD ALTA: Journal of Interdisciplinary Research*. 2022. Special Issue (12/02-XXX.). P. 159–164. DOI: 10.33543/1202. URL: http://www.magnanimitas.cz/ADALTA/120230/papers/K_15.pdf. (дата звернення: 23.08.2025).

507. Shuliak A., Voznyuk Ye., Patlashinska I., Shuliak N. Info-analytic support for ukrainian-polish cross-border cooperation: a case study of euro-regions. *Codrul Cosminului*. 2020. Issue 2. Vol. 26. P. 431–454. DOI: 10.4316/CC.2020.02.007.

508. Soldatenko I., Chub O., Kopina O. Journalism and the Right to Information as Tools for Combating Corruption in Ukraine: Assessment of Media Access to Anti-Corruption Authorities. URL: https://ajee-journal.com/upload/attaches/att_1749914 250.pdf#page=9 (дата звернення: 15.05.2025).

509. Sovereignty in Cyberspace: Theory and Practice (Version 2.0). URL: https://www.cac.gov.cn/2020-11/25/c_1607869925296336.htm (дата звернення: 13.08.2025).

510. Stanford Encyclopedia of Philosophy. The Ethics of Manipulation. URL: https://plato.stanford.edu/entries/ethics-manipulation (дата звернення: 12.05.2025).

511. Starting at Zero: U.S. Foreign Policy for the 1990-s *Y.S. Foreign Policy After the Gold War.* Ed by Brad Roberts. *MIT Press*. 1992. 380 p.

512. Statistical Abstract India-2002. Ministry of Statistics and Programme Implementation. URL: https://mospi.gov.in/publication/statistical-abstract-india-2002 (дата звернення: 19.07.2025).

513. Stochastic Terrorism: A Linguistic and Psychological Analysis. URL: https://pt.icct.nl/sites/default/files/2023-04/Article%201_12.pdf (дата звернення: 12.08.2025).

514. Stochastic Terrorism: Critical Reflections on an Emerging Concept. URL: https://www.tandfonline.com/doi/full/10.1080/17539153.2024.2305742?scroll=top&needAccess=true#abstract (дата звернення: 12.08.2025).

515. StopFake. Official website. URL: https://www.stopfake.org/uk/golovna/ (дата звернення: 28.08.2025).

516. StratCom Ukraine. Official website. URL: https://stratcomua.org/ua (дата звернення: 28.08.2025).

517. Strategic Communications: East and South. *Report № 30. EU Institute for Security Studies*. July 2016. URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Report_30.pdf (дата звернення: 18.08.2025).

518. Sudhir M. R. Asymmetric War: A Conceptual Understanding. *Centre for Land Warfare Studies Journal. Summer*. 2008. P. 58–66.

519. Summary Cyber Strategy of the Department of Defense 2018. URL: https://dodcio.defense.gov/Portals/0/Documents/Library/CyberStrategy2018.pdf (дата звернення: 20.08.2025).

520. Summary Cyber Strategy of the Department of Defense 2023. URL: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf (дата звернення: 20.08.2025).

521. Summary. Department of Defense Cyber Strategy. URL: https://dodcio.defense.gov/Portals/0/Documents/Library/CyberStrategy2018.pdf (дата звернення: 20.08.2025).

522. The 2022 Code of Practice on Disinformation. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (дата звернення: 17.07.2025).

523. The Basic Act on Cybersecurity（Act No. 104 of 2014). URL: https://www.japaneselawtranslation.go.jp/en/laws/view/3677/en (дата звернення: 24.06.2025).

524. The benefits of Cyber Insurance. URL: https://www.loricainsurance.com/legacy/documents/Summary_-_Cyber.pdf (дата звернення: 13.06.2025).

525. The Benevolent Empire. *American Foreign Policy 00/01* / ed. by G. Hastedt. Guilford: Dushkin / Mc Graw–Hill, 2000. URL: https://www.amazon.com/American-Foreign-Policy-Glenn-Hastedt/dp/1538173751 (дата звернення: 24.06.2025).

526. The Changing Nature of «International Security»: the Need for an Integrated Definition. URL: https://www.diplomatonline.com/pdf_files/npsia/2007-08/2_Int_Security_C_ Elisabeth_St_Jean_FINAL.pdf (дата звернення: 16.05.2025).

527. The Comprehensive National Cybersecurity Initiative. URL: https://nsarchive.gwu.edu/document/21430-document-34 (дата звернення: 27.05.2025).

528. The Cyber Surakshit Bharat Initiative. URL: https://thegfce.org/initiative/the-cyber-surakshit-bharat-initiative/ (дата звернення: 13.06.2025).

529. The Danger Within: Militant Islam in America. *Commentary*. 2001. Vol. 112. № 4. URL: https://www.commentary.org/articles/daniel-pipes/the-danger-within-militant-islam-in-america/ (дата звернення: 13.08.2025).

530. The Digital Personal Data Protection Bill. 2023. URL: https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 (дата звернення: 03.08.2025).

531. The End of American Exceptionalism. *The Public Interest*. 1975. Fall. URL: https://www.scribd.com/document/100212011/Bell-End-of-American-Exceptionalism (дата звернення: 13.08.2025).

532. The End of the American Era: US Foreign. Policy and the Geopolitics of the Twenty-First Century. New York, 2002. P. 416.

533. The European Network and Information Security Agency. URL: http://www.enisa.europa.eu/ (дата звернення: 17.08.2025).

534. The Indian Cybersecurity Landscape: Rapid Progress and Increased Vulnerabilities. URL: https://practiceguides.chambers.com/practice-guides/cybersecurity-2025/india/trends-and-developments/O20301 (дата звернення: 18.08.2025).

535. The National Strategy to Secure Cyberspace February 2003. URL: https://www.nitrd.gov/documents/cybersecurity/documents/NationalStrategytoSecureCyberspace2003.pdf (дата звернення: 13.07.2025).

536. The New Silk Road – Leveraging the Belt and Road Initiative to Drive a New Era of Sustainable Trade. URL: https://www.unleashopportunity.org/wp-content/uploads/2017/02/ok-Day2-BS1-0-Intro-slides-Belt-and-Road-Panel-Introduction-Joyce-Chau-amfori-Greater-China.pdf (дата звернення:14.06.2025).

537. The New US Security Agenda: Trends and Emerging Threats. URL: https://tinyurl.com/3kzjvmpw (дата звернення: 12.08.2025).

538. The Rise of Digital Authoritarianism. URL: https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism (дата звернення: 28.07.2025).

539. The State of Cybersecurity in Mexico: An Overview. URL: https://www.wilsoncenter.org/sites/default/files/cybersecurity_in_mexico_an_overview.pdf (дата звернення: 07.08.2025).

540. The Washington Post. 2002. August 20. URL: https://www.washingtonpost.com/sitemap/2002/8/20/ (дата звернення: 07.08.2025).

541. Thevenet C. Cyber-terrorisme, Mythe ou Réalité? *Série Mémoires et Thèse.* Université de Marne-La-Vallée, 2005. P. 57.

542. Tolipov F. Are the Heartland and Rimland changing in the wake of the operation in Afghanistan – Central Asia and the Caucasus, 2003. P. 99–106.

543. Top Cybersecurity Regulations in India. URL: https://www.upguard.com/blog/cybersecurity-regulations-india (дата звернення: 12.08.2025).

544. Torres-Soriano M. R. Between the Pen and the Sword: The Global Islamic Media Front in the West. November 2012. *«Terrorism and Political Violence»*. 2012. 24(5). P. 769–786.

545. Tran-Tam. Crimes of Terrorism and International Criminal Law. *A Treatise on International Criminal Law.* 1973. Vol. 1: *Crimes and Punishment*, USA. P. 493.

546. Treasury Designates ISIS Cyber Facilitators and Trainers. URL: https://home.treasury.gov/news/press-releases/jy2056 (дата звернення: 21.08.2025).

547. Twelve against Empire: The Anti-Imperialists, 1898. 1900. New York, 1968. P. 310.

548. U.S. International Trade Administration, «Japan – Cybersecurity Market Overview». URL: https://www.trade.gov/market-intelligence/japan-cybersecurity (дата звернення: 11.08.2025).

549. United Nations Secretary-General. Kofi Annan 2001. URL: https://www.un.org/sg/en/subsite-section/kofi-annan?page=320 (дата звернення: 16.03.2018).

550. Vetrov K., Voznyuk Ye. Information Terrorism as a Modern Threat for Information Security of European States. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2019. № 1(5). P. 34–42.

551. Voelz G. J. The rise of iWar: identity, information, and the individualization of modern warfare. *Strategic Studies Institute and U.S. Army War College Press*. October 2015. URL: https://press.armywarcollege.edu/cgi-/viewcontent.cgi?params=/context/monographs/article/1436/&path_info=2361.pdf (дата звернення: 15.08.2025).

552. Vozniuk E. North Korea Nuclear Program as the Main Source of Instability in Northeast Asia. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2017. № 6 (355). P. 4–11.

553. Vozniuk E. Principles and Features of Japan's Information Security System. *Політичне життя*. № 4. 2017. P. 8–12.

554. Vozniuk E. Vozniuk V. Ukrainian-Polish Relations: Challenges and Perspectives. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2018. № 5 (378). P. 3−9.

555. Vozniuk Ye., Kunytskyy M., Mykhaliuk N., Novak O. International information security. *AD ALTA: Journal of Interdisciplinary Research*. 2021. Vol. 11. Issue 01. P. 429. DOI: 10.33543/1101. URL: https://www.magnanimitas.cz/ADALTA/1101/papers/A_voznyuk.pdf. (дата звернення: 23.08.2025).

556. Voznyuk E. V., Bespalikova O. O. World Leaders in Cyber Security. *Актуальні проблеми регіональних досліджень*: матеріали І Міжнар. наук.-практ. інтернет-конф. (м. Луцьк, 11–12 груд. 2017 р.) / за ред. В. Й. Лажніка. Луцьк: Вежа-Друк, 2017. P. 230–234.

557. WannaCry. URL: https://uk.wikipedia.org/wiki/WannaCry (дата звернення: 15.07.2025).

558. What is China’s Belt and Road Initiative? URL: https://www.theguardian.com/cities/nginteractive/2018/jul/30/what-china-belt-road-initiative-silk-road-explainer (дата звернення: 16.07.2025).

559. What is cyber insurance and why you need it. URL: https://www.cio.com/article/3065655/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html (дата звернення: 08.08.2025).

560. What is hactivism? 2.0. URL: http://www.thehacktivist.com/whatishacktivism.pdf (дата звернення: 24.08.2025).

561. What is Stochastic Terrorism? URL: https://guides.uflib.ufl.edu/stochastic_terrorism (дата звернення: 13.05.2025).

562. What is the Cyberspace Administration of China (CAC). URL: https://www.chinafy.com/blog/what-is-the-cyberspace-administration-of-china-cac (дата звернення: 07.08.2025).

563. Who controls the media in Brazil? URL: https://brazil.mom-gmr.org/ (дата звернення: 12.06.2025).

564. Why 27 % of U.S. Firms Have no Plans to Buy Cyber Insurance. URL: https://www.insurancejournal.com/news/national/2017/05/31/452647.htm (дата звернення: 17.07.2025).

565. Why Russians Are Souring on Putin’s War. URL: https://www.journalofdemocracy.org/online-exclusive/why-russians-are-souring-on-putins-war/ (дата звернення: 13.08.2025).

566. On the Protection of Individuals with regard to the of Personal Data and on the free movement of such Data: Directiva 95/46/EC of the European Parliament and of the Council. URL: https://www.evropa.eu.int/ISPO/legal/en/dataprot/directiv/directiv.html (дата звернення: 12.08.2025).

567. 杂多县举办骨干网评员、通讯员培训会 [Zadoi County held a training session for key online commentators and correspondents]. *The Paper (in Chinese). Cyberspace Administration of China, Zadoi County*. 2019. 14 November.

ДОДАТКИ

Додаток А

Список публікацій здобувача за темою дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації

Статті у виданнях, що індексуються у міжнародних наукометричних базах даних Scopus та Web of Science:

1. Vozniuk Ye., Kunytskyy M., Mykhaliuk N., Novak O. International Information Security. *AD ALTA: Journal of Interdisciplinary Research.* 2021. Vol. 11, Issue 01. P. 381–385. (авторський внесок 25%). **Web of Science, Scopus, Q3.**

DOI: 10.33543/1101.

URL: https://www.magnanimitas.cz/ADALTA/1101/papers/A_voznyuk.pdf.

2. Shuliak A., Vozniuk Ye., Patlashynska I. [et al.]. The Impact of the 4.0 Technological Revolution on the Hybrid War of the Russian Federation in Ukraine. *AD ALTA: Journal of Interdisciplinary Research.* 2022. Special Issue (12/02-XXX). P. 159–164. (авторський внесок 30%). **Web of Science, Scopus, Q3.**

DOI: 10.33543/1202.

URL: http://www.magnanimitas.cz/ADALTA/120230/papers/K_15.pdf.

3. Kachkovska L., Blahovirna N., Vozniuk Ye. [et al.]. Documentary-Information Communication in Public Administration: Legal Aspects and Digital Transformation. *International Journal of Basic and Applied Sciences.* 2025. 14 (3) P. 42–47. (авторський внесок 30%). **Scopus, Q4.**

DOI: 10.14419/v1jmq034.

URL: www.sciencepubco.com/index.php/IJBAS.

4. Shuliak A., Voznyuk Ye, Patlashinska I., Shuliak N. Info-Analytic Support for Ukrainian-Polish Cross-Border Cooperation: a Case Study of Euro-Regions. *Codrul Cosminului*. 2020. Issue 2. Vol. 26. P. 431–454, (авторський внесок 30%) **Scopus, Q2.**

DOI: 10.4316/CC.2020.02.007.

URL: https://codrulcosminului.usv.ro/article-7-vol-26-2-2020/

5. Kotsan N., Kopachinska G., Vozniuk Ye., Kotsan R. Basic Models of Protection and Functioning of the Ukrainian Border in Modern Geopolitical Realities: a View from Ukraine. *European Spatial Research and Policy*. 2022. Vol. 29. N. 1. P. 79–95. (авторський внесок 25%). **Web of Science**, **Scopus, Q2.**

DOI: 10.18778/1231-1952.29.1.04.

URL: https://czasopisma.uni.lodz.pl/esrap/article/view/9908.

Статті у наукових фахових виданнях України:

6. Vozniuk E. North Korea Nuclear Program as the Main Source of Instability in Northeast Asia. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2017. № 6 (355). С. 4–11.

URL: http://nbuv.gov.ua/UJRN/Nvvnum_2017_6_3.

7. Hych I., Vozniuk E. The Threats and Opportunities of Crisis on Ukraine’s Accession to the EU. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2017. № 6 (355). С. 12–16. (авторський внесок 80%).

URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Nvvnum_2017_6_4.

8. Shimuleni M. S., Vozniuk E. Regional Integration and Development: a Theoretical Review of the SADC Region. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2017. № 10 (359). С. 111–116. (авторський внесок 80%).

URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21

REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Nvvnum_2017_10_21.

9. Vozniuk E. Principles and Features of Japan's Information Security System. *Політичне життя.* 2017. № 4. С. 8–12.

URL: https://jvestnik-politology.donnu.edu.ua/index.php/pl/article/view/4933.

10. Hrynchuk V., Vozniuk E. Information Security of India. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини.* 2018. № 1 (374). С. 15–20. (авторський внесок 75%).

11. Ничипорчук Н., Вознюк Є. Секрет успіху США у сфері інформаційної безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2018. № 1 (3). С. 66–71. (авторський внесок 75%).

DOI: 10.29038/2524-2679-2018-01-66-71.

URL: https://relint.vnu.edu.ua/index.php/relint/article/view/28.

12. Vetrov K., Voznyuk Ye. Information Terrorism as a Modern Threat for Information Security of European States. *Міжнародні відносини, суспільні комунікації та регіональні студії,* 2019. № 1 (5). С. 34–42. (авторський внесок 80%).

DOI: 10.29038/2524-2679-2019-01-34-41.

URL: https://relint.vnu.edu.ua/index.php/relint/article/view/88.

13. Вознюк Є. Поширення впливу мексиканських картелів засобами інформаційних технологій і пропаганди. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини.* 2019. № 8 (392). С. 35–41.

URL: https://evnuir.vnu.edu.ua/bitstream/123456789/22741/1/35-41.pdf.

14. Бекеша О., Матюшок В., Вознюк Є. Розвиток кібербезпеки Бразилії на сучасному етапі. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2020. № 2 (406). С. 52–58. (авторський внесок 70%).

URL: https://evnuir.vnu.edu.ua/bitstream/123456789/22730/1/%d0%9d%d0%92_%d0%9c%d0%92_2020_2-52-58.pdf.

15. Вознюк Є., Романцов Д., Рошко І. Кібербезпека в умовах російської агресії. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2020. № 2 (406). С. 58–66. (авторський внесок 70%)

URL: https://evnuir.vnu.edu.ua/handle/123456789/22733.

16. Вознюк Є. Громадські об'єднання на захисті інформаційного простору України. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2021. № 3 (11). С. 48–61.

DOI: 10.29038/2524-2679-2021-03-48-61.

URL: https://relint.vnu.edu.ua/index.php/relint/article/view/230.

17. Вознюк Є. Особливості поширення російських фейків в Україні. *Історико-політичні проблеми сучасного світу: зб. наук. ст*. Чернівці: Чернівец. нац. ун-т, 2021. Т. 44. С. 52–63.

URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Ippss_2021_44_8.

18. Вознюк Є. SWOT-аналіз стану інформаційної безпеки України. *Науковий часопис НПУ імені М. П. Драгоманова. Серія 22: Політичні науки та методика викладання соціально-політичних дисциплін.* 2021. 22 (30). С. 116–124.

DOI: 10.31392/pnspd.v22i30.1147

URL: https://sj.udu.edu.ua/index.php/pnspd/article/view/116-129.

19. Вознюк Є., Андрюхіна В. Порівняльний аналіз кібербезпеки Європейського Союзу. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2025. № 2 (22). С. 161–180. (авторський внесок 75%).

DOI: 10.29038/2524-2679-2025-02-136-154.

URL: https://relint.vnu.edu.ua/index.php/relint/article/view/454.

20. Kachkovska L., Vozniuk Ye. Countering Information Threats in Ukraine: Current Issues for Solving at the State Level. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2024. № 1 (18). С. 85–102. (авторський внесок 60%)

DOI: 10.29038/2524-2679-2024-01-85-102.

URL: https://relint.vnu.edu.ua/index.php/relint/article/view/367.

Статті в іноземних журналах:

21. Novak O., Vozniuk Ye. The Influence of the Information Society Development on Political Ideologies. *Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate.* 2021. 11 (1). P. 19–26. (авторський внесок 70%)

DOI: 10.24917/26578549.11.1.2.

URL: https://studiadesecuritate.uken.krakow.pl/wp-content/uploads/sites/43/2021/06/2_Novak_Vozniuk.pdf.

22. Morenchuk A., Vozniuk Ye., Morenchuk A. junior Sources of Russian Policy Aggressiveness. *Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate*. 2024. 14 (1). P. 91–105. (авторський внесок 60%)

DOI: 10.24917/26578549.14.1.5.

URL: https://studiadesecuritate.uken.krakow.pl/wp-content/uploads/sites/43/2025/04/5.-Andriy-Morenchuk.pdf.

23. Bairak S., Buslenko V., Vozniuk Ye. State Policy in the Field of Information Security Providing in Ukraine. *Annales Universitatis Paedagogicae Cracoviensis*. *Studia de Securitate.* 2024. 14 (1). P. 107–117. (авторський внесок 35%)

DOI: 10.24917/26578549.14.1.6

URL: https://studiadesecuritate.uken.krakow.pl/wp-content/uploads/sites/43/2025/04/6.-Serhii-Bairak.pdf.

Розділи у монографіях:

24. Vozniuk E. Information Terrorism as a Modern Dynamic Part of International Terrorism. *International and National Security: Politics, Information, Ecology, Economy: collective monograph* / ed. by A. Mytko. Kyiv: MPBP «Hordon», 2018. P. 165–174. 320 p.

ISBN 978-966-8398-55-1

URL: https://evnuir.vnu.edu.ua/handle/123456789/23755

25. Вознюк Є. Європейський інспектор із захисту даних. *Зелений і безпечний Європейський Союз: монографія* / [А. О. Бояр (кер. авт. кол.), І. В. Кицюк, Н. І. Романюк та ін.]; за ред. А. О. Бояра, В. Й. Лажніка. Луцьк: Вежа-Друк, 2023. С. 82–85.

ISBN 978-966-940-505-0,

URL: d084d0a1-d0bad0bdd0b8d0b3d0b0_final.pdf (wordpress.com).

Наукові праці,
які засвідчують апробацію матеріалів дисертації:

26. Підлісний А. Ю., Вознюк Є. В. Участь України у миротворчих операціях НАТО. *Актуальні проблеми країнознавчої науки:* матеріали ІІ Міжнар. наук.-практ. інтернет-конференції (м. Луцьк, 14–15 травня 2015 р.) / за ред. В. Й. Лажніка. Луцьк: Вежа-Друк, 2015. С. 187–189.

27. Подолець С. В., Вознюк Є. В. Особливості забезпечення сучасної інформаційної безпеки держави. *Проблеми і перспективи практичної реалізації наукових досліджень:* матеріали XXXVI Міжнар. наук.-практ. конф., Чернівці, 15–16 берез. 2016 р. Т. 2. Київ: Наук.-вид. центр «Лабораторія думки», 2016. С. 31–33.

28. Voznyuk E. V., Voinkova A. O. The Features of Providing Information Security of European Countries. *Актуальні проблеми регіональних досліджень*: матеріали І Міжнар. наук.-практ. інтернет-конференції (м. Луцьк, 11–12 груд. 2017 р.) / за ред. В. Й. Лажніка. Луцьк: Вежа-Друк, 2017. С. 236–240.

29. Ничипорчук Н. С., Вознюк Є. В. Нормативно-правове регулювання інформаційної безпеки США. *Проблеми та перспективи наукових досліджень:* матеріали LX Міжнар. наук.-практ. конф. (Чернівці, 15–16 червня 2018 р.). Київ: Науково-видавничий центр «Лабораторія думки», 2018. С. 28–30.

30. Джигалюк Н., Вознюк Є. Особливості стратегічних комунікацій у німецькомовному інформаційному просторі з точки зору національної безпеки України. *Інформаційна війна як новий вимір геополітичної ривалізації:* матеріали ІІ міжнар. наук.-практ. конф. Луцьк, 2019. С. 8-12

31. Вознюк Є. В. Особливості політичної комунікації сьогодні. *Міжнародні та регіональні системи: актуальні питання міжнародних відносин і регіональних студій*: зб. тез Міжнар. наук-практ. конф. (м. Луцьк, 17 трав. 2019 р.) / за ред. В. Й. Лажніка та С. В. Федонюка. Луцьк: Вежа-Друк, 2019. С. 96–98.

32. Вознюк Є., Дідух Д. Ботоферми як загроза інформаційній безпеці. *Інформаційна гігієна як напрям національної безпеки*: матеріали І міжнар. наук. онлайн-конф. Луцьк, 2021. С. 23–25.

33. Horbach A., Vozniuk Ye. Influence of Non-Governmental Organizations on Information Security of Ukraine. *Актуальні проблеми міжнародних відносин і регіональних досліджень*: матеріали Міжнар. наук.-практ. інтернет-конф. (м. Луцьк, 6 груд. 2021 р.) / за ред. В. Й. Лажніка. Луцьк: Вежа-Друк, 2021. С. 167–170.

URL: https://wiki.vnu.edu.ua/images/d/df/%D0%9A%D0%9E%D0%9D%D0%A4-2021-%D0%B3%D1%80%D1%83%D0%B4.pdf.

34. Шуляк А., Вознюк Є. Інформаційна сингулярність російсько-української війни 2022 р. *Стратегічні комунікації в контексті безпекової політики: європейський і глобальний рівні*: матеріли інтернет-конф. / за заг. ред. Н. Карпчук. Луцьк: ВНУ ім. Лесі Українки, 2022. С. 67–72.

URL: https://inter-dep.vnu.edu.ua/wp-content/uploads/2022/06/%D0%9C%D0%B0%D1%82%D0%B5%D1%80-%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80-19.05.22.pdf

35. Вознюк Є., Крищук А. Початок активного російсько-українського протистояння в кіберпросторі. *Мультидисциплінарні підходи до аналізу суспільно-політичних проблем в умовах російсько-української гібридної війни*: матеріали. міжнар. круглого столу (28 квіт. 2022 р.). Львів: Вид-во Львів. політехніки, 2022. С. 18–21.

URL: https://lpnu.ua/sites/default/files/2022/6/24/news/20253/tpp-verstkatezikrugliystil2022-1.pdf.

36. Baranyk O. S., Vozniuk Ye. V. Global Impact of Information Weapons. *Актуальні проблеми міжнародних відносин і регіональних досліджень:* матеріали III Міжнар. наук.-практ. інтернет-конф. (м. Луцьк, 15 лист. 2023 р.) / укладачі: С. Кулик; О. Борисюк (технічна підтримка). Луцьк: Волин. нац. ун-т ім. Лесі Українки, 2024. С. 250–253.

37. Вознюк Є. Кібербезпека Європейського Союзу: інституційна архітектура та сучасні виклики. *Зовнішнє інформаційне маніпулювання та втручання в умовах сучасних конфліктів*: матеріли інтернет-конф. / за заг. ред. проф. Н. Карпчук. Луцьк: ВНУ ім. Лесі Українки, 2025. С. 106–110.

URL: https://fimieu.wordpress.com/%d0%ba%d0%be%d0%bd%d1%84%d0%b5%d1%80%d0%b5%d0%bd%d1%86%d1%96%d1%97/

38. Завадська В., Вознюк Є. Інформаційна та кібербезпека країн Африки. *Європейська інтеграція України: виклики, досвід, перспективи:* матеріали міжнар. наук.-практ. конф. (Луцьк, 21 трав. 2025 р.) / за заг. ред. С. Федонюка. Луцьк: ВНУ ім. Лесі Українки, 2025. С. 76–79

URL: https://euaccession.wordpress.com/wp-content/uploads/2025/06/d09ad09ed09dd0a4d095d0a0d095d09dd0a6d086d0af-euaccession-2025-1-1.pdf

Наукові праці,

які додатково відображають наукові результати дисертації:

39. Khoma N. Vozniuk E Turkey's Middle East Policy: Vectors, Aims and Results *Studia Politica. Romanian Political Science Review.* Vol. XXI, No. 2, 2021. P. 577-601. **Scopus, Q4**

URL: https://www.researchgate.net/profile/Nataliya-Khoma-2/publication/361182581_Turkey's_Middle_East_Policy_Vectors_Aims_and_Results_Studia_Politica_Romanian_Political_Science_Review_2021_Vol_XXI_No_2_R_578-601/links/62a18d4bc660ab61f86df60a/Turkeys-Middle-East-Policy-Vectors-Aims-and-Results-Studia-Politica-Romanian-Political-Science-Review-2021-Vol-XXI-No-2-R-578-601.pdf.

40. Kotsan R., Kotsan N., Kopachinska G. Vozniuk E Transformations of Ukrainian-Polish border regions transformation: experience of Ukraine. *Forum Geographic* Vol. 21, Issue 1, 2022, pp. 92-101. ***Web of Science***

DOI 10.5775/fg.2022.071.i.

URL: http://forumgeografic.ro/wp-content/uploads/2022/1/Kopachinska.pdf

41. Кулик С., Вознюк Є. Фейк російської пропаганди: Олена Підгрушна – снайпер АТО. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2021. № 1 (9). С. 83–101. ***Фахове видання України.***

DOI: 10.29038/2524-2679-2021-01-82-101

URL: https://relint.vnu.edu.ua/index.php/relint/uk/article/view/125.

42. Вознюк Є. Війна свідомості (консцієнтальна війна), гібридні загрози, інформаційна війна, інформаційний омбудсмен, інформаційний тероризм, культура інформаційної безпеки, методи боротьби з інформацією в електронних засобах масової інформації, операційна безпека «OPSEC». *Глосарій: навчальний енциклопедичний словник-довідник з питань інформаційної безпеки* / за заг. ред. д-ра. політ. наук, проф. А. М. Шуляк, 2019. С. 42–45; 54–56; 135–138; 165–166; 168–170; 242–244; 289–293; 343–345.

43. Wozniuk E. Informacyjny ombudsman; Metody walki z informacją w elektronicznych środkach masowego przekazu. *Vademecum bezpieczeństwa informacyjnego* / red. nauk. Olga Wasiuta, Rafał Klepka. T. 1. Kraków: AT Wydawnictwo, Wydawnictwo LIBRON – Filip Lohner, 2019. P. 452–454, 647–651.

44. Wozniuk E. Terroryzm informacyjny. *Vademecum bezpieczeństwa informacyjnego* / red. nauk. Olga Wasiuta, Rafał Klepka. T. 2. Kraków: AT Wydawnictwo, Wydawnictwo LIBRON – Filip Lohner, 2019. P. 466–468.

Додаток Б

Апробація результатів дисертації здобувачкою Вознюк Є. В.

1. IV Всеукр. наук. конф. з міжнар. участю «Сучасні соціально-гуманітарні дискурси» (м. Дніпропетровськ, 2014);
2. Міжнар. наук.-практ. конф. «Перспективи розвитку науково-практичних досліджень у сфері гуманітарних та суспільних наук» (м. Київ, 2014);
3. Міжнар. наук.-практ. інтернет-конф. «Актуальні проблеми країнознавчої науки» (м. Луцьк, 2015);
4. XXVI Міжнар. наук.-практ. конф. «Зміни в соціально-економічному розвитку країни» (м. Чернівці, 2015);
5. IX Міжнар. наук.-практ. конф. студентів та молодих вчених «Актуальні проблеми зовнішньої політики України» (м. Чернівці, 2015);
6. III Міжнар. наук.-практ. інтернет-конф. «Актуальні проблеми країнознавчої науки» (м. Луцьк, 2015);
7. XXXVI Міжнар. наук.-практ. конф. «Проблеми і перспективи практичної реалізації наукових досліджень» (м. Чернівці, 2016);
8. I Міжнар. наук.-практ. інтернет-конф. «Актуальні проблеми регіональних досліджень» (м. Луцьк, 2017);
9. LX Міжнар. наук.-практ. конф. «Проблеми та перспективи наукових досліджень» (м. Чернівці, 2018);
10. II міжнар. наук.-практ. конф. «Інформаційна війна як новий вимір геополітичної ривалізації» (м. Луцьк, 2019);
11. Міжнар. наук-практ. конф. «Міжнародні та регіональні системи: актуальні питання міжнародних відносин і регіональних студій» (м. Луцьк, 2019);
12. II Міжнар. наук.-практ. конф. «Інформаційна війна як новий вимір геополітичної ривалізації» (м. Луцьк, 2019);

13. Міжнар. наук.-практ. конф. «Інформаційна гігієна як напрям національної безпеки» (м. Луцьк, 2021);

14. Міжнар. наук.-практ. інтернет-конф. «Актуальні проблеми міжнародних відносин і регіональних досліджень» (м. Луцьк, 2021);

15. Міжнар. наук.-практ. інтернет-конф. «Стратегічні комунікації в контексті безпекової політики: європейський і глобальний рівні» (м. Луцьк, 2022);

16. Міжнар. круглого столу «Мультидисциплінарні підходи до аналізу суспільно-політичних проблем в умовах російсько-української гібридної війни» (м. Львів, 2022);

17. ІІІ Міжнар. наук.-практ. інтернет-конф. «Актуальні проблеми міжнародних відносин і регіональних досліджень» (м. Луцьк, 2023);

18. Міжнар. наук.-практ. інтернет-конф. «Зовнішнє інформаційне маніпулювання та втручання в умовах сучасних конфліктів», (м. Луцьк, 2025);

19. Міжнар. наук.-практ. конф. «Європейська інтеграція України: виклики, досвід, перспективи: матеріали Міжнар. наук.-практ. конф. (Луцьк, 2025).

Додаток В

Етапи становлення та розвитку концепції інформаційного тероризму

Період / рік	**Подія / концепт**	**Що з'являється / як змінюється**	**Значення для інформаційного тероризму**
1	2	3	4
Давнина / класичний період	Стратегеми інформаційного впливу – «викривлення фактів», риторика, пропаганда	У праці Сунь-цзи й пізніших мислителів – ідеї про вплив на мораль і волю супротивника	Дає «прецеденти» для розуміння, що інформація – частина війни
XIX – початок XX ст.	Друк, масова преса, політична пропаганда	Засоби поширення ідей стають масовими; націоналістичні рухи використовують пропаганду	Формуються технології комунікації, які пізніше стануть фундаментом інформаційних атак
Перша половина XX ст.	Радіо, кінематограф, централізовані державні пропагандистські машини	Тоталітарні режими використовують мас-медіа як інструмент контролю	Зростає вплив державних медіа у формуванні світоглядів
Середина XX ст.	Холодна війна – «активні заходи», дезінформація, психологічна війна	Стратегії агентурного впливу, фальшиві документи, підставні організації, операції спецслужб	Починає формуватися концепція «інформаційної зброї» як такої
1980-ті	Поява «інформаційної війни» як терміна (наприклад у Китаї 1985 р.)	Визнання, що стратегії інформаційного впливу – це окрема «війна» без прямих бойових дій (social-science.uu.edu.ua)	Виникає термінологічна база, концепції «політика через інформацію»
1980–1990-ті	Кібернетичні атаки, саботаж інформаційних систем	Наприклад, група CLODO у Франції атакувала комп'ютерні центри 1980-х як акти проти	Атаки на інфраструктуру – перші «грузини» кібер/інформаційної складової

Період / рік	**Подія / концепт**	**Що з'являється / як змінюється**	**Значення для інформаційного тероризму**
1	2	3	4
		інформаційної інфраструктури (Вікіпедія)	
1990–2000-ті	Інтернет, глобалізація, цифрові платформи	Зростання значення мереж, поширення інформації із географічних обмежень	З'являється середовище, де інформаційні атаки можуть бути масовими, швидкими
Середина 2000-х	«Тероризм 2.0» / мережевий тероризм	Використання соціальних мереж для пропаганди, вербування, координації дій	Підсилюється роль платформи як носія інформаційної агресії
2010–2015	Активні інформаційні кампанії, гібридна війна	Російська кампанія проти України, операції впливу на вибори в США (IRA), Cambridge Analytica	Поява «інформаційного фронту» як складової частини сучасного конфлікту
2020–2022	Інфодемія, пандемія, синтетичні маніпуляції	COVID-19 породжує хвилі дезінформації, вимога контролю інформаційного простору	Концепція «інформаційного тероризму» починає охоплювати й громадські шоки
2022–дотепер	Повномасштабна інформаційна війна, OSINT, deepfakes	У війні України ми бачимо поєднання атак, контрдій, масових дезінформаційних кампаній	Інформаційний тероризм стає не абстрактним, а тактичним елементом війни

Джерело: розробка здобувача.

Додаток Д

Розширений аналіз із прикладами застосування інформаційної зброї окремими державами, *які активно використовують ці інструменти в глобальному інформаційному просторі*

Таблиця Д.1

Застосування інформаційної зброї. РФ

Тип інформаційної зброї	**Приклади застосування**	**Мета**
Дезінформація, deepfakes, тролі	Агентство «Інтернет-досліджень» (т. зв. «фабрика тролів» у Санкт-Петербурзі), фейкові новини про «біолабораторії» в Україні	Дискредитація Заходу, виправдання агресії, деморалізація противника
Кібератаки	Атака на електромережу України (2015, 2016), злам урядових сайтів перед вторгненням 2022 року	Дестабілізація інфраструктури
PSYOPS	Масове розсилання повідомлень у месенджерах про «здачу ЗСУ», фейки про «втрати»	Паніка, демотивація українського населення
Алгоритмічний вплив	Маніпуляції через Telegram-канали, YouTube з російською пропагандою	Вплив на громадську думку в Україні, ЄС

Джерело: розробка здобувача.

Таблиця Д.2

Застосування інформаційної зброї. Китай

Тип інформаційної зброї	**Приклади застосування**	**Мета**
1	2	3
Цензура й інформаційні блокади	Великий Китайський Фаєрвол, контроль над пошуковиками та соцмережами	Формування контрольованої реальності всередині країни

Тип інформаційної зброї	Приклади застосування	Мета
Дезінформація за кордоном	Кампанії про COVID-19 (перекладання провини на інші держави), просування версії про «нормальність» політики щодо уйгурів	Захист іміджу, просування «м'якої сили»
Цільова пропаганда	Використання TikTok для м'якої пропаганди серед молоді	Формування позитивного іміджу Китаю

Джерело: авторська розробка.

Таблиця Д. 3

Застосування інформаційної зброї. Іран

Тип інформаційної зброї	Приклади застосування	Мета
Соціальна інженерія, фішинг	Злам акаунтів журналістів, активістів в Ізраїлі	Збір даних, шантаж
Фейкові акаунти в соцмережах	Маскування під західні акаунти на Facebook, Twitter	Вплив на вибори, посилення ісламських меседжів
PSYOPS у Близькому Сході	Відео про «мучеників», маніпуляції релігійною риторикою	Мобілізація шиїтської аудиторії

Джерело: розробка здобувача.

Таблиця Д. 4

Застосування інформаційної зброї. США

Тип інформаційної зброї	Приклади застосування	Мета
Психологічні операції (PSYOPS)	В'єтнам, Ірак, Афганістан – листівки, радіо, відеозаписи	Деморалізація ворога
Кібероперації	Stuxnet (2010) – вірус проти іранської ядерної програми	Фізичне знищення інфраструктури через IT
Цільова пропаганда	«Голос Америки», USAID-ініціативи	Поширення демократичних цінностей, контрпропаганда

Джерело: розробка здобувача.

Додаток Е

Візуалізація індексу інформаційної стійкості

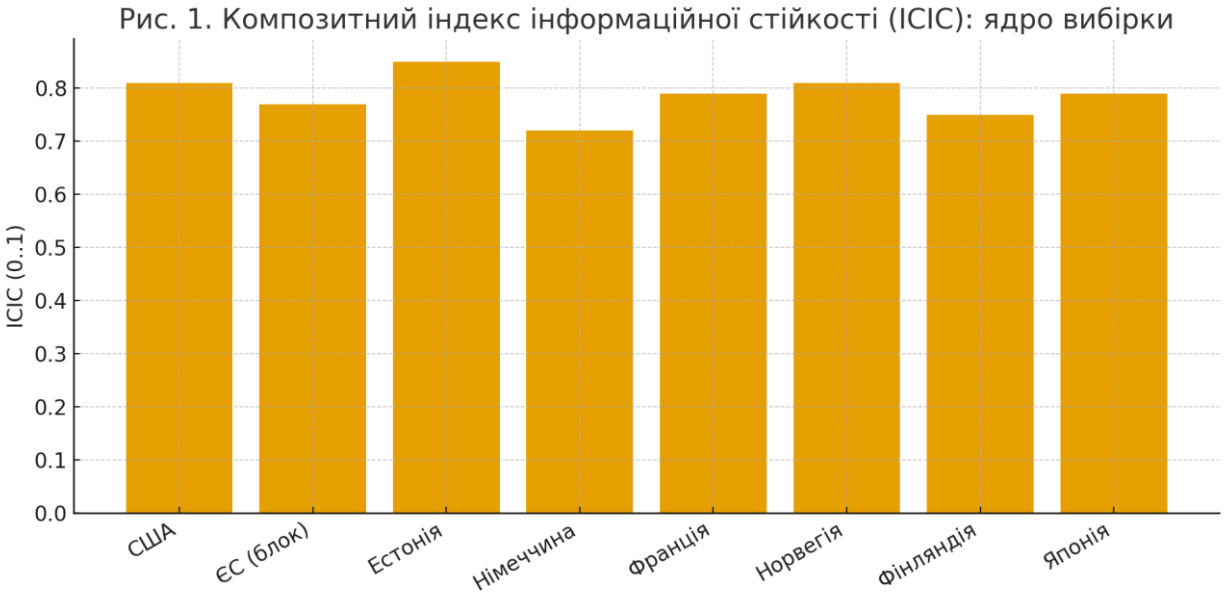


Рис. Є. 1. ***Композитний індекс інформаційної стійкості (ICIC) ядро вибірки за розділом 4.***

Джерело: розробка здобувача.

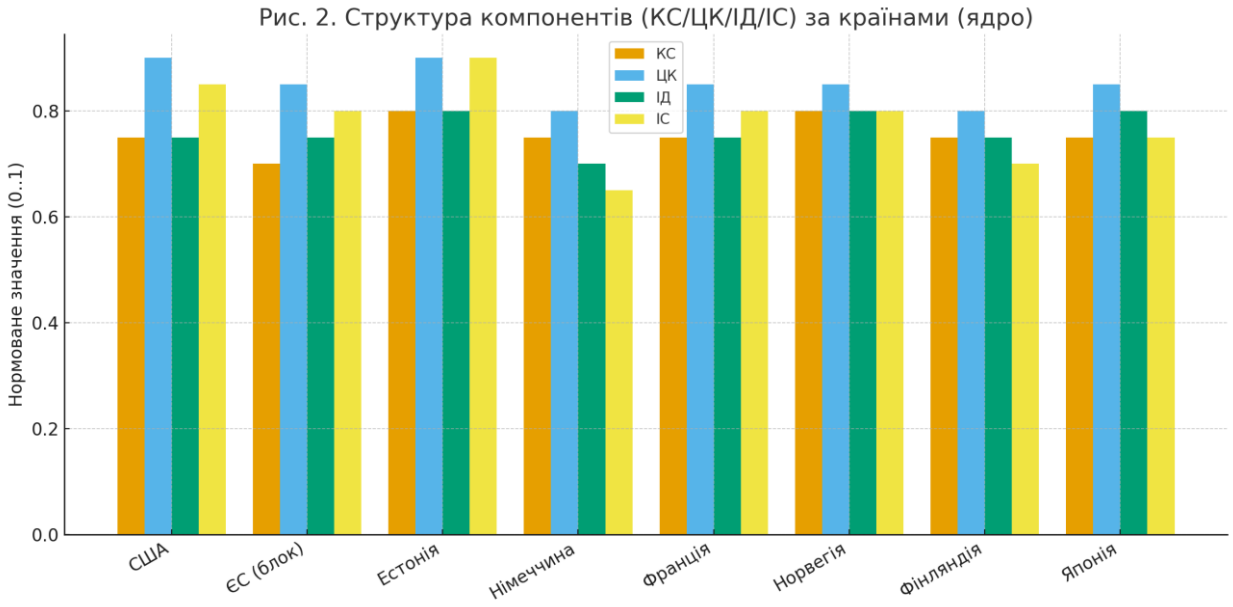


Рис. Є. 2. ***Структура компонентів (КС/ЦК/ІД/ІС) за країнами (ядро вибірки за розділом 4)***

Джерело: авторська здобувача.

Рис. 3. ICIC: регіональне порівняння (Африка/Лат. Америка) та кей

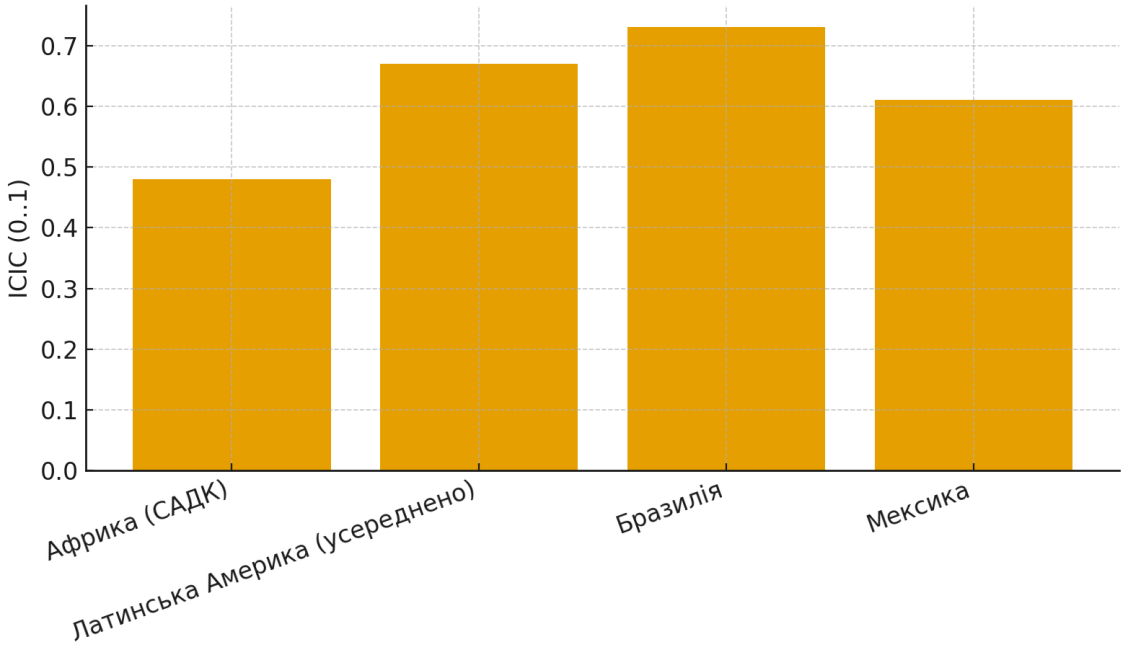


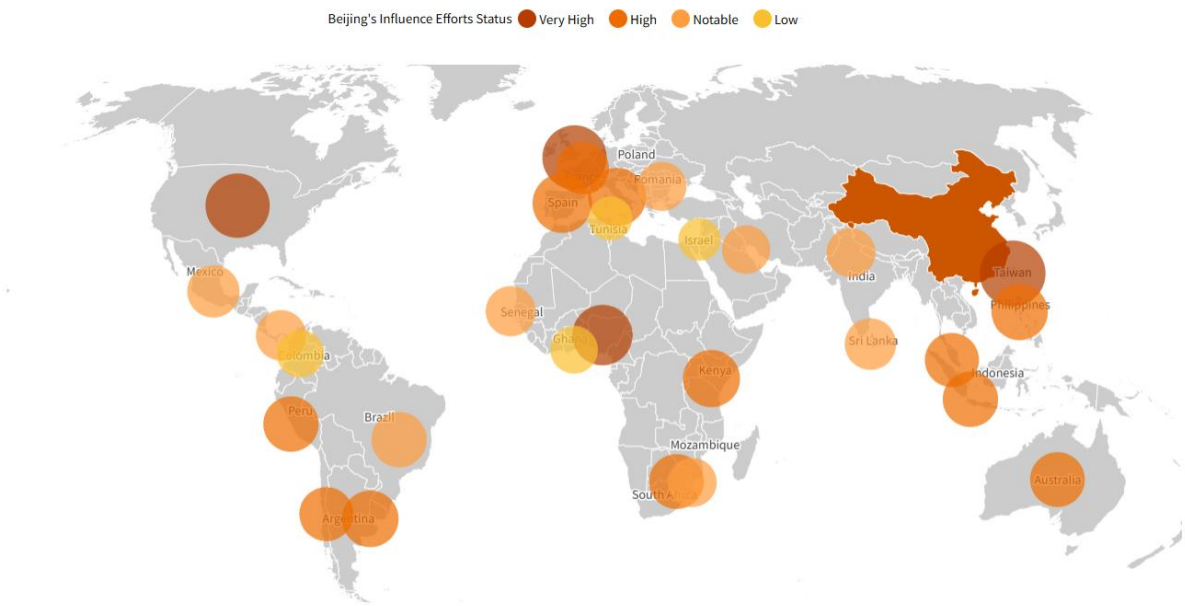
Рис. Є. 3. ***ICIC: регіональне порівняння =та кейси***

(ядро вибірки за розділом 4.3)

Джерело: розробка здобувача.

Додаток Є

Глобальний медіавплив Пекіна 2022



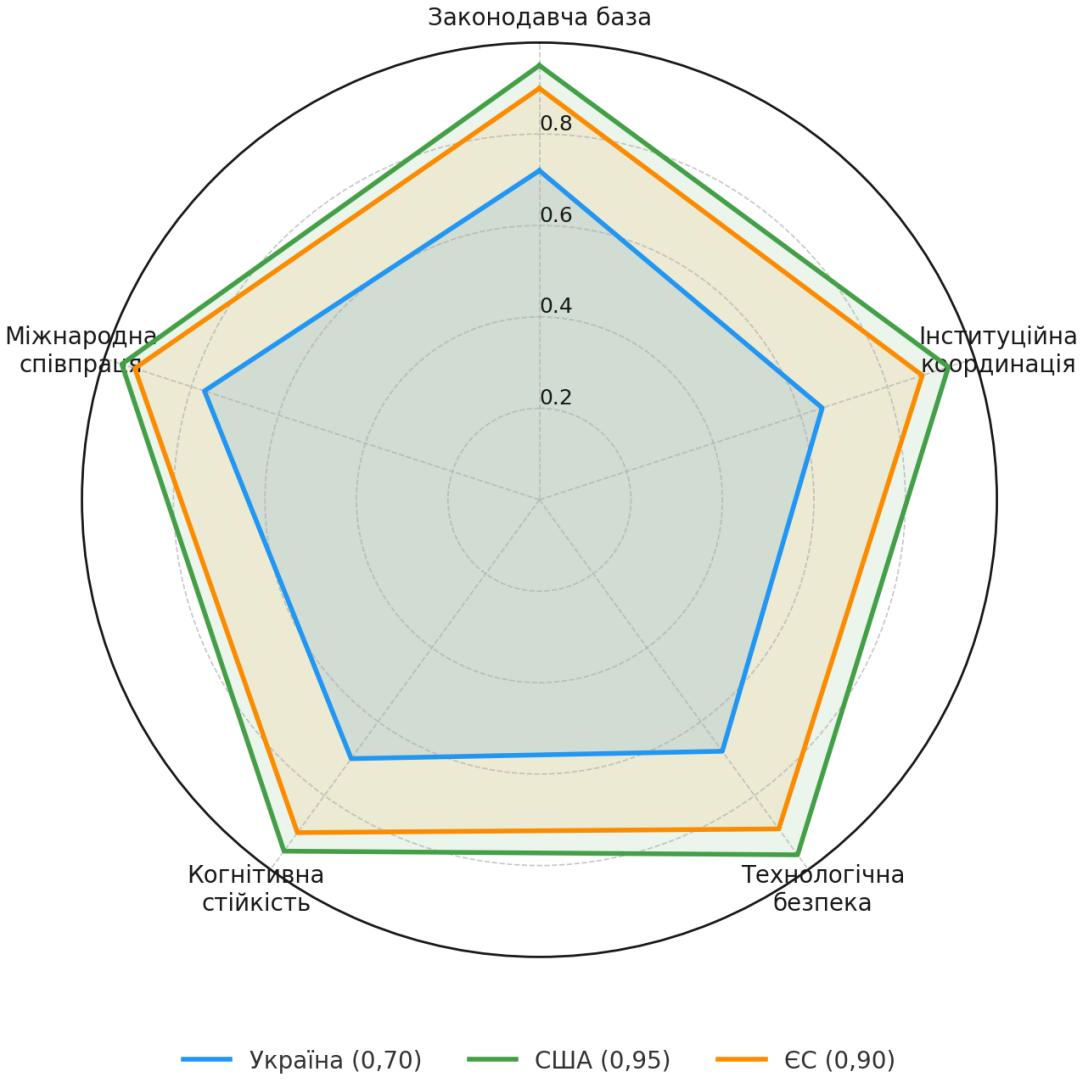
Мал. Е.1. ***Глобальний медіавплив Пекіна 2022:***

Авторитарна експансія та сила демократичної стійкості[1]

[1] Beijing's Global Media Influence 2022. URL : https://freedomhouse.org/report/beijing-global-media-influence/2022/authoritarian-expansion-power-democratic-resilience?utm_source=chatgpt.com (дата звернення 08.08.2025)

Додаток Ж

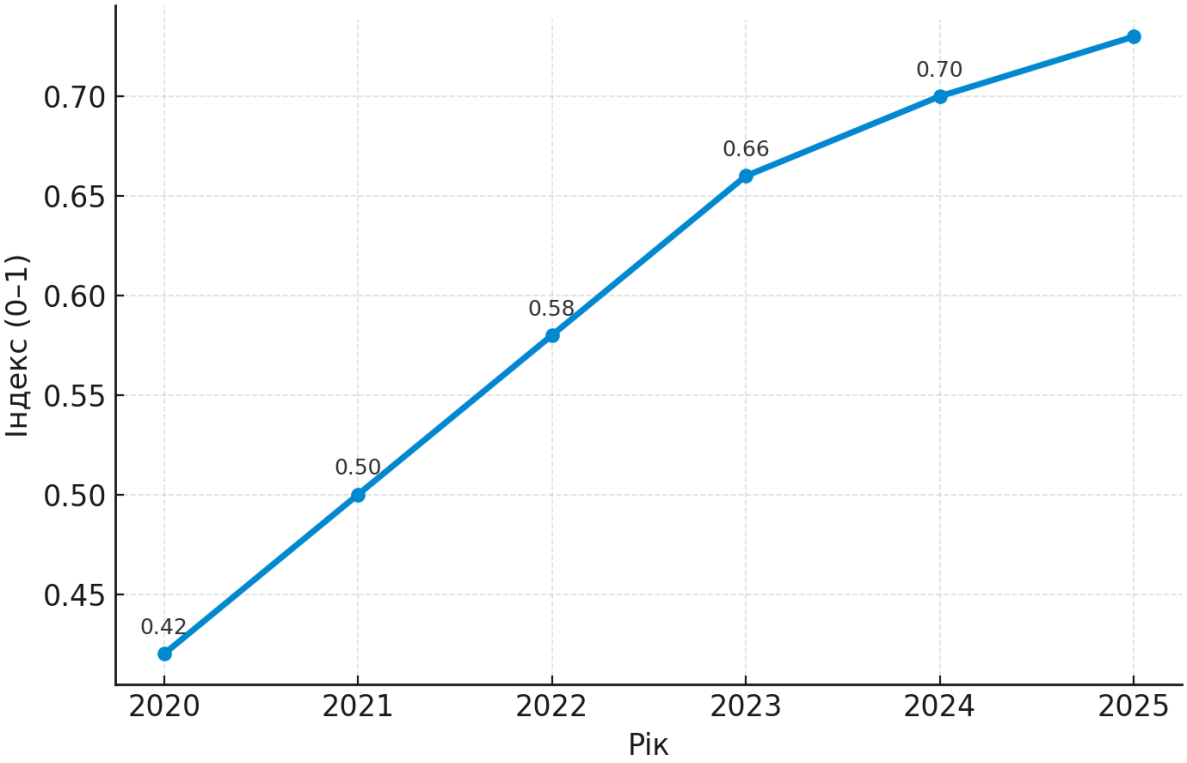
Інформаційна стійкість України



Джерело: авторська розробка.

Рис. Ж. 1. ***Профіль інформаційної стійкості України (ІСІС)***

Джерело: розробка здобувача.



Джерело: авторська розробка.

Рис. Ж. 2. ***Динаміка індексу ICIC України (2020–2025)***

Джерело: розробка здобувача.

Додаток З

Рекомендації для України щодо інформаційної стійкості

Таблиця З. 1

Рекомендації для України → конкретний крок → очікуваний ефект (індикатор)[2]

Виявлена проблема	**Крок політики**	**Очікуваний ефект**
Фрагментарність координації, різні центри відповідальності	Створити **єдиного нацкоординатора** інформац./кіберстійкості з мандатом над ЦОВВ+КІ; запровадити *обов'язковий інцидент-репортинг* (24–72 год) для операторів КІ	↑ІД, ↑ІС
Застарілі ІТ/нерівна зрілість захисту	Увести **держпрофіль Zero Trust** для держсектору/КІ; **SBOM** у держзакупівлях; щорічні **стрестести** (cyber + comms)	↑ЦК, ↑ІС
Deepfake/ІІ-маніпуляції	Наццентр **детекції/атрибуції ІІ-контенту** (форензика відеозвуку, верифікація), протокол кризових комунікацій (єдина мова/частота брифінгів)	↑ІД, ↑КС
Анонімні канали/ботоферми	Розширити **правозастосування**: прозорість походження контенту/реклами; швидкі **Takedown-процедури** з платформами; «чорні списки» бот-мереж	↑ІД
Кадровий дефіцит	Нацпрограма **кадрового резерву кібербезпеки** (стипендії, швидкі треки в ЦОВВ/КІ), держ-програма *bug-bounty*	↑ЦК
Низька цифрова грамотність частини населення	Масштабувати **медіаосвіту** (школи/ЗВО/служба), регулярні **антифішингові кампанії** з банками/поштовими сервісами	↑КС

[2] *Кожен крок напряму випливає із зазначених у тексті вразливостей і вже наявних інституцій*

Таблиця 3. 2

Цільові орієнтири (24–36 міс.) та очікувана динаміка індексу[3]

Індикатор	**12 міс.**	**24 міс.**	**36 міс.**	**Ключовий драйвер**
КС	0,80	0,82	**0,84**	Медіаосвіта + антифішинг, контр-deepfake
ЦК	0,75	0,78	**0,82**	Zero Trust, SBOM, stress-tests
ІД	0,64	0,68	**0,72**	Єдиний координатор, кризкомунікації
ІС	0,72	0,75	**0,78**	Інцидент-репортинг, ISAC-мережа
ІСІС	**0,73**	**0,76**	**0,79**	Комплексна реалізація

Джерело: розробка здобувача.

Таблиця 3. 3

Індикатори інформаційної стійкості України порівняно з провідними демократіями

№	**Індикатор**	**США**	**ЄС**	**Україна**	**Рівень України**
1	Нормативно-правова база у сфері кібер- та інформаційної безпеки	Високий (NIST, CISA, Executive Orders)	Високий (NIS2, DSA)	Середній (фрагментарні закони, проєкти)	Часткова відпо-відність
2	Інституційна координація (центральний орган, стратегія)	Висока (CISA, USCYBERCOM)	Висока (ENISA, CERT-EU)	Середня (CERT-UA, Держспец-зв’язку)	Недостатня інтеграція
3	Система реагування на інциденти	Висока	Висока	Середня	Часткова готовність
4	Рівень цифрової грамотності населення	Високий	Високий	Середній	Залежить від регіону
5	Кіберстрахування,	Розвинене	Частково розвинене	Низьке	Потребує розвитку

[3] *Досягнення 0,79 означає вихід до «високої» межі; найбільші прирости дають ZT/SBOM та інцидент-репортинг.*

№	Індикатор	США	ЄС	Україна	Рівень України
	економічна стійкість				
6	Протидія дезінформації та стратегічні комунікації	Висока (CISA, GEC, FactCheck.org)	Висока (East StratCom, EUvsDisinfo)	Середня (Центр стратегічних комунікацій)	Проміжний рівень
7	Міжнародна кооперація у сфері кібербезпеки	Висока	Висока	Висока (НАТО, ЄС)	Високий потенціал

Джерело: розробка здобувача.

Таблиця 3. 4

Динаміка основних показників інформаційної стійкості України (2020–2025)

Рік	Індекс інформаційної стійкості (ICIC)	Кількість кібератак (тис.)	Рівень довіри до державних онлайн-сервісів, *(%)*	Частка населення з базовою цифровою грамотністю, *(%)*
2020	0,42	22,5	31	48
2021	0,49	25,8	40	56
2022	0,56	38,4	45	60
2023	0,63	41,0	52	65
2024	0,69	47,2	58	70
2025*	0,73 (прогноз)	50,0 (зменшення ефективних атак)	63	75

Джерело: розробка здобувача.

Додаток И

Нормативно-правові засади забезпечення інформаційної стійкості в контексті протидії тероризму

1. Стан нормативного забезпечення

Закон України *«Про боротьбу з тероризмом»* (2003 р.) був ухвалено в контексті класичної парадигми безпеки, де тероризм трактувався переважно як фізичне насильство – вибухи, захоплення заручників, насильницькі акти з використанням зброї чи небезпечних речовин. Його структура зосереджена на запобіганні, виявленні та припиненні злочинів, що мають матеріальну форму прояву.

Однак трансформація терористичних практик у добу цифрових технологій зумовила виникнення нових форм – інформаційного та кібертероризму, які здійснюються не шляхом фізичного впливу, а через інформаційно-психологічні операції, кібератаки, маніпуляції свідомістю населення, використання дезінформаційних кампаній та технологій штучного інтелекту. У цьому контексті чинна редакція закону не забезпечує достатньої нормативної бази для протидії інформаційним формам терористичної діяльності, не визначає інформаційну стійкість як критерій безпеки, не передбачає процедур моніторингу та реагування на інформаційні інциденти.

2. Необхідність інтеграції концепту інформаційної стійкості в антитерористичну політику

Інформаційна стійкість держави постає антиподом інформаційного тероризму та одним з індикаторів ефективності системи національної безпеки. Її сутність полягає в спроможності суспільства, інституцій і держави зберігати когнітивну рівновагу, достовірність інформаційного середовища та довіру до легітимних джерел у ситуаціях гібридних загроз. Уключення цього концепту до законодавчої системи протидії тероризму забезпечить перехід від реактивної моделі – реагування на вже скоєні акти – до превентивної та

адаптивної, що ґрунтується на моніторингу, аналітиці, освіті та цифровій компетентності.

3. Концептуальні напрями модернізації Закону України «Про боротьбу з тероризмом»

3.1. Розширення термінологічного апарату

Доцільним є введення до закону нових дефініцій, які б відображали сучасні виклики безпеки:

- Інформаційний тероризм – цілеспрямоване використання інформаційних технологій, цифрових платформ і засобів масової комунікації для дестабілізації суспільства, підриву авторитету держави, маніпулювання громадською свідомістю або залякування населення.
- Кібертероризм – здійснення терористичних дій у кіберпросторі, зокрема кібератак на критичну інформаційну інфраструктуру, банківські системи, енергетичні мережі тощо.
- Інформаційно-психологічна операція (ІПсО) – скоординований вплив на масову свідомість, щоб змінити поведінку суспільних груп, дестабілізувати політичну ситуацію або сприяти реалізації терористичних цілей.

Уключення таких понять створить правову основу для кваліфікації інформаційних атак як форм терористичної діяльності.

3.2. Розширення об'єктів терористичних посягань

Чинний закон визначає основними об'єктами терористичних посягань людей, державні органи, підприємства, громадські об'єднання та об'єкти інфраструктури.

У сучасних умовах до цього переліку треба додати:

«інформаційні ресурси, системи електронних комунікацій, цифрові платформи, медіапростір, соціальні мережі, канали масової комунікації та інші елементи національної інформаційної інфраструктури».

Таке доповнення дасть змогу офіційно розглядати атаки на інформаційні системи як терористичні дії, що мають потенціал масового ураження – через паніку, дезінформацію, знищення цифрових даних.

3.3. Уведення статті «Інформаційно-терористична діяльність»

Запропоновано доповнити закон новою статтею, яка б регулювала форми та наслідки інформаційно-терористичної діяльності:

Стаття Х. Інформаційно-терористична діяльність

1. Підготовка, організація або здійснення інформаційно-психологічних операцій, кібератак, масового поширення дезінформації чи фальсифікованого контенту з метою дестабілізації суспільного порядку або підриву національної безпеки визнається актом тероризму.

2. Особи, винні у вчиненні таких дій, несуть кримінальну відповідальність відповідно до закону.

3. Суб'єкти критичної інформаційної інфраструктури зобов'язані повідомляти уповноважені органи про інформаційні інциденти протягом 24 годин із моменту їх виявлення.

4. Уряд України забезпечує створення та функціонування єдиного національного центру моніторингу, аналізу й реагування на інформаційно-терористичні загрози.

3.4. Запровадження принципу інформаційної стійкості

До статті 4 Закону («Основні принципи боротьби з тероризмом») доцільно включити принцип інформаційної стійкості, який передбачає:

- забезпечення достовірності, прозорості та безперервності офіційних комунікацій у кризових ситуаціях;
- розвиток критичного мислення й медіаграмотності громадян;
- системну взаємодію держави, медіа, наукових установ і громадянського суспільства в протидії інформаційному тероризму;
- використання сучасних цифрових технологій для моніторингу й нейтралізації деструктивних інформаційних впливів.

Отже, законодавство отримує стратегічний вимір, орієнтований на підтримку когнітивної та соціальної стабільності як складової частини безпеки.

3.5. Освітньо-просвітницький компонент

Із метою запобігання інформаційному тероризму потрібно запровадити окремий розділ або підрозділ у законі щодо освітніх заходів, зокрема:

- створення державних програм медіаосвіти та кібергігієни для школярів, студентів, держслужбовців;
- розробку навчальних курсів і тренінгів із виявлення дезінформації;
- підтримку незалежних фактчекінгових організацій;
- формування культури «інформаційної відповідальності» у громадян.

Цей компонент розширює антитерористичну політику в напрямі профілактики та підвищення когнітивної стійкості населення.

3.6. Міжнародна співпраця

До статті 7 («Міжнародне співробітництво») запропоновано додати положення про участь України в міжнародних ініціативах щодо протидії інформаційному тероризму, обмін розвідувальними даними, спільні кібернавчання, визнання цифрових доказів відповідно до стандартів ЄС і НАТО.

4. Очікувані результати впровадження

Імплементація запропонованих змін дасть змогу:

1. Розширити поняття тероризму до рівня сучасних гібридних загроз.
2. Підвищити ефективність національної системи реагування на кібератаки та інформаційні кампанії.
3. Інституціоналізувати механізми оцінки й моніторингу інформаційної стійкості як офіційного показника безпеки.
4. Сформувати міжвідомчу координацію між СБУ, МВС, Міноборони, Мінцифри, Мінінформполітики та громадянським сектором.

Підвищити довіру населення до державних комунікацій і знизити вплив інформаційного тероризму на суспільну свідомість.