Київський національний університет імені Тараса Шевченка
Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка
Міністерство освіти і науки України

Кваліфікаційна наукова праця на
правах рукопису

ФУРСАЙ ОЛЕКСАНДРА ВОЛОДИМИРІВНА

УДК 351.746.1+004.056:342.1
(44):327.51(410:477:4-672ЄС)(043.3)

ДИСЕРТАЦІЯ

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФРАНЦУЗЬКОЇ РЕСПУБЛІКИ В УМОВАХ МІЖНАРОДНО-ПОЛІТИЧНИХ ТРАНСФОРМАЦІЙ

Галузь знань 29 – «Міжнародні відносини»
Спеціальність 291 – «Міжнародні відносини, суспільні комунікації
та регіональні студії»

Подається на здобуття наукового ступеня доктора філософії

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

Науковий керівник **Даниленко Сергій Іванович**, доктор політичних наук, професор

Київ – 2024

АНОТАЦІЯ

Фурсай О. В. Політика інформаційної безпеки Французької Республіки в умовах міжнародно-політичних трансформацій.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 291 – Міжнародні відносини, суспільні комунікації, регіональні студії. – Київський національний університет імені Тараса Шевченка, МОН України. – Київ, 2024.

Дисертаційну роботу присвячено дослідженню політики інформаційної безпеки Франції в умовах трансформації системи міжнародних відносин, для якої все більш характерною є зростаюча роль інформаційно-технологічної складової як одного із ключових чинників могутності та впливу держави на міжнародній арені.

У роботі розглянуто теоретико-методологічні аспекти інформаційної безпеки, її взаємозв'язок з концепціями «м'якої сили», «розумної сили», «гібридної війни», а також ключові особливості політики інформаційної безпеки на наднаціональному та національному рівнях.

Узагальнено діяльність міжнародних акторів в сфері інформаційної безпеки, зокрема національних – Франції, Великої Британії та Німеччини, та наднаціональних – Європейського Союзу та Північноатлантичного альянсу (НАТО). Політики інформаційних суб'єктів досліджені на кількох рівнях:

- нормативно-правова та концептуальна основи політик, де досліджено ключові стратегічні документи, закони, концепції, рішення, які регламентують діяльність акторів у сфері інформаційної безпеки;

- інституційна структура, де досліджено організацію зазначених суб'єктів, ключові органи, їх роботу та результати цієї роботи;

- роль приватного сектору та громадськості у формуванні та реалізації політики інформаційної безпеки;

- конкретні приклади реалізації політики інформаційної безпеки, які дають зрозуміти особливості взаємодії цих політик з реальним політичним середовищем.

Особлива увага надана дослідженню політики інформаційної безпеки в частині протидії інформаційним загрозам та викликам, згенерованих в рамках

гібридної війни Росії проти Заходу. Методом компаративного аналізу виокремлено ключові тенденції, закономірності та специфіку політик інформаційної безпеки зазначених суб'єктів міжнародних відносин.

Акцент дисертаційної роботи на політиці інформаційної безпеки Франції дозволив розглянути цей напрям політики Франції у всій його комплексності та системності. Зокрема, детально досліджено нормативно-правову базу, яка визначає та регулює політику інформаційної безпеки Французької Республіки, встановлено інституційну структуру, на яку опирається ця політика, та деталізовано роль громадськості та приватного сектору як партнерів держави в убезпеченні суспільства від загроз інформаційної доби. На прикладі конкретних кейсів інформаційних викликів, які поставали перед Францією, продемонстровано здатність вибудованої політики інформаційної безпеки ефективно реагувати та протидіяти насамперед зовнішнім загрозам.

Окрім цього, виокремлено ключовий ефективний досвід реалізації політики інформаційної безпеки Франції у контексті його потенційного використання Україною у розбудові аналогічної власної політики. Такий підхід дозволяє оцінити політику Франції з точки зору її прикладної користі як шаблону для інших національних держав.

Наукова новизна дослідження полягає в актуальному та системному аналізі політики інформаційної безпеки Франції в сучасних міжнародних відносинах. Дисертаційна робота розглядає актуальні тенденції теорії та практики зовнішньої та безпекової діяльності держав-лідерів Європи. Зокрема, розглянуто питання інформаційної безпеки не з технічної точки зору, а з урахуванням численних політичних, соціально-економічних і міжнародних чинників. Так, досліджено політику інформаційної безпеки Франції у її взаємозв'язку з аналогічною політикою ЄС та НАТО щодо позиції власного суспільства, зокрема інформаційними гравцями на кшталт бізнесу та громадськості, а також виокремлено напрям інформаційної політики Франції з протидії російським гібридним загрозам.

Наукова новизна дослідження визначається також і тим, що питання інформаційної безпеки розглядаються як одне з найбільш актуалізованих напрямів у забезпеченні національної безпеки Французької Республіки. У зв'язку з цим особлива увага надана питанням державного регулювання в сфері інформаційної безпеки.

За результатами дисертаційної роботи сформульовано авторські основні положення, які містять елементи наукової новизни та виносяться на захист. Основними з них є такі:

уперше:

- комплексно досліджено на сучасному етапі політику інформаційної безпеки Франції як у її внутрішньому національному вимірі, так і в контексті лідерства Франції в ЄС, та цілеспрямованої стратегії офіційного Парижу з посилення власної геополітичної ролі;

- систематизовано у прикладному вимірі особливості та ключові складові політики інформаційної безпеки Франції як набору підходів та практик, які можуть бути використані Україною для зміцнення власної інформаційної безпеки, зокрема в контексті повномасштабної агресії Росії. Також виділено ті напрями співпраці між двома державами, які можуть бути найбільш перспективними для України щодо посилення свого інформаційно-технологічного потенціалу;

- методом компаративного аналізу проведено порівняння актуальних політик інформаційної безпеки лідерів Європи – Франції, Німеччини та Великої Британії, що дозволило виокремити ключові «плюси» та «мінуси» підходів цих держав, що своєю чергою дозволило зробити необхідні висновки для удосконалення політики інформаційної безпеки України.

удосконалено:

- розуміння державної політики Франції у сфері національної безпеки, зокрема фокус на інформаційній складовій дозволив покращити наукову «візуалізацію» такої політики як складної, комплексної системи, яка опирається на використання Францією «розумної сили» як ключового фактору нарощування власного геополітичного впливу;

- розуміння специфіки синхронізації політик інформаційної безпеки національного актора-члена ЄС та безпосередньо Європейського Союзу як організації. На прикладі Франції продемонстровано процес паралельного скоординованого руху національних політик та європейської стратегії;

- аналіз політики інформаційної безпеки Франції як складної системи суб'єктів, які включають як державу, так і приватних акторів, громадськість, зокрема фактчекінгові організації та ЗМІ. Це дозволило розглянути інформаційну безпеку як комплексну екосистему.

набуло подальшого розвитку:

- дослідження політики інформаційної безпеки на наднаціональному та національному рівнях, і встановлено, що в умовах поглиблення інтеграції всередині Європейського Союзу важливою є співпраця та максимальна координація зусиль національних держав та наднаціональних інституцій задля ефективної протидії сучасним інформаційним викликам;

- дослідження зовнішньої політики Франції, у частині її інформаційного наповнення, в умовах трансформації системи міжнародних відносин, зокрема зростанням рівня гібридизації загроз з акцентом на інформаційно-технологічну складову. Доведено важливість швидкої адаптації держави, приватного сектору та громадськості до нових викликів та інформаційно-технологічного поступу як необхідної умови «виживання» в сучасних реаліях глобального інформаційного протиборства;

- визначення ключових компонентів політики інформаційної безпеки Франції на нормативно-правовому та інституційному рівнях в сферах протидії дезінформації та кібератакам. На основі цього запропоновано висновки для удосконалення політики інформаційної безпеки України як однієї з необхідних умов перемоги у російсько-українській війні.

Практичне значення одержаних результатів полягає у можливості використання висновків дослідження для подальших наукових розвідок політики інформаційної безпеки, зокрема в контексті євроінтеграційного руху України.

Також результати дисертації можуть використовуватися у діяльності дипломатичних установ та Міністерства закордонних справ України, зокрема у напрямі співпраці з міжнародними організаціями, альянсами та іншими партнерами. Також вони можуть стати важливим джерелом інформації для урядових, політичних та громадських інституцій, чиєю сферою відповідальності є стратегічне планування національної безпеки та оборони. Так, висновки дослідження можуть бути враховані у процесі вдосконалення Стратегії кібербезпеки та Доктрини інформаційної безпеки України.

Окрім цього, результати можуть бути використані українськими медіа та фактчекінговими організаціями для взяття на озброєння досвіду Франції, зокрема держави, приватного сектору, громадськості для удосконалення власної роботи з боротьби з дезінформацією та деструктивним інформаційним впливом з-поза меж країни.

Ключові слова: інформаційна безпека, дезінформація, кіберпростір, гібридна війна, Франція, Європейський Союз, НАТО, Україна, Велика Британія, Німеччина, Росія, кібератака, національна безпека, ЗМІ, міжнародні організації, міжнародно-політичні трансформації.

ABSTRACT

Oleksandra Fursai. Information security policy of the French Republic in the context of international political transformations.

The thesis for the Doctor of Philosophy degree on speciality 291 – International Relations, Social Communications and Regional Studies. – Taras Shevchenko National University of Kyiv, MES of Ukraine. – Kyiv, 2024.

The focus of the thesis lies in the study of the information security policy of France within the framework of the transformation of the international relations system, which is increasingly characterised by the growing role of the information technology component as one of the key factors of the state's power and influence in the international arena.

The scientific paper examines the theoretical and methodological aspects of information security, its relationship with the concepts of "soft power", "smart power", and "hybrid war", as well as key features of information security policy at the supranational and national levels.

Specifically, the analysis encompasses the actions of international actors in the realm of information security, notably at the national level, focusing on France, Great Britain, and Germany, and at the supranational level, considering the European Union and the North Atlantic Alliance (NATO). The policies of information subjects are researched at several levels:

- regulatory and conceptual foundations of policies, where key strategic documents, laws, concepts, and decisions regulating the activities of actors in the field of information security are examined;
- institutional structure, where the organisation of the mentioned subjects, key bodies, their work, and the results of this work are examined;
- the role of the society and private sector in the formation and implementation of information security policy;
- concrete examples of the implementation of information security policy, which make clear the peculiarities of the interaction of these policies with the real political environment.

The study of information security policy is particularly focused on addressing information threats and challenges stemming from Russia's hybrid activities against Western nations. Using the method of comparative analysis, the key trends, regularities and specifics of the information security policies of the specified subjects of international relations have been identified.

The focus of the thesis on France's information security policy allowed for a comprehensive and systematic examination of this aspect of French policy, considering its complexity and coherence. Specifically, a detailed examination has been conducted on the regulatory and legal framework that delineates and oversees the information security policy of the French Republic. The institutional structure underpinning this policy has been identified, and the involvement of both the private and public sectors as state

partners in safeguarding society from information age threats has been thoroughly outlined. On the example of specific cases of information challenges encountered by France, the study illustrated the effectiveness of the established information security policy in responding to and mitigating threats.

Furthermore, the study underscores the crucial and effective experiences gained from the implementation of France's information security policy, emphasizing its potential applicability for Ukraine in crafting a comparable policy. This approach makes it possible to evaluate French policy in terms of its practical utility as a template for other nation-states.

The research's scientific novelty is grounded in its thorough analysis of the information security policy of France in modern international relations. The thesis delves into the present-day trends within the theoretical framework and practical implementation of foreign and security endeavours among Europe's leading states. In particular, the issue of information security was considered not from a technical point of view, but taking into account numerous political, socio-economic and international factors. Thus, the information security policy of France was investigated in its relationship with the similar policy of the EU and NATO, its society, in particular, information players such as business and the public, as well as the direction of the information policy of France to counter Russian hybrid threats was highlighted.

The research's scientific novelty is also determined by the fact that the issue of information security is considered as one of the most pressing aspect in ensuring the national security of the French Republic. In this context, particular emphasis is placed on matters pertaining to state regulation within the sphere of information security.

Based on the results of the scientific study, the author's main provisions, which are submitted for defence and contain elements of scientific novelty, are formulated. The main ones are as follows:

for the first time:

- the current information security policy of France underwent thorough examination, encompassing its internal national dimension as well as considering

France's leadership within the EU and Paris's deliberate strategy to enhance its geopolitical role;

- the study systematized the applied dimension of the features and key components of France's information security policy as a set of approaches and practices that can be used by Ukraine to strengthen its information security, particularly in the context of Russia's full-scale aggression. Additionally, the research has emphasized potential areas of collaboration between the two states, which hold promise for Ukraine's advancement in information and technology capabilities;

- the comparative analysis was conducted to examine the information security policies of European leaders – France, Germany, and Great Britain. This method allowed for the identification of key "advantages" and "disadvantages" in the approaches of these countries. Concluding this analysis can contribute to enhancing and improving the information security policy of Ukraine.

the following questions were advanced:

- the examination of France's state policy in the realm of national security, with a particular emphasis on the information component, has enhanced the scientific visualization of such policy. It portrays it as a sophisticated and intricate system, showcasing France's reliance on "smart power" as a pivotal factor in shaping its geopolitical influence.;

- understanding the specifics of the synchronisation of the information security policies of the national EU member actor and directly the European Union as an organisation. On the example of France, the process of parallel coordinated movement of national policies and European strategy is demonstrated;

- analysis of the information security policy of France as a complex system of entities that include both the state and private actors, the public, in particular fact-checking organisations and the media. This made it possible to consider information security as a complex ecosystem.

the following questions were further developed:

- research on information security policy at the supranational and national levels, and it was established that in the conditions of deepening integration within the European

Union, cooperation and maximum coordination of the efforts of national states and supranational institutions is important to effectively counter modern information challenges;

- research on the foreign policy of France, in terms of its information content within the evolving landscape of international relations, notably the rising hybridization of threats focusing on the information and technological aspects, has been explored. The importance is proven rapid adaptation of the private, the state sector and the public to new challenges and information-technological progress as a necessary condition for "survival" in the modern realities of the global information struggle;

- determination of the key components of France's information security policy at the regulatory and institutional levels in the areas of combating disinformation and cyber attacks. Based on this, conclusions are proposed for improving Ukraine's information security policy as one of the necessary conditions for victory over Russia.

The practical significance of the study results lies in their applicability for subsequent scientific investigations, particularly within the context of information security policy and the European integration movement of Ukraine.

Certainly, the results of the thesis can be directly applicable and beneficial to the activities of diplomatic institutions and the Ministry of Foreign Affairs of Ukraine, in particular in the line of cooperation with international organisations, alliances and other partners. They can also become important sources of information for governmental, political and public institutions whose area of responsibility is strategic planning of national security and defence. Thus, the findings of the study hold significant relevance for enhancement of Ukraine's Cyber Security Strategy and Information Security Doctrine.

In addition, the results can be used by Ukrainian media and fact-checking organisations to adopt the experience of France, in particular, the private, the state sector, and the public to improve their work in the fight against disinformation and destructive external information influence.

Keywords: information security, disinformation, cyberspace, hybrid warfare, France, European Union, NATO, Ukraine, Great Britain, Germany, Russia, cyber attack,

national security, mass media, international organisations, international political transformations.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації

Статті у наукових фахових виданнях України,

включених до міжнародних наукометричних баз даних:

1. Фурсай О. В. Система забезпечення інформаційної безпеки Франції / Олександра Володимирівна Фурсай. // Вісник Львівського університету. Серія Філосовсько-політологічні студії – 2021. – №34. – С. 222–227, DOI https://doi.org/10.30970/PPS.2021.34.29

2. Фурсай О. В. Політика інформаційної безпеки Європейського Союзу / Олександра Володимирівна Фурсай. // Літопис Волині. – 2023. – №29. – С. 165–170, DOI https://doi.org/10.32782/2305-9389/2023.29.27

3. Фурсай О. В. Російська дезінформаційна кампанія «Doppelgänger» як новітній виклик інформаційній безпеці держав заходу / Олександра Володимирівна Фурсай. // Філософія та політологія в контексті сучасної культури. –2024. – Том 16 № Спецвипуск. – С. 84-92, DOI https://doi.org/10.15421/352411

4. Фурсай О. В. «Штучний інтелект» як виклик міжнародній інформаційній безпеці / Олександра Володимирівна Фурсай. // Регіональні студії. – 2023. – № 35. – С. 167, DOI https://doi.org/10.32782/2663-6170/2023.35.28

Статті в наукових періодичних виданнях інших держав,

включених до міжнародних наукометричних баз даних:

5. Fursai O. “Vaccinodemic” as a component of the global hybrid conflict between democracy and autocracy: the case of Ukraine / S. Danylenko, O. Fursai. // Rocznik Instytutu Europy Środkowo-Wschodniej. – 2022. – Vol. 20, Iss. 2 – p. 19–45, DOI https://doi.org/10.36874/RIESW.2022.2.2

Опубліковані праці апробаційного характеру:

6. Фурсай О. В. Інфодемія в епоху Covid-19 / Олександра Володимирівна Фурсай. // ІМВ. Міжнародна науково-практична конференція студентів, аспірантів і молодих вчених «Актуальні проблеми міжнародних відносин». – 2021. – С. 120–123.

7. Фурсай О. В. Медіа-агент як базова ланка пропагандистської діяльності терористичних угрупувань / Олександра Володимирівна Фурсай. // ІМВ. Міжнародна науково-практична конференція студентів, аспірантів та молодих вчених «Шевченківська весна». – 2021. – С. 147–149.

8. Фурсай О. В. «Вакцинодемія» як елемент світового гібридного протистояння демократії та автократії / Олександра Володимирівна Фурсай. // ГО «Грузинсько-український експертний центр». Міжнародна науково-практична інтернет-конференція «Сучасні загрози глобальній та регіональній безпеці». – 2023. – С. 115–120.

9. Фурсай О. В. Інформаційна безпека як аспект національної безпеки / Олександра Володимирівна Фурсай. // ІМВ. Міжнародна науково-практична конференція студентів, аспірантів і молодих вчених «Актуальні проблеми міжнародних відносин». – 2023. – С. 143–146.

10. Фурсай О. В. Глобальне інформаційне суспільство: теоретико-методологічні засади концепції / Олександра Володимирівна Фурсай. // The 6th International scientific and practical conference “Current challenges of science and education” MDPC Publishing, Berlin, Germany. – 2024. – С. 339–345.

11. Фурсай О. В. «Doppelgänger»: нова зброя Росії на інформаційному фронті війни проти заходу / Олександра Володимирівна Фурсай. // The 3rd International scientific and practical conference “Science and society: modern trends in a changing world” MDPC Publishing, Vienna, Austria.. – 2024. – С. 252–258.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дисертаційного дослідження визначається зростанням ролі інформаційного простору як одного з полів геополітичного протистояння міжнародних акторів або їх міжнародного співробітництва. Зокрема, стрімка технологізація сучасного життя, зростання ролі нефізичного простору трансформують систему міжнародних відносин з дедалі більшим ухилом до інформаційно-технологічного аспекту. Це стосується і змін в концепції національної безпеки – держави сьогодні роблять ключовий акцент на збільшенні власного інформаційного потенціалу як одного з головних чинників у відстоюванні національних інтересів на міжнародній арені.

Вибір теми дослідження щодо політики інформаційної безпеки Французької Республіки визначається також тим, що світ сьогодні стає все більш інформаційним, ніж це було раніше. Це посилення і призвело до того, що інформаційні «м'язи» можуть тепер діяти самостійно, відірвавшись від фізичної реальності, щоб сіяти дезінформацію. Наразі інформаційному простору не потрібна ніяка зачіпка за фізичне та віртуальне, як це було раніше. Тепер це не тільки властивість релігії, ідеології, літератури, а взагалі всього життя.

Актуальність дослідження проблеми інформаційної безпеки у сучасних міжнародних відносинах, зокрема на національному та наддержавному рівнях, викликає підвищений інтерес багатьох зарубіжних науковців, а саме: Дж. Ная, Р. Армітіджа, А. Чонга, К. Волкера та Д. Людвіга, М. Лібіцкі, Р.Шафранскі, Д. Арквілли і Д. Ронфельдта, Л. Жанчевскі та Е. Коларіка, П. Померанцева, Д. Стейна. Ці дослідники присвятили свої праці вивченню таких концепцій як «м'яка сила», «розумна сила» та ролі інформації в цих наукових концепціях. Окрім цього, вони досліджували феномен інформаційної війни та кібервійни, кібертероризму, а також значну увагу приділяли дослідженню дезінформації, фейків, пропаганди як елементів сучасного інформаційного протиборства. Вагомі результати досліджень та висновки фахівців були враховані в дисертаційній роботі.

Дослідження з інформаційної безпеки мають в Україні послідовний характер. Наукові праці і публікації, зокрема О. Дзьобаня, М. Ожевана, Д. Дубова, О. Курбана, О. Литвиненка, Б. Юськіва, О. Фролової, С. Даниленка, Г. Почепцова, В. Лук'янової та А. Лаутара, П. Біленчука, А. Баровської, О. Добржанської, М. Капітоненка, В. Ліпкана, М. Рижкова, Н. Піпченко, О. Запорожець та ін., розкривають теоретичні та практичні аспекти міжнародного інформаційного протиборства.

На наш погляд, зазначена наукова проблема, зокрема дослідження політики інформаційної безпеки, яка здійснюється на державному рівні, потребує комплексного аналізу з використанням як теоретично-методологічних напрацювань, так і аналізу практичного виміру політики інформаційної безпеки, що реалізується Французькою Республікою. Результати дослідження є важливими в процесі формування, розвитку та реалізації зовнішньої політики України в умовах повномасштабної війни з Росією, яка включає в себе і активне інформаційне та кіберпротиборство. Вважаємо, що дослідження також є важливим в контексті формування і захисту Україною власного інформаційного суверенітету.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація виконана в рамках Комплексної наукової програми Київського національного університету імені Тараса Шевченка «Модернізація суспільного розвитку України в умовах світових процесів глобалізації», затвердженої Вченою Радою Університету, протокол № 13 від 20 червня 2011 року, і науково-дослідної теми Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка «Україна в процесі трансформації світового порядку» (16КФ048-05). У межах зазначеної теми дисертаційна робота відповідає напряму наукової діяльності кафедри міжнародних медіакомунікацій та комунікативних технологій як структурного підрозділу Навчально-наукового інституту міжнародних відносин Київського національного університету імені Тараса Шевченка «Встановлення наслідків реконфігурації співвідношення сил на трансформацію світового порядку».

Мета: визначити сутність, комплексно розглянути та провести аналіз політики інформаційної безпеки Франції як невід'ємного елемента загальноєвропейської архітектури безпеки в умовах міжнародно-політичних трансформацій, зокрема під час російської збройної агресії проти України. Це дасть можливість дослідити роль Франції у побудові загальноєвропейської політики протидії деструктивним зовнішнім впливам, що спрямовані на хаотизацію та руйнування внутрішньополітичних процесів у Європі та єдності Європейського Союзу.

У більш конкретному плані в дисертації поставлено такі дослідницькі **завдання:**

1) окреслити актуальний стан теоретичних та методологічних підходів до вивчення концептів «інформаційне суспільство», «інформаційна безпека», «інформаційна операція»;

2) визначити чинники, що формують французьку внутрішньо- і зовнішньополітичну стратегію в сфері інформаційної безпеки;

3) розкрити сутність загальноєвропейських та євроатлантичних безпекових політик як основи формування політики інформаційної безпеки Французької Республіки;

4) виявити та охарактеризувати інституційні та нормативні засади політики інформаційної безпеки П'ятої Республіки та визначити їх взаємозв'язок з загальноєвропейською політикою інформаційної безпеки;

5) окреслити стратегічний та тактичний виміри розвитку безпекової політики Франції в інформаційній сфері;

6) запропонувати, на основі французького досвіду, шляхи вдосконалення політики України в сфері інформаційної безпеки та залучення комунікативних і інноваційних інструментів для її реалізації.

Згідно із зазначеною метою і завданнями **об'єктом дослідження** є система міжнародних відносин у Європі, зокрема її інформаційна складова як невід'ємний елемент зовнішньої політики держави, а **предметом дослідження** є політика

інформаційної безпеки Франції в умовах міжнародно-політичних трансформацій, насамперед в контексті російської повномасштабної агресії.

Хронологічні рамки дисертаційного дослідження охоплюють період 2017 – 2024 рр., що збігається з часом президентської каденції Е. Макрона.

Методи дослідження. Для вирішення завдань, поставлених у дисертації, використано загальнонаукові та спеціальні методи. Зокрема, **історичний метод** був використаний для аналізу змін технологій політики інформаційної безпеки у контексті зв'язку минулого, сьогодення і майбутнього, змін політики інформаційної безпеки Франції, ЄС, Великої Британії та Німеччини; **структурно-функціональний** метод – для дослідження новітніх технологій впливу як цілісної системи, у рамках якої кожна технологія, яка є її структурним елементом, виконує визначені функції (ролі), що спрямовані на задоволення відповідних потреб політичної системи з урахуванням цілісності останньої та її взаємодії із зовнішнім середовищем; **компаративний** метод – для порівняння політик інформаційної безпеки Франції, ЄС, НАТО, Великої Британії, Німеччини та виокремлення ключових спільних характеристик, а також розробки рекомендацій для їх удосконалення.

Метод системного аналізу був використаний під час розгляду політики інформаційної безпеки Франції в контексті дослідження її нормативних, інституційних складових частин. **Синтез** використовувався для виокремлення ключових характерних рис, закономірностей політики інформаційної безпеки Французької Республіки. **Метод індукції** був застосований для аналізу інформаційної політики Франції, Великої Британії, ЄС та Німеччини шляхом розгляду їх ключових складових. **Метод аналогії** широко застосовувався під час аналізу політики інформаційної безпеки Франції через порівняльну призму політик ЄС, Німеччини та Великої Британії. **Метод івент-аналізу** дав змогу побачити та проаналізувати причини, хід подій та наслідки інформаційного впливу на соціально-політичні події у Франції.

Серед спеціальних методів, використаних у даному дослідженні, слід відзначити **метод групування**. З допомогою нього було згруповано інформацію

про ключові кібератаки та дезінформаційні кампанії, які здійснювала Росія проти Франції, України, Німеччини та Великої Британії. Також було використано **графічний метод** зображення результатів соцопитувань громадської думки та ключових кількісних показників, які характеризують сферу інформаційної безпеки.

Наукова гіпотеза: Франція вибудовує власну національну систему інформаційної безпеки з урахуванням загальноєвропейських інтересів. Франція прагне залишатися ключовим гравцем у визначенні ключових напрямів та інструментів інформаційної безпеки насамперед країн Європейського Союзу.

Наукова новизна дослідження полягає у глибокому аналізі політики інформаційної безпеки Франції у сучасних міжнародних відносинах. Дисертаційна робота розглядає актуальні тенденції теорії та практики зовнішньої та безпекової діяльності на тлі російської загрози на європейському континенті. Зокрема, йдеться про дослідження нормативних та інституційних основ політики інформаційної безпеки Франції в сучасних умовах, розгляд їх у взаємозв'язку з конкретними прикладами загроз та викликів інформаційній безпеці Французької Республіки.

Крім того, наукова новизна полягає в дослідженні питань інформаційної безпеки не з технічного погляду, а з урахуванням численних політичних, соціально-економічних і міжнародних чинників. Так, досліджено як реагувала система інформаційної безпеки Франції в умовах складних політичних процесів, зокрема виборчих та трансформації геополітичного порядку, як ця система адаптується до технологічного прогресу і як вона реагує на російську стратегію гібридної війни.

За результатами дисертаційної роботи сформульовано авторські основні положення, які містять елементи наукової новизни та виносяться на захист. Основними з них є такі:

уперше:

- комплексно досліджено на сучасному етапі політику інформаційної безпеки Франції як у її внутрішньому національному вимірі, так і в контексті лідерства Франції в ЄС та цілеспрямованої стратегії офіційного Парижа з посилення власної геополітичної ролі;

- систематизовано у прикладному вимірі особливості та ключові складові політики інформаційної безпеки Франції як набору підходів та практик, які можуть бути використані Україною для зміцнення власної інформаційної безпеки, зокрема в контексті повномасштабної агресії Росії. Також виділено ті напрями співпраці між двома державами, які можуть бути найбільш перспективними для України щодо посилення свого інформаційно-технологічного потенціалу;

- методом компаративного аналізу проведено порівняння актуальних політик інформаційної безпеки лідерів Європи – Франції, Німеччини та Великої Британії, що дозволило виокремити ключові «плюси» та «мінуси» підходів цих держав, що своєю чергою дозволило зробити необхідні висновки для удосконалення політики інформаційної безпеки України.

удосконалено:

- розуміння державної політики Франції у сфері національної безпеки, зокрема фокус на інформаційній складовій дозволив покращити наукову «візуалізацію» такої політики як складної, комплексної системи, яка опирається на використання Францією «розумної сили» як ключового фактору нарощування власного геополітичного впливу;

- розуміння специфіки синхронізації політик інформаційної безпеки національного актора-члена ЄС та безпосередньо Європейського Союзу як організації. На прикладі Франції продемонстровано процес паралельного скоординованого руху національних політик та європейської стратегії;

- аналіз політики інформаційної безпеки Франції як складної системи суб'єктів, які включають як державу, так і приватних акторів, громадськість, зокрема фактчекінгові організації та ЗМІ. Це дозволило розглянути інформаційну безпеку як комплексну екосистему.

набуло подальшого розвитку:

- дослідження політики інформаційної безпеки на наднаціональному та національному рівнях, і встановлено, що в умовах поглиблення інтеграції всередині Європейського Союзу важливою є співпраця та максимальна

координація зусиль національних держав та наднаціональних інституцій задля ефективної протидії сучасним інформаційним викликам;

- дослідження зовнішньої політики Франції, у частині її інформаційного наповнення, в умовах трансформації системи міжнародних відносин, зокрема зростанням рівня гібридизації загроз з акцентом на інформаційно-технологічну складову. Доведено важливість швидкої адаптації держави, приватного сектору та громадськості до нових викликів та інформаційно-технологічного поступу як необхідної умови «виживання» в сучасних реаліях глобального інформаційного протиборства;

- визначення ключових компонентів політики інформаційної безпеки Франції на нормативно-правовому та інституційному рівнях в сферах протидії дезінформації та кібератакам. На основі цього запропоновано висновки для удосконалення політики інформаційної безпеки України як однієї з необхідних умов перемоги у російсько-українській війні.

Одержані результати можуть знайти своє практичне застосування в наукових дослідженнях сучасної політики інформаційної безпеки. Це дослідження може бути важливим для покращення розуміння процесів глобалізації, впливу інформаційних технологій та розвитку інформаційного суспільства. Розуміння суті операцій впливу та особливостей розвитку медіапростору є ключовим елементом для будівництва стратегічної інформаційної стійкості держави та запобігання реалізації масштабних дезінформаційних кампаній в її інформаційному просторі. Висновки за результатами глибокого вивчення теми є корисною основою для подальших досліджень і можуть бути враховані у діяльності дипломатичних установ та Міністерства закордонних справ України у співпраці з міжнародними організаціями, альянсами та партнерами. Також вони можуть стати важливим джерелом інформації для урядових, політичних та громадських інституцій, зайнятих стратегічним плануванням національної безпеки та оборони, і бути враховані у процесі вдосконалення Стратегії кібербезпеки та Доктрини інформаційної безпеки України.

Окрім цього, результати можуть бути використані українськими медіа та фактчекінговими організаціями для взяття на озброєння досвіду Франції, зокрема держави, приватного сектору, громадськості для удосконалення власної роботи щодо боротьби з дезінформацією.

Апробація результатів дослідження. Основні результати наукового дослідження були висвітлені на міжнародних науково-практичних конференціях. А саме: міжнародній науково-практичній конференції студентів, аспірантів і молодих вчених «Актуальні проблеми міжнародних відносин 2021» (28 жовтня 2021р., м. Київ); міжнародній науково-практичній конференції студентів, аспірантів і молодих вчених «Шевченківська весна 2021» (29 березня 2021р., м. Київ); міжнародній науково-практичній інтернет-конференції «Сучасні загрози глобальній та регіональній безпеці» (29 жовтня 2023 р., м. Одеса); міжнародній науково-практичній конференції студентів, аспірантів і молодих вчених «Актуальні проблеми міжнародних відносин 2023» (1 грудня 2023 р., м. Київ); VI міжнародній науково-практичній конференції *«Current challenges of science and education»* (12-14 лютого 2024 р., м. Берлін, Німеччина); III міжнародній науково-практичній конференції *«Science and society: modern trends in a changing world»* (19-21 лютого 2024 р., м. Відень, Австрія).

Публікації. За результатами дослідження опубліковано 11 наукових праць, а саме: 5 наукових статей, з яких 4 статті – у фахових виданнях України, 1 стаття – в іноземному науковому виданні, 6 публікацій, які додатково відображають наукові результати дисертаційного дослідження.

Структура дисертації. Дисертаційне дослідження складається з переліку умовних скорочень, вступу, трьох розділів та висновків до них, загальних висновків, списку використаних джерел та додатків. Загальний обсяг дисертації – 225 сторінок. Обсяг основного тексту – 162 сторінки. Список використаних джерел включає 333 найменування.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Теоретико-методологічні підходи до вивчення інформаційної безпеки в міжнародній політичній науці

В останні роки інтенсивність генерування та споживання інформації значно зросла у всіх сферах суспільного життя, включаючи науково-технічну, соціальну, політичну та економічну. Процеси збору, накопичення, переробки та розповсюдження інформації наразі максимально інтегровані в роботу практично усіх суб'єктів системи міжнародних відносин, як національних держав, міжнародних інтеграційних утворень, так і бізнесу, громадського сектору, які починають відігравати дедалі більшу роль в міжнародному житті. Ця тенденція має свої ризики, адже інформація володіє потужним дестабілізуючим потенціалом через свої майже необмежені можливості впливу на індивідуумів і суспільство загалом. Дослідження, проведене *World Economic Forum* показує, що світ наразі розцінює дезінформацію, згенеровану «штучним інтелектом» та кібератаки одним із 5-ти глобальних топ-ризиків для світового розвитку. Окрім цього, уже сьогодні світова громадськість називає дезінформацію та незахищеність в кіберпросторі одним з топ-10 глобальних ризиків в короткостроковій та довгостроковій перспективах (див. Додаток А).

Уряди кількох країн, включаючи ЄС, визнають, що фейкові новини стають все більшою загрозою в умовах домінування цифрових платформ та нових медіа. Країни ЄС доходять висновку, що розповсюдження дезінформації може підірвати легітимність нових урядів, спровокувати масові протести та терористичні акції. На думку голови *World Economic Forum* Саадії Заході, стрімкий ріст «синтетичного інтелекту» під час виборчих кампаній може стати справжньою вибуховою сумішшю в інформаційному середовищі (The Global Risks. Report 2024, 2024, с. 7).

Віртуалізація суспільно-політичних відносин безсумнівно стала одним із мегатрендів глобального розвитку, поряд з такими трендами як глобалізація, демократизація, інтеграція, а також, як відзначають науковці, зниження ступеня захищеності людства, віртуалізація суспільно-політичних відносин, криза інституту глобального лідерства, зміна політичної структури світу, універсалізація міграційних потоків, переміщення центру світового розвитку, інверсія фундаментальних цінностей тощо. Своєю чергою такі «інформаційні» мегатренди глобального розвитку як перехід до інформаційного суспільства, кібернетична революція, зростання ролі мережевих структур та інші, здійснюють значний вплив на мегатренди світової політики (Коппель & Пархомчук, 2022, с. 10-15).

Саме тому виникають такі нові концепції як «кібербезпека» та «інформаційна безпека», актуальність дослідження яких тільки зростає (Ісмайлов, 2016, с. 32-33).

Сьогодні інформаційна безпека стає ключовим фактором успішного здійснення зовнішньополітичної стратегії держави та забезпечення безпеки держави від зовнішніх загроз загалом, встановлюючи нові орієнтири її зовнішньополітичної поведінки, трансформуючи звичні критерії оцінки ролі та співвідношення військової могутності та політичних можливостей у реалізації геополітичних інтересів, зіткнення яких перетворює інформаційне протиборство за лідерство в інформаційній війні. У зв'язку з цим інформаційну безпеку тепер розглядають як окремий та ключовий елемент національної безпеки (Войціховський, 2020, с. 281-288).

Що ж до дефініцій поняття «інформаційна безпека», то тут базовим є визначення, встановлене Стратегією інформаційної безпеки України, затвердженої указом Президента України від 28 грудня 2021 року. Вона визначає інформаційну безпеку як «складову частину національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного устрою, інтересів людини та держави, за якого в потрібній мірі забезпечуються права і свободи людини на роботу з інформацією, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, зокрема

скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом». Таке визначення демонструє, що держава розглядає інформаційну безпеку як комплексну систему, де є місце як «технічним» аспектам, зокрема йдеться про захищеність систем, так і «наративним» – коли йдеться про поширення недостовірної інформації (Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки», 2021).

Якщо українська держава розглядає «інформаційну безпеку» як стан, то Європейський Союз акцентує на процесі. Так, Європейське агентство з мережевої та інформаційної безпеки *(ENISA)*, яке є ключовим органом ЄС, відповідальним за інформаційну безпеку організації, визначає «інформаційну безпеку» як захист інформації та інформаційних систем від неавторизованого доступу, використання, розкриття, порушень, модифікації чи знищення, покликаним забезпечити конфіденційність, цілісність та доступність інформації та інформаційних систем. Як ми бачимо, дефініція *ENISA* має більш прикладний характер і зосереджена на конкретних діях («INFOSEC», б. д.). Тому тут важливим є поступова синхронізація тлумачення поняття «інформаційна безпека» в контексті руху України до набуття членства в Європейському Союзі.

Схоже «інформаційну безпеку» трактує і Організація Об’єднаних Націй (ООН). Зокрема, вона визначає таку безпеку як дисципліну ризик-менеджменту, яка стосується захисту конфіденційності, цілісності та доступності інформації, а також систем, які її зберігають, обробляють і передають. Зазначимо, що саме цілісність, конфіденційність та доступність інформації визначаються міжнародною спільнотою, на прикладі ЄС та ООН, як головна ціль інформаційної безпеки, а сама ж інформаційна безпека тлумачиться саме як набір інструментів, засобів захисту (Information Security Policy Directive for the United Nations Secretariat, 2013).

Зауважимо, що аналогічне визначення «інформаційної безпеки» закріплене у законодавстві провідної держави світу – Сполучених Штатів Америки (США), яка теж акцентує на прикладній, практичній сутності цього поняття («Information

security», б. д.). На такому характері «інформаційної безпеки» акцентують і великі приватні інформаційні компанії. Зокрема, одні з найбільших інформаційних компаній світу Microsoft та CISCO прямо визначають «інформаційну безпеку» як набір інструментів та процесів, створених і задіяних для захисту чутливої інформації від модифікацій, її порушень, знищення та відстеження. Окрім цього, компанія виділяє основні типи інформаційної безпеки:

- захист програмного забезпечення, зокрема веб та мобільних додатків, а також інтерфейсів програмування програм. Ця робота передбачає пошук вразливостей, які можуть бути використані хакерами для зламування додатків, та їх усунення (*API*);

- захист «хмар», в яких зберігається інформація. Йдеться про захист віртуального спільного простору, в якому партнери чи співробітники однієї компанії спільно працюють з одними й тими ж цифровими інструментами;

- криптографія, зокрема використання шифрування для захисту інформації. Прикладом такого типу інформаційної безпеки є цифровий підпис, який використовується для авторизованого та конфіденційного входу користувачів до системи;

- інфраструктура інформаційної безпеки включає роботу над захистом внутрішньої та зовнішньої мережі, технічних лабораторій, дата-центрів, серверів;

- реагування на інциденти. Цей тип інформаційної безпеки передбачає моніторинг та відстежування потенційно шкідливих дій, тобто фактично це робота над превенцією небезпечних хакерських дій;

- менеджмент вразливостей передбачає оцінку вразливостей програмного забезпечення та створення ефективного плану їх мінімізації чи усунення ("What Is Information Security?", б. д.).

Попри очевидну «бізнесову» спрямованість визначення та типологізації, а також акцент даного дослідження на «державній» формі «інформаційної безпеки», розуміння погляду приватного сектору на таку безпеку є фундаментальним в сучасних реаліях. Адже сьогоднішня інформаційна безпека держави – це вже не

тільки безпека державних інформаційних систем та безпосередньо інформації, а складна екосистема, яка включає як державу, так і різні сфери суспільства.

Щодо української наукової школи, то науковець В. Гурковський визначає національну інформаційну безпеку в Україні як комплекс соціальних відносин, що стосуються захисту критично важливих інтересів громадян та країни від потенційних та реальних загроз в інформаційному просторі. Ці відносини необхідні для забезпечення захисту і розвитку духовних і матеріальних цінностей нації, а також для прогресивного розвитку України. Цей захист і розвиток визначаються ефективною інформаційною політикою, гарантіями, охороною, обороною і захистом національних інтересів країни (Гурковський, 2004).

Відповідно до визначення В. Лук'янової та А. Лаутара, інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання та розвиток на користь громадян, організацій і держави. Інформаційне середовище, що охоплює сферу діяльності учасників інформаційних відносин, розглядається як комплексна система, яка включає в себе створення і розповсюдження інформації, формування інформаційних ресурсів, споживання інформації, а також забезпечувальні елементи, такі як інформаційні системи та технології, які гарантують недоторканість інформації – інформаційної безпеки (Лук'янова & Лаутар, 2013, с. 97-101).

Своєю чергою П. Біленчук охарактеризував інформаційну безпеку як стан захищеності інформаційного середовища суспільства, спрямований на забезпечення його формування, використання і розвиток в інтересах особи, суспільства і держави. Ця категорія включає різноманітні організаційні, соціально-економічні та правові механізми, спрямовані на підтримку сталого розвитку суспільства і держави.

П. Біленчук вважає, що безпека в інформаційній сфері передбачає низку заходів. А саме:

- забезпечення інформаційного суверенітету;
- удосконалення державного регулювання шляхом створення фінансових і правових умов для вироблення та застосування сучасних технологій;

- забезпечення доступу до публічної інформації;
- розвиток державної інформаційної інфраструктури, і водночас запобігання свавільному втручанню органів влади у функціонування ЗМІ;
- захист національного інфопростору;
- запобігання монополії держави в інформаційній сфері (Біленчук, 2018).

Окремо слід наголосити на важливості розмежування понять «інформаційна безпека» та «комунікативна безпека». Остання розуміється сучасними дослідниками як безпека людини в інформаційну епоху, де технології часто-густо загрожують людині та її психіці. Сьогодні ключовим питанням комунікативної безпеки є захист від дезінформації, яка прагне хаотизувати свідомість споживачів інформації задля створення сприятливого ґрунту для поширення певних наративів.

Саме акцентування на гуманітарному вимірі впливу інформаційного середовища відрізняє поняття «комунікативної безпеки» від поняття «інформаційна безпека», яке має більш технічний «присмак», зокрема базовою складовою якого є поняття «кібербезпека» як захищеність інформаційно-технологічних систем (Даниленко, Нестеряк & Грінчук, 2018, с. 171-187).

Також окремо відзначимо різницю дефініцій «інформаційна безпека» та «кібербезпека». Так, згідно Закону України «Про основні засади забезпечення кібербезпеки України», кібербезпека визначається як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». Важливим для розуміння саме сутності приставки «кібер» є визначення законом об’єктів кіберзахисту – це, зокрема:

- комунікаційні системи органів державної влади та місцевого самоврядування;
- критична інформаційна інфраструктура;
- системи електронного документообігу та урядування.

Тобто, можемо зробити висновок, що законодавство України визначає кібербезпеку все ж більш як опис «технічної» захищеності, де у фокусі самі системи, інфраструктура, програмне забезпечення, в той час як визначення інформаційної безпеки є значно ширшим та акцентоване не тільки на технічній частині, але й на змісті інформації (Про основні засади забезпечення кібербезпеки України, 2017).

Також на «технічній» захищеності акцентує увагу Європейський Союз у своєму визначенні «кібербезпеки». Так, у чинному Акті про кібербезпеку від 2019 року ЄС визначив кібербезпеку як набір заходів, необхідних для захисту мережі та інформаційних систем, користувачів таких систем та інших осіб, які зіткнулися з кіберзагрозами (Papakonstantinou, 2022). Як ми бачимо, ця дефініція є вужчою від вищезазначеного визначення ЄС поняття «інформаційна безпека», що свідчить про спільне розуміння меж понять в Києва та Брюсселя. Зазначимо, що такий підхід контрастує з розмежуванням, яке традиційно використовують великі приватні інформаційні компанії. Зокрема, вони розглядають «кібербезпеку» як ширше поняття, ніж «інформаційна безпека», акцентуючи на тому, що «інформаційна безпека» є виключно описом процесів, створених для захисту даних ("What Is Information Security?", б. д.).

Також важливим є акцентування на понятті «інформаційний суверенітет держави». Попри те, що ця дефініція була встановлена Законом України «Про Національну програму інформатизації» 1998 року, ця категорія вже не згадується в оновленій версії законодавства – Законі України «Про Національну програму інформатизації» від 1 грудня 2022 року. Відповідно до визначення інформаційного суверенітету, це є верховенство держави в інформаційній сфері на своїй території та можливість надавати об'єктивну інформацію про внутрішню та зовнішню політику держави незалежно та безперешкодно. Навіть за умови втрати чинності закону, цей принцип може бути визнаний як ключовий для забезпечення незалежності та ефективного функціонування інформаційної сфери держави. Важливо зазначити, що верховенство держави в інформаційній сфері передбачає регулювання інформаційної діяльності з метою забезпечення безпеки і захисту

інтересів держави, прав та інтересів, життя та здоров'я людини шляхом встановлення законодавчого контролю, умов ліцензування та інших механізмів регулювання такої діяльності (Кононенко, Здоровко & Корольова, 2023, с. 244-250).

Китайський дослідник Венсян Конг визначав «інформаційний суверенітет держави» як верховенство держави у встановленні та реалізації інформаційної політики та інформаційного порядку в державі, забезпеченні правової рівності держав та незалежності від зовнішнього контролю процесів створення та використання інформації (Kong, 2005, с. 119-135). На наш погляд, в сучасних інформаційних реаліях, для яких притаманні всепроникність інформації, хаотичність інформаційних процесів, забезпечити незалежність від зовнішнього контролю, про яку пише Венсян Конг, є надзвичайно складно. Особливо це стосується держав Заходу з їх демократичними, ліберальними моделями розвитку суспільства, де інформаційні процеси не контролюються в такий спосіб, як це притаманно тоталітарним або авторитарним державам.

Конструктивнішим та більш адаптованим до сучасних реалій інформаційної доби є визначення українського дослідника В. Полевого. Зокрема, він визначив «інформаційний компонент національного суверенітету» як право та здатність держави визначати та імплементувати інформаційну політику, гарантувати інформаційну безпеку та діяти як рівний суб’єкт міжнародного інформаційного обміну. Такий «інформаційний суверенітет» має базуватися на законі та брати до уваги баланс інтересів громадян, держави та суспільства (Полевий, 2018, с. 136-144). Інша українська дослідниця О. Солодка розглядає «інформаційний суверенітет держави» як властивість державної влади, що полягає у її верховенстві, самостійності, повноті і неподільності в інформаційному просторі України, рівноправності та незалежності у відносинах з іншими державами у глобальному інформаційному просторі (Солодка, 2020, с. 80-87).

Окремо відзначимо термін «інформаційне суспільство», який є значно ширшим від визначення «інформаційний суверенітет держави» і свідчить про сучасний стан інформаційних відносин та процесів, де ключову роль грають не

тільки держави, але й недержавні суб’єкти. Термін «інформаційне суспільство» був введений науковцем Ю. Хаяші з Токійського технологічного інституту в 1970 році. В першому визначенні, це суспільство, де процес комп'ютеризації забезпечує доступ людства до надійних джерел інформації та сприяє високому рівню автоматизації виробництва. Виробництво інформаційного продукту вважалося каталізатором розвитку освіти та, відповідно, розвитку суспільства (Білоусов, 2013, с. 60-68).

Інший японський науковець Й. Масуда визначив свою концепцію інформаційного суспільства, яке, за його думкою, відрізняється відсутністю класових конфліктів. Він виділяє особливість інформаційного суспільства у часі, що сприяє збільшенню значення культурного дозвілля. За Й. Масудою, інформаційне суспільство сприяє трансформації сутності особистості та виникненню нового типу – від *Homo sapiens* до *Homo intelligens*. В цьому контексті основним видом діяльності для людини стає інтелектуальна сфера (Masuda, 1985, с. 479-494).

Як зазначає С. Даниленко, термін «інформаційне суспільство» передусім є гуманітарною концепцією, яка визначає якісні трансформації в суспільстві. Ці трансформації включають переміщення акцентів з виробничої на невиробничу сферу, зміну характеру інформаційних потоків та еволюцію групових та індивідуальних ідентичностей. Хоча розвиток інформаційно-комунікаційних технологій теж важливий, увага державної політики інформаційно розвинених країн вже тривалий час зосереджується на розробці доктринальних підходів. Ці підходи призначені для відстеження та, за можливості, контролювання суспільних змін, що виникають внаслідок впровадження інформаційних технологій (С. Даниленко, 2013, с. 64-76).

Повертаючись до поняття «інформаційна безпека», слід зазначити, що сутність його феномену значною мірою визначається через призму оцінки інформаційних загроз та ризиків, які вказуються в національних доктринальних документах. У Доктрині інформаційної безпеки України, яка була переглянута у

2017 році, визначено низку реальних загроз національній безпеці України в інформаційній сфері. Серед них:

1) проведення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, сприяння екстремістським проявам, розпалювання панічних настроїв, загострення та дестабілізація суспільно-політичної та соціально-економічної ситуації, а також розпалювання міжетнічних та міжконфесійних конфліктів в Україні;

2) проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою формування негативного іміджу України у світі;

3) інформаційна експансія держави-агресора та підконтрольних їй структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

4) інформаційне домінування держави-агресора на тимчасово окупованих територіях;

5) недостатній розвиток національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії;

6) неефективність державної інформаційної політики, недосконалість законодавства щодо регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу та низький рівень медіакультури суспільства;

7) поширення закликів до радикальних дій, пропаганда федералізму та сепаратизму в Україні (Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», 2017).

Стратегія національної безпеки України актуальні загрози національній безпеці в інформаційній сфері визначає таким чином:

1) розробка систем озброєнь на основі інформаційних технологій;
2) поширення тероризму та злочинності в кіберпросторі;
3) посилення боротьби за світове лідерство між США та Китаєм з використанням інформаційно-психологічних та кіберзасобів;

4) використання Росією інформаційної зброї в рамках стратегії гібридної війни;
5) посилення кіберзагроз в критичній інфраструктурі;
6) відтік фахівців, зокрема в сфері інформаційної безпеки.

Ці аспекти стають ключовими під час формулювання стратегічних заходів для забезпечення національної безпеки в інформаційній сфері (Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України», 2020).

У сучасному політичному і соціально-економічному контексті набуває дедалі більшого значення також проблема наростання протиріч між потребою у розширенні вільного обміну інформацією та важливістю збереження обмежень на її поширення. Розширення соціальної відкритості, інтенсифікація обміну інформацією та широке використання новітніх технологій збору та обробки інформації створюють передумови для можливих порушень щодо інформації та її користувачів. Тому важливо, щоб відкритість інформації супроводжувалася дотриманням прав людини, соціальних і конституційних норм, що стосуються захисту обмеженого доступу до інформації.

У цих умовах кожна держава або група держав формує власну стратегію щодо поведінки в кіберпросторі та розробляє внутрішню та зовнішню політику інформаційної безпеки, яка відповідає сучасним умовам розвитку інформаційно-комунікаційних технологій (ІКТ). Наприклад, в Європі спостерігається пошук балансу між державним інтересом та захистом прав людини та бізнесу від надмірного втручання (Парахонський, 2015).

Виходячи з цього, державна політика інформаційної безпеки повинна бути розглянута як об'єктивна складова національної безпеки, а також як частина загальної політики, що ґрунтується на національних інтересах. Така політика має враховувати баланс між державним контролем і захистом основних прав та свобод громадян. Застосування правових демократичних принципів є ключовим у розробці та впровадженні державної інформаційної політики.

Створення умов для інформаційної діяльності повинно гарантувати дотримання принципів свободи висловлення поглядів і переконань, свободи поширення, обміну та отримання інформації, права на інформацію, відкритості та доступності інформації, достовірності і повноти інформації, а також захищеності особи від втручання в її особисте та сімейне життя. Забезпечення безпеки процесів обміну інформацією має важливе значення для окремої країни та міжнародного співтовариства загалом. Такий підхід дозволяє розглядати інформаційну безпеку як стійкий та безпечний стан всієї соціальної системи, що гарантує ефективне функціонування та розвиток як інформаційної сфери, так і суспільства в цілому (Кононенко, Здоровко & Корольова, 2023, с. 244-250).

Також важливо, щоб ця політика враховувала національне та міжнародне право. Вона має бути реалізована через розробку та впровадження відповідних національних доктрин, стратегій та програм, що відповідають принципам і нормам, закріпленим у національному та міжнародному праві (Бондар, 2014, с. 68-75).

Очевидно, що інформаційна безпека є не тільки складовою національної безпеки, але й безпосереднім базисом міжнародної безпеки. Як ми бачимо, розробка та розширення арсеналу інформаційно-технологічної та інформаційно-психологічної зброї, яку ми можемо спостерігати сьогодні, зумовлює зміни балансу сил в системі міжнародних відносин, а також провокує стан постійного конфлікту держав, створюючи загрози як національній, так і глобальній безпеці.

Перехід до інформаційного суспільства, глобалізація, та швидкий розвиток передових технологій значно вплинули на стратегії ведення війни та зміну системи міжнародної безпеки. Принципи, ресурси і інструменти воєнного конфлікту відчутно трансформувалися. В сучасному світі кібернетичний простір дедалі частіше використовується для проведення різноманітних інформаційних операцій, охоплюючи широкий спектр дій: від крадіжки цінної інформації до актів кібертероризму (Гуржій, 2018, с. 16-26).

Сучасні виклики і загрози для глобальної інформаційної безпеки створили необхідність переосмислення концепцій та практичних підходів до міжнародного співробітництва в сфері інформаційної безпеки. Для забезпечення безпеки і

стабільності у сучасному світі необхідно ухвалити єдині правила, принципи та норми відповідальності. ООН виступає універсальною та унікальною платформою для закріплення позитивних тенденцій у розбудові системи міжнародної інформаційної безпеки.

ООН присвячує свою діяльність розробці міжнародно-правового фундаменту та установленню положень з метою протидії незаконному використанню організованою злочинністю і терористичними угрупуваннями науково-технологічного прогресу. Питання забезпечення інформаційної безпеки у контексті розвитку сталого глобального інформаційного суспільства є наразі важливим і також є складовою частиною роботи низки спеціалізованих установ ООН (Фролова, 2018).

Проблеми міжнародної інформаційної безпеки періодично обговорювалися на Генеральній Асамблеї ООН. Нові міжнародні документи розроблялися на основі резолюцій, зокрема «Роль науки і техніки в контексті міжнародної безпеки і роззброєння» і «Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки». В цих документах висвітлювалися питання використання сучасних технологій як у цивільних, так і у військових сферах, модернізації озброєнь за допомогою досягнень науки і техніки, а також важливість протидії деструктивним інформаційним впливам (Копійка, 2020, с. 102-109).

Згідно з визначенням ООН, «міжнародна інформаційна безпека» є станом міжнародних відносин, який передбачає відсутність порушень світової стабільності та загрози безпеці держав і світовій спільноті в інформаційному просторі (Kavanagh, 2017).

У зв'язку з поширенням інформаційних правопорушень в 2019 році Генеральна Асамблея ООН ухвалила резолюцію під назвою «Заохочення відповідальної поведінки держав в кіберпросторі в контексті міжнародної безпеки». В цьому документі визначається необхідність створення безпечного, відкритого, доступного, стабільного та мирного інформаційно-комунікаційного середовища. Резолюція також закликає до встановлення відповідальних відносин між державами, розширення можливостей урядів для співпраці та просування

сучасних технологій, що сприятимуть зменшенню можливостей активізації конфліктів.

Також важливим кроком в сфері міжнародної інформаційної безпеки є створення під егідою ООН Групи високого рівня з питань загроз, викликів і змін. Ця ініціатива свідчить про бажання спільноти держав ефективно реагувати на сучасні виклики і загрози в інформаційному просторі. Крім того, держави пораховують варіант формування спільного та єдиного координаційного центру ООН з протидії тероризму і комісії щодо світобудівництва. Це свідчить про потребу у комплексному підході до вирішення проблем безпеки та стабільності в світі, враховуючи сучасні тенденції і виклики, пов'язані з інформаційним простором (Кононенко, Здоровко & Корольова, 2023, с. 244-250).

Іншим важливим кроком у розвитку заходів з протидії кіберправопорушенням, але вже на рівні Європи, є Конвенція про кіберзлочинність, прийнята Радою Європи у 2001 році та ратифікована Україною 7 вересня 2005 року. Ця конвенція спрямована на боротьбу з різноманітними кіберзлочинами та визначає стандарти та процедури для міжнародного співробітництва в цій сфері. Зокрема, ця конвенція закріпила на нормативному рівні базові цілі інформаційної безпеки, підтримані міжнародним співтовариством, а саме захисту цілісності, конфіденційності та доступності інформації (*Convention on cybercrime*, 2022; Дубов & Ожеван, 2012).

Слід відзначити, що розвиток і впровадження подібних нормативних актів є важливим етапом в забезпеченні інформаційної безпеки, оскільки вони сприяють координації зусиль країн для протидії кіберзагрозам. Враховуючи постійні технологічні зміни та зростання кількості кіберзлочинів, міжнародне співробітництво у цьому напрямку набуває дедалі більшої актуальності.

На рівні Європейського Союзу політика інформаційної безпеки реалізується заснованим у 2004 році Європейським агентством з мережевої та інформаційної безпеки (*ENISA*). У 2012 році це агентство опублікувало огляд під назвою «Національні стратегії кібербезпеки: Практичний посібник з розвитку та виконання», в якому було відзначено, що в національних стратегіях відсутнє

загальноприйняте та однозначне визначення категорії «кібербезпека» (Довгань, 2017). Окрім цього, в 2013 році в структурі Європола (Європейського поліцейського офісу) був створений Європейський центр боротьби з кіберзлочинністю. Усвідомивши важливість забезпечення цифрової безпеки як невід'ємної складової системи національної безпеки, багато країн світу розпочали впровадження внутрішньодержавних заходів з інформаційної безпеки. Ці заходи включають у себе розробку та вдосконалення національного законодавства в цій сфері, а також створення спеціалізованих органів, відповідальних за безпеку в кіберпросторі (Войціховський, 2020, с. 281-288).

Керуються вони у своїй роботі принципами, закладеними двома основоположними системними стратегіями ЄС в сфері безпеки. Йдеться про прийняту у 2016 році Глобальну стратегію зовнішньої та безпекової політики ЄС, яка визначає фундаментальні цілі, завдання, принципи та цінності цих політик (*A Global Strategy for the European Union's Foreign And Security Policy*, 2016), а також опубліковану в 2020 році Єврокомісією Кіберстратегію ЄС, яка концентрується безпосередньо на політиці захисту ЄС в кіберпросторі (*The EU's Cybersecurity Strategy for the Digital Decade*, 2020).

Особливо важливою є роль інформаційної складової в сучасних гібридних конфліктах, оскільки вона виступає не лише як засіб прикриття, але і як інструмент прямого впливу на супротивника. Наприклад, НАТО вказує на те, що досягнення Росією своїх цілей у Криму в 2014 році було результатом взаємодії різноманітних факторів, таких як дії російського спецназу, активності місцевих збройних груп, економічний тиск, інформаційна війна та розповсюдження дезінформації, а також використання соціально-політичної поляризації (Bilal, 2021).

Так, В. Горбулін вказує, що успіх у гібридній війні залежить від використання комплексу факторів, включаючи стратегії і тактики, інформаційний вплив та своєчасну фізичну реалізацію створеної сприятливої ситуації. Наприклад, незаконна анексія Криму була вдалою завдяки тривалій інформаційній та політичній підготовці, а також влучно обраному моменту для її реалізації. Це включало в себе ослаблення центральної влади, зміни влади, зростання

суперечностей між центром і регіонами, незадовільний стан українських безпекових структур, антагонізм між силовими структурами та активну інформаційно-пропагандистську роботу (Горбулін, 2014, с. 5-12).

Враховуючи вказані особливості сучасної гібридної війни, НАТО активно працює над створенням та розвитком інституцій, які б враховували у своїй роботі реалії сьогодення. Так, Альянс створив у державах-членах такі центри як багатонаціональні інститути для розробки стратегій цифрової безпеки, вдосконалення міждержавної співпраці, впровадження теоретичних розробок у практику протидії цифровим загрозам та для обміну досвідом захисту інформації між країнами-партнерами та країнами-членами. Наразі Центр кібербезпеки НАТО знаходиться в Естонії і не входить до структури збройних формувань НАТО. Його діяльність фінансується державами-спонсорами та членами Північноатлантичного альянсу (Кононенко, Новікова & Копицька, 2021, с. 353-358).

Окремо слід відзначити діяльність Ради Європи, яка зосереджується не на «технічній» складовій інформаційної безпеки, а на гуманітарній компоненті. Зокрема, саме Рада Європи Декларацією про засоби масової інформації та права людини від 1970 року створила одну із базових фундаментальних рамок для роботи медіа як засобу інформування населення. Зокрема, одним із базових принципів Декларації є повага до приватності осіб, яка повинна забезпечуватися шляхом мінімізації державою обсягів приватної інформації для збору в бази даних, а ті обсяги, які все ж збираються, повинні бути захищені від незаконного поширення.

Окрім цього, в сучасній системі міжнародних відносин Рада Європи відіграє важливу роль контролера законодавчих ініціатив в інформаційній сфері, які продукуються державами-членами Європи, роботи їх внутрішніх інституцій, відповідальних за інформацію та права людини. Часто саме моніторингова робота організації дозволяє запобігти прийняттю нормативно-правових актів, які погіршують інформаційну захищеність громадян або сприяють непропорційному використанню персональних даних поставленим законним цілям тієї чи іншої держави. Це дозволяє нам говорити про важливу роль Ради Європи як наглядача за

нормативним виміром забезпечення інформаційної безпеки та свободи в Європі (Danylenko & Shustenko, 2020, с. 133-146).

Організація з безпеки та співробітництва в Європі (ОБСЄ) відіграє важливу роль у зміцненні кібербезпеки та безпеки інформаційно-комунікаційних технологій, сприяючи зниженню ризиків виникнення конфліктів між державами через використання інформаційних технологій. Організація фокусується на тому, щоб регіональні групи урядових експертів реалізовували відповідні директиви ООН. Ключовим аспектом є практична реалізація директив та спільних підходів до кібербезпеки. У 2011 році в Австрії відбулася конференція «Загальний підхід до кібербезпеки: визначення майбутньої ролі ОБСЄ», яка була спрямована на розробку спільного підходу організації до проблем кібербезпеки. У 2013 році ОБСЄ прийняла інноваційні рекомендації щодо зміцнення довіри в сфері кібербезпеки. Ці рекомендації передбачали взаємодію з приватними компаніями та провайдерами інфраструктури, спрямовану на підвищення прозорості та забезпечення безпеки в регіоні, а також розвиток спільних підходів до управління кібербезпекою («Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States», 2023).

Необхідно зазначити, що надійність та безпека інформаційно-телекомунікаційних мереж та інформаційних систем безпосередньо визначають сталий розвиток країн та їх національну безпеку. Очевидно, що роль інформаційної безпеки та її статус у системі національної безпеки також визначаються тісною взаємодією національної інформаційної політики та політики забезпечення національної безпеки через систему інформаційної безпеки. Це є важливою ланкою, яка об'єднує всі основні компоненти національної політики в єдину систему.

Проте, не тільки національним та міжнародним рівнями характеризуються сучасні інформаційні процеси. Запровадження новітніх інформаційно-комунікаційних технологій (ІКТ) створює нову ситуацію в соціальній комунікації та міжнародних відносинах. Зв'язок, комп'ютеризація та інші технології значно прискорили потоки інформації, своєю чергою прискоривши сучасний спосіб життя.

Впровадження ІКТ дозволяє говорити про формування єдиного глобального простору та часу, що стає головною ознакою глобального інформаційного суспільства (Бебик, Шергін & Дегтерьова, 2006).

Впровадження мультимедійних ІКТ призвело до створення інформаційних супермагістралей, що представляють собою інтегральні комплекси глобальних, міжнародних, національних і локальних мереж супутникової, кабельної та наземної комунікації, які базуються на елементах та ресурсах інформаційної інфраструктури. До складу цієї інфраструктури входять комп'ютери з мультимедійними додатками, бази даних, відеоігри, стільниковий зв'язок, програмування тощо.

Інформатизація стає домінуючою характеристикою сучасності. Відповідно, рівень розвитку суспільства визначається сьогодні рівнем процесів інформатизації. Між розвиненим світом і світом, що розвивається, утворюється «цифровий розрив». Таким чином, політичне лідерство у світі передбачає також інформаційне лідерство, лідерство в інформаційних технологіях. Як правило, багато авторів зазначають, що сьогодні інформація та інформаційні технології виступають у ролі важливої складової – «сукупної могутності» держави. За Г. Моргентау, світова політика є боротьбою за владу (Morgenthau, 1948). Показниками інформаційної сили держави є наявність/відсутність на її території великих баз даних (зберігання інформації), суперкомп'ютерів (обробка даних), а також кореневих серверів та доступу до широкосмугового Інтернету (передача інформації).

Водночас Інтернет не є незалежним агентом змін, який визначає ключові характеристики сучасного суспільства та світової політики. Як і будь-яка інша технологія, Інтернет вписаний у ширший соціальний, політичний, економічний контекст і чутливий до процесів, що відбуваються на суспільному та міжнародному рівнях. У сфері міжнародної політики вплив інформаційної глобалізації може бути систематизовано так:

- зростає значимість інформації та знань, унаслідок чого економічний розвиток більшою мірою, ніж раніше, залежить від ідей та знань, а держави, на

території яких розташовані центри інновацій та високотехнологічних виробництв, посилюють свій вплив на міжнародній арені;

- розмиваються кордони між міжнародною та внутрішньою політикою, між військовою та цивільною сферами, міждержавні кордони стають більш чіткими, що сприяє «розмиванню» державного суверенітету, проте сильні держави зберігають потенціал впливу у глобальній інформаційній сфері;

- розвивається «дифузія влади» у світовій політиці, внаслідок чого недержавні актори (зокрема бізнес-компанії, неурядові організації, дослідницькі інституції, а також окремі люди) стають частиною міжнародних відносин;

- стискаються час та простір – в умовах глобальної інформатизації зміни, включно з міжнародно-політичними процесами, розвиваються швидше, і ними складно керувати;

- змінюється природа влади у світовій політиці, відбувається розширення публічної сфери, формуються транснаціональні рухи, організовані за мережевою ознакою, контроль за інформацією, знаннями, віруваннями та ідеями починає розглядатися як важливий компонент контролю над матеріальними ресурсами: ІКТ дозволяють накопичувати інформацію та трансформувати її у знання, що є ресурсом влади;

- в умовах відсутності загальноприйнятих правил взаємодії запускаються національні, а не міжнародні ініціативи, що створює або ж загострює ризики та загрози для міжнародної інформаційної безпеки.

На думку дослідника В. Бебика, формування глобального інформаційного суспільства створює об'єктивні передумови для розбудови глобальної держави та глобального громадянського суспільства. Ці структури дедалі більше впливають на розвиток національних держав, національних моделей громадянського суспільства та національних систем соціальної комунікації. Сучасні реалії інформаційно-комунікаційного світу вимагають посилення боротьби держав-націй та національних громадянських структур проти авторитарних тенденцій глобальної держави і глобального уряду. У зв’язку з чим постає важливе питання – як

забезпечити ефективний захист національної соціокультурної системи, зокрема національної системи соціальних комунікацій (Бебик, 2011, с. 41-49).

Як ми бачимо, сучасні інформаційні відносини, зокрема їх безпекова складова, є об'єктом розгляду на 3-х базових рівнях: національному, міжнародному та глобальному. Такий підхід свідчить про фундаментальну значимість інформаційної компоненти в сучасних міжнародних відносинах, яка сьогодні не тільки є однією з ключових характерних рис світової політики, але й є її системоутворюючим чинником.

1.2. Стан розробки наукової проблеми та джерельно-документальна база дослідження

Сучасна цифрова революція торкається всіх сфер життя суспільства і держави. Система міжнародних відносин стає цифровою, причому у ній формуються різні кластери чи підсистеми, серед яких – система відносин з питань забезпечення інформаційної безпеки (Brooke, 2016, с. 29-53).

Можна погодитись з тим, що цифрові технології для сучасних міжнародних відносин відіграють ту саму роль, що й ядерні технології для другої половини XX століття. Цифровий простір є полем геополітичних протиріч, тому доступ до передових цифрових технологій визначає можливості держави на міжнародній арені і спектр доступних зовнішньополітичних можливостей, а також рівень економічного розвитку. При цьому, як зазначають дослідники, лідерство у галузі цифрових технологій є запорукою лідерства у світовій політиці XXI століття (Cahyadi & Magda, 2021).

Сучасні міжнародні відносини перейшли в епоху, коли взаємодію між країнами, проксі-групами чи користувачами у кіберпросторі необхідно регулювати цифровими правилами на кшталт Ялтинсько-Потсдамських угод та проведення певних меж у використанні Інтернету.

Насамперед, такі правила потрібні для забезпечення стабільного розвитку інформаційного середовища, що особливо затребуване в сучасних умовах

зростання кількості та масштабів цифрових загроз, більша частина з яких має транскордонний характер. Найбільшу небезпеку сьогодні представляє військово-політичний вимір загроз інформаційній безпеці. Стала очевидною «гонка цифрових озброєнь», до якої залучається дедалі більше держав. Події, що відбуваються сьогодні у світі, свідчать про тенденцію посилення інформаційного протистояння між провідними державами. Держави все частіше використовують ІКТ як засоби деструктивного впливу на інформаційну інфраструктуру та суспільну свідомість противника. Особливу небезпеку становлять атаки на об'єкти критичної інформаційної інфраструктури (Palma, 2024).

На сьогодні інтенсивність інформаційного протистояння досягла пікових значень у всьому світі, а особливо після початку російсько-української війни. Саме Росія є одним із світових лідерів з деструктивного використання інформаційних технологій для впливу на інших суб’єктів міжнародних відносин (Paul & Matthews, 2016; *The Kremlin’s Efforts to Covertly Spread Disinformation in Latin America*, 2023; Kayali & Calcutt, 2023).

Потенціал цифрових технологій також дедалі активніше застосовується терористичними та екстремістськими організаціями, злочинцями та іншими зловмисниками для досягнення своїх протиправних цілей. Особливого розмаху набуло шахрайство з використанням ІКТ, з якими стикається більшість користувачів мобільного зв'язку та мережі Інтернет. Ці погрози також мають транскордонний характер і зачіпають усі держави (*Cybersecurity and New Technologies*, 2023).

Сучасна система міжнародних відносин перебуває у триваючому процесі геополітичних, політичних, економічних та соціальних трансформацій, які характеризуються загостреною конфліктністю, хаотизацією системи міжнародних відносин, збільшенням ролі недержавних суб’єктів та проксі-акторів, руйнуванням системи міжнародного права як регулюючого інструменту в міжнародних відносинах, а також все активнішим використанням «розумної сили» як комбінації «м’якої» та «жорсткої» сил. Сьогодні на прикладі агресії Росії проти України чітко простежується крах системи глобальної та європейської безпеки, сформованої

після Другої світової війни. Порушення Росією базових норм та принципів міжнародного права, зокрема Статуту ООН, Гельсінського заключного акту, в поєднанні з можливістю Росією штучно блокувати міжнародні механізми реагування шляхом використання права вето в Раді безпеки ООН, свідчать про потребу переосмислення сучасної міжнародної системи безпеки. Адже наявна система, сформована майже 100 років тому, уже не дає відповіді на існуючі виклики, а контури нової системи все ще не сформовані (Horbulin, 2017).

Сьогодні ми можемо спостерігати трьохскладову трансформацію сучасної політичної організації світу, яка включає трансформацію:

- Вестфальської моделі, обумовлену глобалізацією;
- сучасної міжнародної системи, обумовлену процесами інтеграції/дезінтеграції;
- політичних систем окремих країн, обумовлену демократизацією (Коппель & Пархомчук, 2022, с. 10-15).

Також для системи міжнародних відносин в процесі її трансформації дедалі більш характерною стає гібридизація відносин, зміщення їх в напрямку асиметрії, що знаходить своє найяскравіше відображення у сучасному феномені «гібридної війни» як нового виду глобального протистояння. Саме сучасне розуміння цього феномену найкраще, на нашу думку, відображене у визначенні Міжнародного інституту стратегічних досліджень, опублікованого в звіті *Military Balance* від 2015 року. Проаналізувавши події 2014 року, а саме незаконну анексію Росією півострова Крим та вторгнення у східні області України, аналітики визначили «гібридну війну» як «використання військових та невійськових засобів в інтегрованій кампанії, що створені з метою «здивування» противника, захоплення ініціативи і отримання психологічної та фізичної переваги шляхом використання засобів дипломатії, проведення складних і швидких інформаційних та кібероперацій, військових і спеціальних операцій, а також економічного тиску» (Witner, 2020, с. 7-15).

Цікавим також є визначення «гібридної війни», запропоноване Північноатлантичним альянсом на основі аналізу дій Росії в Україні з 2014 року.

Так, НАТО визначає «гібридну війну» як використання військових та не військових, прихованих та відкритих засобів (зокрема, дезінформацію, кібератаки, економічний тиск тощо) для розмиття кордонів між війною і миром, породження сумніву в свідомості цільових груп населення, дестабілізації і підриву суспільної системи. Виходячи з цього розуміння «гібридної війни», НАТО також деталізує саме інформаційні аспекти такої стратегії. Серед них особливо цікавим є поняття «ворожої інформаційної діяльності» як широкий спектр скоординованих дій, направлених на сіяння недовіри і маніпуляцію громадською думкою. До таких дій відносяться дезінформація, пропаганда, маніпулювання на рівні наративів, соціальний інжиніринг тощо (*NATO's approach to countering disinformation*, 2023).

Дослідник з Норвегії Г. Х. Карлсен провів аналіз щорічних звітів 15 спецслужб у 11 західних країнах за період 2014-2018 років та виявив широкий спектр інструментів та методів, які використовує російський режим для політико-інформаційного впливу. Результати дослідження вказують на те, що Росія намагається найактивніше впливати на європейську політику та процеси прийняття рішень, перевершуючи навіть Китай та інші країни. Дії Росії націлені на три стратегічні цілі: забезпечення безпеки свого режиму, утримання впливу в колишніх радянських республіках та збереження статусу світової держави.

Довгострокова мета підривної діяльності Росії полягає у послабленні НАТО та ЄС. Кремль використовує підхід *«divide et impera»*, використовуючи різні інструменти впливу. Населення основним чином охоплюється через традиційні медіа та соціальні мережі. Меншини, біженці та екстремісти використовуються для створення соціального напруження. У своїх зусиллях Росія використовує розгалужену мережу політичних союзників та громадських організацій, які спотворюють реальність та допомагають переписати історію для легітимізації свого режиму та дискредитації інших країн (Karlsen, 2019).

Сьогодні на прикладі війни України та Росії як безпосередньо конфлікту двох держав, так і елементу геополітичного протистояння держав Заходу зі східними автократіями, ми можемо чітко простежити ключові особливості сучасної «гібридної війни». Серед таких особливостей слід відмітити максимально широкий

арсенал інструментів та методів, які охоплюють політичну, економічну, військову, культурну, інформаційну, технологічну та інші площини. Наразі держави та недержавні суб'єкти намагаються відстояти власні інтереси, досягнути поставлених цілей на міжнародній арені, шукаючи найкращу комбінацію різнопланових заходів, починаючи від безпосередньо військових дій, економічних акцій, завершуючи кібератаками та кампаніями дезінформації. Фактично ми можемо говорити про «гібридну війну» як концепцію, максимально взаємопов'язану з концепцією «розумної сили», для якої гібридний формат протистояння є ідеальним середовищем для реалізації (Kofman & Rojansky, 2015).

Одним із ключових засобів, який використовується сьогодні в рамках гібридних протистоянь, є інформація. Причиною є прискорення технологізації сучасного світового суспільства, збільшення ролі комунікацій, зокрема мережі Інтернет, та здатність інформації бути елементом, який найкраще проникає в середовище противника. Для розуміння, згідно дослідження *Telecommunication Development Sector (ITU-D)*, станом на 2023 рік користувачами Інтернету є 5,4 млрд. людей, що становить 67% всього населення світу. У 2005 році частка користувачів глобальної мережі становила 16% (див. Додаток Б) («Statistics», б. д.). Глобалізація світу, зменшення бар'єрів у взаємодії людей, держав, бізнесу, та переважання ліберальних підходів до регулювання інфопростору в державах Заходу створили ідеальні умови «незахищеності» західних національних інформаційних систем, чим користуються світові автократії, такі як Росія та Китай.

Зокрема, Росія, чиє суспільство є значно закритішим, ніж суспільство Заходу, під час війни з Україною активно використовує цю «відкритість» західного простору для проведення власних дезінформаційних кампаній. Фактично війна України та Росії наразі демонструє вразливість «інформаційно відкритих суспільств» в умовах повноцінного конфлікту. Водночас «інформаційно закрите суспільство», яким є російське, менш чутливе до ворожих інформаційних кампаній, адже використовує низку обмежувальних заходів, таких як цензура, використання фаєрволу для блокування інформації, посилення стеження за власним інфопростором (W. Kong & Marler, 2022).

Зазначимо, що західна модель демократії, яка сприймається Росією як чутлива до впливу, сама опинилася в ситуації трансформації під впливом інформаційної доби, зокрема появи нових медіа. Триває процес формування демократій, орієнтованих на комунікацію та віртуалізацію політичного простору та діяльності громадянина, а міжнародна арена стала полем інформаційної боротьби за демократію. За таких умов залишається відкритим питання, наскільки в такій демократії громадянин якісно поінформований, щоб приймати свідомі та конструктивні рішення в демократичному процесі своєї держави, що своєю чергою актуалізує потребу покращення інформаційної грамотності громадян (Даниленко, 2021, с. 90-105). Очевидно, що такі трансформації демократії та важливість «озброєння» людей якісними навиками для боротьби з дезінформацією у своїй голові ще більше актуалізуються, коли Росія системно тестує інформаційну безпеку Заходу своєю стратегією гібридної війни.

Також важливим для розуміння місця інформаційної складової в контексті сучасних гібридних загроз є усвідомлення збільшення ролі соцмереж як простору протистояння. Розвиток технологій маніпуляції, зокрема йдеться про створення фейкових сторінок, функціонування мережі «ботів» та «тролів», дозволяє державам та недержавним акторам сіяти інформаційний хаос, спрямовувати громадську думку у вигідному для них напрямку. В умовах демократичних ліберальних суспільств це створює безпосередню загрозу дестабілізації політико-соціальної ситуації та потенційно зміни конфігурації влади (Nissen, 2016).

Одним із ключових інструментів для маніпулювання в інфопросторі традиційно є дезінформація, під якою ми розуміємо оманливу або недостовірну інформацію, яка поширена цілеспрямовано з метою маніпулювання думкою і діями інших людей (*NATO's approach to countering disinformation*, 2023). Зокрема, важливою характеристикою такої дезінформації є її інституціональність, тобто дезінформація, яка виробляється і поширюється на замовлення російської держави. С. Даниленко у роботі «Інституціональність дезінформації та симетрична протидія її деструктивному впливу» підкреслює, що особливістю дезінформації є її гнучкість. На думку дослідника, держава-інформаційний агресор оперативно

перенаправляє свою пропаганду, зокрема змінює теми та меседжі, водночас зберігаючи основний наратив, що також створює додаткові загрози для інформаційної безпеки (Сергій Даниленко, 2020, с. 17-19). Така здатність дезінформації ускладнює процес її ідентифікації, зокрема її ключового наративу, а отже ускладнює процес формування інституціональної протидії.

Очевидно, що у цих обставинах на перший план виходить поняття інформаційної безпеки як запобіжника від інформаційного шкідливого втручання. Встановлення цього запобіжника можливе тільки через реалізацію комплексної політики інформаційної безпеки. Варто підкреслити, що основні теорії щодо політики інформаційної безпеки у міжнародних відносинах висвітлено у працях Дж. Ная, Р. Армітіджа, Д. Галларотті, А. Чонга, К. Волкера та Д. Людвіга, М. Лібіцкі, Р. Шафранскі, Д. Арквілли і Д. Ронфельдта, Л. Жанчевскі та Е. Коларіка, П. Померанцева, Д. Стейна, Ю. Марзукі та О. Ульє.

Так, Дж. Най першим ввів в науковий обіг поняття «м'якої сили», яка включає в себе також інформаційні аспекти впливу на суб'єктів міжнародних відносин. На думку науковця, «м'яка сила» фактично означає здатність, потенціал держави досягати своїх цілей у взаємодії з іншими суб'єктами міжнародних відносин не шляхом «жорсткої сили», зокрема військових дій, економічних санкцій тощо, а шляхом переконування. На прикладі США та їх геополітичного розвитку після закінчення Холодної війни Дж. Най демонструє, що «м'яка сила» в умовах руйнування біполярної «жорсткої» системи є ефективним інструментом для США у захисті своїх національних інтересів та поширення свого впливу (Nye, 1991).

На думку науковця, США в процесі забезпечення своїх геополітичних інтересів необхідно впровадити так звану «інформаційну парасолю», яка полягатиме в узгодженому обміні інформацією для налагодження міжнародної співпраці і підтримки миру. Інформаційно-технологічна перевага США, на переконання Дж. Ная, дозволить створити ефективну глобальну демократичну систему, в якій Вашингтон виступить лідером і де США зможуть використовувати інформацію для допомоги союзникам, попередження міжнародних конфліктів, які не відповідають інтересам Америки (Nye, 2004).

Сучасний розвиток мережі Інтернет та передових технологій призвів до виникнення нового цифрового середовища, у якому цифрова дипломатія стає необхідним інструментом для здійснення міжнародних відносин за допомогою інформаційних технологій. Зараз спілкування в мас-медіа та в інтернет-просторі стало звичайним явищем для сучасного населення, що робить особливо актуальним використання нових технологій у дипломатичних практиках. У світі інформаційного впливу «м'яка сила» вважається ключовим елементом у міжнародному контексті. Вона базується на комунікативних можливостях та відрізняється від «жорсткої сили», що включає в себе військову чи економічну потужність. Стратегія «м'якої сили» використовує ресурси Інтернету, а цифрова дипломатія успішно застосовує «м'яку силу» через соціальні мережі як потужний інструмент комунікації з цільовою аудиторією – соціальні медіа як інструмент «м'якої сили 2.0» (Háberová, 2019; Dzitac, 2023).

Соціальні мережі виступають як платформа для будівництва соціальних відносин, впливаючи на розвиток глобальної спільноти та формуючи смаки та пріоритети. Однак, важливо враховувати й негативні тенденції у розвитку глобальних технологій, зокрема у мережі. Виникнення інформаційних та мережевих конфліктів спричинене поширенням недостовірної, низької якості чи умисно неправдивої інформації. У цьому контексті цифрова дипломатія може бути використана для полегшення комунікації між урядом та громадянами, використовуючи ІКТ, медіаплатформи, блоги та соціальні мережі.

Загалом джерела «м’якої сили» можна умовно поділити на 2 види: міжнародні та внутрішні. Міжнародними джерелами такої сили є:

- повага до міжнародного права, інституцій, міжнародних договорів та зобов’язань в рамках альянсів;
- акцент на мультилатералізмі;
- готовність пожертвувати короткостроковими національними інтересами задля досягнення загального блага;
- ліберальна спрямованість зовнішньоекономічної політики.

Що ж до внутрішніх джерел, то тут йдеться про:

- культуру (привабливий образ життя, свобода, толерантність, можливості для самореалізації тощо);
- політичні інституції (демократія, конституціоналізм, плюралізм/лібералізм, ефективно функціонуюча державна бюрократія (Gallarotti, 2015, с. 245-281).

Водночас Дж. Най наголошував, що використанням виключно «м'якої сили» неможливо досягнути усіх цілей зовнішньої політики США. Тому критичною є комбінація «м'якої» та «жорсткої» сил, симбіоз найкращих елементів яких науковець визначав як «розумну силу». Вона має опиратися на найкращі надбання сучасності, зокрема інноваційно-технологічний та науково-освітній потенціали, інноваційну дипломатію і високі технології у військовій справі. В дослідженні Американського центру стратегічних і міжнародних досліджень «Більш розумна, більш безпечна Америка» (2006), підготовленого Дж. Наєм, Р. Армітіджем, наголошено, що необхідність використання «розумної сили» є наслідком вичерпання потенціалу політики, яка опирається виключно на «м'яку» чи «жорстку» сили. На думку дослідників, вдале поєднання найкращих підходів та практик обох концепцій дозволить США повернути собі статус глобального інтелектуального лідера (Nye, Cohen & Armitage, 2007).

Проте, Дж. Най та Р. Армітідж наголошували, що практичне втілення владою Сполучених Штатів Америки концепції «розумної сили» має низку проблем, серед яких проблеми кооперації з неурядовими суб'єктами міжнародних відносин, зосередження фінансування на тих напрямках, які дають швидкий результат, чого часто неможливо досягнути методами «розумної сили», недостатній рівень військово-цивільного співробітництва, розпилення ресурсів «м'якої сили» на багатосторонні та неурядові формати тощо (Nye & Armitage, 2007).

Важливий внесок у розвиток концепції «розумної сили» вніс науковець А. Чонг. Він стверджує, що попри те, що «розумна сила» є своєрідним симбіозом «жорсткої» та «м'якої» сил, вона все ж має тяжіти до дипломатії та мирних способів досягнення своїх зовнішньополітичних цілей. Військовий фактор може бути ключовим тільки тоді, коли всі інші інструменти та методи вичерпали себе і не

залишається іншого вибору, крім використання військової компоненти (Chong, 2015, с. 233-244).

Також слід розглянути науковий доробок дослідника Д. Галларотті, який значну увагу приділяв дослідженню феномену «розумної сили». Зокрема, в роботі «Космополітична сила в міжнародних відносинах»: синтез реалізму, неолібералізму та конструктивізму» він наголошував, що умовою ефективної зовнішньополітичної стратегії держави має бути поєднання 3 складових:

1) м'яке розширення прав та можливостей (потреба у збільшенні впливу держави через підвищення рівня використання «м'якої сили», зокрема шляхом збільшення використання інформації як засобу впливу);
2) жорстке обмеження (з умовою уникнення надмірного покладання надій на «жорстку силу», що в підсумку призводить до негативних наслідків для того, хто її використовує);
3) збалансована комбінація «м'якої сили» та «жорсткої сили» (Gallarotti, 2010).

Цікавим є науковий внесок американських дослідників К. Волкера та Д. Людвіга, зокрема запропонована ними концепція «гострої сили» як своєрідного авторитарного антипода «розумної сили». Ця концепція, продемонстрована науковцями на прикладі Китаю, передбачає, що геополітичні інтереси забезпечуються шляхом використання маніпуляцій, дезінформації, точкових інформаційних операцій (Walker, Kalathil & Ludwig, 2018). Як ми бачимо на прикладі таких держав як Китай, Росія, Іран та КНДР, на сьогодні концепція «гострої сили» активно використовується авторитарними та тоталітарними державами і уже є безпосередньою загрозою глобальній безпеці.

Що ж до безпосередньо інформаційного аспекту, зокрема понять інформаційної безпеки, політики інформаційної безпеки, інформаційних війн, то слід виокремити наукову думку М. Лібіцкі. Зокрема, у дослідженні «Що таке інформаційна війна?» (1995) він виділив основні параметри інформаційної війни, такі як інформаційно розвідувальні операції, електронна та психологічна боротьба, хакерські й кібератаки, мережеве протиборство та інформаційний тероризм (Libicki, 1995). Розвинув теорію інформаційних війн дослідник Р. Шафранскі, який

визначив цілі інформаційних війн на стратегічному та оперативному рівнях. У першому випадку йдеться про вплив на систему прийняття рішень противника, у другому – створення перешкод для противника, зокрема порушення координації, зниження ефективності його дій. Також Р. Шафранскі наголошував, що інформаційна війна за своєю природою є надзвичайно складною, адже у ній розмите поняття комбатантів, ворогуючих сторін, засобів ураження, що робить інформаційну війну надзвичайно складним концептом для систематизації (Szafranski, 1995).

Дослідники О. Фрідман, В. Кабернік, Дж. Піерс у своїй праці «Гібридні конфлікти й інформаційна війна: нові ярлики, стара політика» акцентують на важливості контролю за поширенням інформації в умовах масштабного використання інформаційного простору для здійснення гібридних атак. Науковці наголосили, що попри те, що явища дезінформації та пропаганди не є новими для світової спільноти і історія їх використання сягає тисяч років, проте сучасний розвиток інформаційних технологій дозволяє акторам міжнародних відносин поширювати неправдиву інформацію значно швидше і зі значно більшим охопленням споживачів такої інформації. Це наочно демонструється в праці на прикладі стратегії гібридної війни Росії та діяльності «Ісламської держави», які використовують інфопростір як для просування власних інтересів та наративів, так і для вербування лояльних до себе осіб (Friedman, 2019).

Безпосередньо кіберпростір як один з вимірів інформаційної війни досліджували американські науковці Д. Арквілла і Д. Ронфельдт. Вони визначили кібервійну як військову операцію, що ведеться відповідно до інформаційних принципів. Її ціль – руйнування інформаційних мереж та контроль за потоками інформації. Водночас вони диференціювали поняття «кібервійна» та «мережева війна», останню з яких Д. Арквілла і Д. Ронфельдт визначали як спроби модифікувати з допомогою інформаційних, політичних, культурних та кіберзасобів систему знань населення супротивника про свою ідентичність та значення в світі. Фактично «мережева війна», за визначенням науковців, є ширшим поняттям, ніж

«кібервійна», яка є тільки одним із елементів сучасних війн (Arquilla & Ronfeldt, 1997, с. 24-60).

Цікавим у контексті кібервійни та використання кіберпростору для ведення спеціальних операцій є праця «Кібервійна та Кібертероризм» Л. Жанчевскі та Е. Коларіка. Науковці дослідили феномен кібертероризму як політично мотивованих атак проти інформаційних систем та баз даних. Вони наголошують, що жертвою таких атак переважно є цивільне населення (Janczewski & Colarik, 2008). Слід зазначити, що сьогодні концепція кібертероризму є надзвичайно актуальною, адже цей інструмент наразі масово використовується державними акторами, хакерськими групами, кримінальним світом як в корисливих цілях власного збагачення, так і для відстоювання національних інтересів, дестабілізації ситуації в цільовій державі.

Важливим є науково-публіцистичний доробок П. Померанцева, який у своїй праці «Це не пропаганда. Подорож на війну проти реальності» дослідив різні інструменти, методи, прийоми та тактики інформаційного маніпулювання масовою свідомістю як аспекти сучасної інформаційної війни між державами та війни держави проти власного населення. Автор сконцентрував свою увагу на феномені пропаганди та того, як вона стала повноцінною індустрією авторитарних держав. Так, з допомогою фейків, дезінформації, інформаційно-психологічних операцій, кібератак, «фабрик троллів» сучасні авторитарні держави отримали можливість ефективно поширювати власні наративи як у власному інфопросторі, так і в інфопросторі сусідніх держав. Створення потрібного образу реальності дозволяє таким державам сформувати необхідні умови для наступних військових, політико-економічних дій (Померанцев, 2020).

Важливим в контексті дослідження дезінформації є наукові праці Д. Стейна, в яких він зосереджувався на вивченні когнітивних війн. Їх мета, згідно Д. Стейна, полягає у впливі на людей, які приймають ключові рішення в державі шляхом забезпечення такої людини дезінформацією або суттєво викривленими фактами. Як наслідок, така особа приймає завідомо неефективне рішення, адже воно базується на фіктивній реальності, яка не має зв’язку з існуючою реальністю.

Водночас науковець наголошував, що в сучасному світі когнітивні операції стає проводити значно складніше, адже інформаційно-технологічний потенціал міжнародних акторів постійно збільшується, що створює труднощі при намаганні ворожої сторони вплинути на систему прийняття рішень в іншій державі (Stein, 1995).

Не можна не відзначити прогресивне дослідження інформаційного впливу французьких науковців Ю. Марзукі та О. Ульє. На прикладі подій Арабської весни вони зобразили інформаційний вплив, який здійснювався через соцмережі, на «віртуальну колективну свідомість» учасників революційних подій. Фактично об'єктом інформаційного впливу були не конкретні особи чи інституції, а населення як колективна одиниця, що зрештою призвело до зміни режимів в декількох країнах шляхом не організованого та керованого протесту, а хаотичного, інформаційно інспірованого руху мас. Цінність цього дослідження полягає в тому, що воно яскраво демонструє величезний потенціал соцмереж як майданчику інформаційних операцій та інформаційної кооперації (Marzouki & Oullier, 2012).

Загалом мережеве суспільство як новий тип громадянського суспільства зумовило виникнення значних соціально-політичних рухів, інспірованих соціальними мережами. Тепер Інтернет слугує не тільки майданчиком для реагування на певні меседжі, але й виступає інструментом революційної дії, коли умовний автор контенту, зокрема журналіст, може запустити цілком фізичні соціально-політичні процеси, використавши такі відомі платформи як Facebook чи X. Це, зокрема, було яскраво продемонстровано на прикладі України під час подій Революції гідності, коли активність українців в соцмережах сприяла розгортанню протесту (Сергій Даниленко, 2014, с. 49-61). Така тенденція розвитку мережевого інформаційного суспільства підтверджує тезу, що сьогодні ядро генерування громадської думки в політичному житті країни переходить від традиційних ЗМІ (ТБ, газети тощо) до віртуального середовища, зокрема соціальних мереж, і головним генератором цієї думки стає безпосередньо соціум-користувач Інтернету (С. Даниленко & Прокопенко, 2011, с. 96-102).

У XXI столітті інформація виступає визначальним фактором прогресу суспільства. Принципи вільного обміну інформацією та відкритості інформаційних систем вважаються основоположними для інформаційного суспільства. Сучасні технології в сфері інформації та комунікацій відкривають нові можливості для широкого поширення та обміну інформацією. Ретельна інформаційна політика стає невід'ємною складовою системи управління за умов переходу від індустріального до інформаційного суспільства.

Під час аналізу викликів, пов'язаних із формуванням глобального інформаційного суспільства, основною передумовою є чітке визначення та методологічний розгляд поняття інформаційного суспільства, його структури та системи соціальної комунікації.

Вивчення питань становлення та розвитку інформаційного суспільства здійснювалося низкою вчених як у вітчизняному, так і в закордонному науковому середовищі. Серед таких дослідників можна вказати: С. Даниленка, Д. Дубова, М. Ожевана, І. Арістову, В. Бакуменка, Д. Белла, Л. Березовець, О. Білоусова, К. Вербу, Е. Гідденса, О. Гриценка, В. Данильяна, О. Дзьобаня, М. Кастельса, Е. Короткова, Дж. Локка, Н. Лютко, М. Маклюена, Ф. Махлупа, І. Мелюхіна, Дж. Мілтона, Н. Ткачеву, Е. Тоффлера, Ю. Хабермаса, П. Хіманена, В. Фірсова та інших.

Ці дослідники зробили значний внесок у розуміння та аналіз різних аспектів інформаційного суспільства, висвітлюючи його ключові характеристики та вплив на сучасне суспільство. Їхні роботи варіюються від соціологічних, філософських до технологічних та економічних підходів, сприяючи розширенню знань у цій сфері. До прикладу, концепція Д. Белла вважається класичною теорією постіндустріального суспільства, в якій відзначається, що основою принципу цього суспільства є теоретичні знання. Так, їх можна використовувати для нових винаходів, запровадження унікальних аналітичних методів, оцінки втрат окремого політичного курсу. Тому, використовуючи термін «інформаційне суспільство», слід акцентувати увагу на пріоритетності комунікативного компонента в інфраструктурних та соціальних зв'язках (Duff, 1998, с. 373-455).

Сучасні концепції інформаційного суспільства, розроблені вченими, такими як Дж. Бенігер, З. Бжезинський, М. Кастельс, М. Маклюен, Й. Масуда, Дж. Нейсбіт, Е. Тоффлер, П. Друкер та інші, розглядаються більшістю дослідників як нова та відносно самостійна стадія розвитку суспільства. Ця стадія характеризується інформаційною складовою цивілізаційних змін.

Елвін Тоффлер, американський науковець, у своїй концепції інформаційного суспільства, яку виклав у трилогії «Шок майбутнього», «Третя хвиля» та «Метаморфози влади», вказує, що інформаційне суспільство являє собою абсолютно нову стадію суспільного розвитку. У своїх працях він систематизував зміни, що відбуваються у процесі розвитку цивілізації під час інформаційної епохи.

Е. Тоффлер поділяє весь процес еволюції людської цивілізації на три основні фази:

1. Сільськогосподарська фаза, яку він називає «першою хвилею».
2. Індустріальна фаза, відома як «друга хвиля».
3. Фаза «третьої хвилі», що характеризує інформаційну епоху.

Кожна з цих фаз має свої унікальні особливості та вплив на розвиток суспільства, а фаза «третьої хвилі» визначається як ключова для формування інформаційного суспільства (Toffler, б. д.).

Прихід «третьої хвилі» відзначився поширенням «немасових» засобів масової інформації. У 1970-х роках спостерігався занепад багатотиражних газет та журналів у великих містах, а збільшилася кількість міні-журналів, спрямованих на задоволення вузьких особистих інтересів. Е. Тоффлер висловлює думку, що «демасифікація засобів масової комунікації» також впливає на структуру наших думок. Замість довгих і зв'язних ідей дедалі частіше суспільству пропонують короткі модульні образи інформації, такі як реклама, теорії, уривки новин і інше (Тоффлер, 2007).

Також цікавою для розуміння генези і етапів розвитку інформаційного суспільства є науковий доробок філософа та економіста П. Друкера. Так, у своїй роботі «Виклики для менеджменту у 21 столітті» він виділив 4 інформаційні революції, які пережило людство:

1. Перша революція відбулася з виникненням письма приблизно 5-6 тисяч років тому і характеризувалася появою можливості передачі інформації через фізичний носій у формі письма.

2. Друга революція відбулася з винайденням книги приблизно в 14 столітті до н.е. Цей період характеризувався появою можливості передачі значних обсягів інформації або ж збереження її.

3. Винайдення друкарського верстату Йоганнесом Гутенбергом в 15 столітті нашої ери, що зумовило масовість передачі інформації через фізичний носій. Як наслідок, у світі відбувся бум книгодрукування, з'явились ЗМІ тощо.

4. Сучасний технологічний період, розпочатий у 1950-х роках з появою комп'ютеру. У цей же період з'явилась мережа Інтернет і комунікація між людьми стала всепроникною.

Також П. Друкер прогнозував, що світ уже в процесі наступної – 5-ої революції, яка на відміну від попередніх не концентруватиметься на революції засобів передачі інформації, технологій. На думку філософа, революція інформаційного суспільства пролягатиме в сфері концептів і розпочне дискусію про саму суть інформації (Drucker, 2001).

Цей підхід П. Друкера яскраво демонструє не тільки еволюцію соціального значення інформації та комунікації як засобу її передачі, але й віхи розвитку інформаційного суспільства, адже саме розвиток засобів комунікації дозволяє говорити сьогодні про появу такого поняття як інформаційне суспільство. До того ж його прогноз майбутньої хвилі уже сьогодні має ознаки реалізації, адже розвиток таких технологій як «штучний інтелект», стрімка «інтернетизація світу», підміна «реальною» реальністю віртуальною свідчать про переосмислення сутності сучасного світу комунікацій та інформації.

Для багатьох науковців, які вивчають наслідки інформаційної революції та приходу інформаційного суспільства, характерне прагнення надати максимально деталізоване визначення самого поняття. Дослідник інформаційного та глобального суспільства В. Бебик твердить, що інформація тепер є одним з «найважливіших суспільних ресурсів», а сфера інформаційної економіки –

ключовою галуззю суспільної діяльності. В. Бебик визначає цей сектор як головний рушійний фактор для науково-технічного, соціально-економічного і культурно-освітнього прогресу (Валерій Бебик, 2011, с. 41-49).

Загалом термін «інформаційне суспільство» виник і був використаний представниками різних наук, такими як А. Турен, П. Серван-Шрайбер, М. Понятовський, М. Хоркхаймер, Ю. Хабермас, Н. Луман, М. Маклюен, Д. Белл, Е. Тоффлер, Д. Масуда, для характеристики особливого типу постіндустріального суспільства. Основною умовою формування цього суспільства вони вважали розвиток потужних і високотехнологічних глобальних інформаційних мереж.

Вчені, такі як Д. Белл і Е. Тоффлер, досліджували вплив інформації та інформатизації на суспільство і процес переходу від індустріального до інформаційного суспільства. М. Маклюен прогнозував становлення глобального інформаційного суспільства у вигляді «глобального села», де глобальна спільнота впливає на дії урядів і міжнародних інституцій через засоби масової комунікації (Валерій Бебик, 2005; Бебик, Шергін & Дегтерьова, 2006).

Світове наукове співтовариство активно дискутує про ідеологічні аспекти становлення інформаційного суспільства, не тільки в контексті формування «глобального села», але і в рамках утворення глобального уряду. У сфері інформації та культури, за Г. Шиллером, це виявляється через реалізацію концепцій медіа-імперіалізму та культурного імперіалізму. З цієї точки зору інформаційно-комунікаційна діяльність, контрольована транснаціональними корпораціями (далі – ТНК), призводить до негативних системних явищ в глобальній інформаційно-культурній сфері. Слід зазначити, що науковець Дж. Томлінсон не згоден з однозначністю ідеологічних впливів медіа-імперіалізму.

Хоча дослідники в цілому одноголосні в тому, що категорія інформації є ключовою у визначенні інформаційного суспільства, визначення поняття «інформаційне суспільство», за деякими вченими, істотно відрізняються. Так, знаменитий іспанський соціолог М. Кастельс під інформаційним суспільством розуміє те суспільство, яке сформоване за мережевою ознакою, і в якому головну роль відіграє приналежність до тієї чи іншої мережі – такої, наприклад, як мережі

ТНК чи ЗМІ. Глобальна інформаційна мережа формує нову організаційну структуру інформаційних процесів і потоків, які змінюють інші існуючі соціальні структури, перетворюючи їх у мережеві. М. Кастельс вважає, що на сьогодні сформувалася культура мережевого суспільства, що виступає каталізатором економічної, інформаційної та культурної глобалізації. М. Кастельс показує, що мережеве суспільство включає держави, але не обмежується ними і представляє собою спільність вищого порядку. У своїй книзі «Мережеве суспільство» Кастельс стверджує, що влада над потоками інформації менш значуща, ніж влада потоків інформації (Castells, 2010).

Соціологи Д. Белл та А. Турен у дослідженні постіндустріального соціуму наполягали на тезі, що потоки інформації трансформували індустріальне суспільство (Bell, 1976; Touraine, 1971). На думку дослідника ЗМІ Г. Шиллера, який, як і Кастельс, дотримується неомарксистських поглядів, в інформаційному суспільстві головну роль відіграють капіталістичні відносини. Сама ж інформація стає економічним товаром, а ТНК отримують можливості експлуатації слаборозвинених в економічному плані держав. Теоретичне осмислення та систематизація різних концепцій інформаційного суспільства представлено у роботі Ф. Вебстера «Теорії інформаційного суспільства» (Webster, 2013).

Т. Фрідман у книзі «Лексус і оливкове дерево», написаній у 1999 р., підкреслює взаємозв'язок між розвитком Інтернету та процесами глобалізації (T. Friedman, 1999). Пізніше, 2005 р., у своїй книзі «Світ плаский: коротка історія XXI століття» він стверджує, що Інтернет та інші інформаційні технології зробили нас «сусідами», вбивають географію, відстань та мову (T. Friedman, 2007). На його думку, все те, що сьогодні розуміється під глобалізацією: вільний обмін товарами, капіталами, робочою силою, незважаючи на відстані та державні кордони, не було б можливим без обміну інформацією, знаннями та ідеями.

Погоджуючись із доказами Т. Фрідмана, не можна не відзначити, що розвиток Інтернету аж ніяк не тягне за собою гомогенізацію та універсалізацію світу, а також не вирішує проблему конфліктності, властивої міжнародній системі. Відповіддю на стрімке зростання обсягу світової інформації та глобалізаційні

процеси є сегментація та маргіналізація суспільства. Державні географічні розмежування доповнюють нові інформаційні кордони. Розвиток Інтернету створює нові лінії нерівності між «інфобагатими» та «інфобідними», що породжує суперечності на міжнародній політичній арені. А саме мова йде про проблему «цифрового розриву», що знайшла своє відображення в Окінавській хартії інформаційного суспільства, підписаної державами *G7* 22 липня 2000 року, в якій закликалося зробити все можливе, щоб кожна людина мала можливість доступу до інформаційних та комунікаційних мереж. Також ця хартія давала своє визначення «інформаційному суспільству» як суспільства, економіка якого заснована на інформаційних технологіях і яка організована таким чином, щоб людина та спільнота могли себе якнайкраще реалізувати (Okinawa Charter on Global Information Society, 2000).

Вітчизняна наукова школа політичних досліджень детально досліджує феномен інформаційної безпеки та інформаційного суспільства, зокрема в контексті активного використання інфопростору для протиборства різних держав світу. Зокрема, слід відзначити наукові праці таких науковців як М. Ожеван, О. Довгань, Б. Юськів, Д. Дубов, О. Курбан, О. Литвиненко, О. Фролова, С. Даниленко, Н. Піпченко, Г. Почепцов, В. Лук'янова та А. Лаутар, П. Біленчук.

Наукові праці М. Ожевана вважаються одними з ключових у вивченні питань інформаційної безпеки в українській науковій думці. Зокрема, дослідник визначав безпекову політику провідної країни світу як поєднання ліберально-демократичної та консервативно-республіканської ідеології. Також М. Ожеван наголошував, що сьогодні політики інформаційної безпеки розвинених держав, зокрема США, все більше мілітаризуються, що призводить до їх активнішого використання в умовах гібридних війн (Ожеван, 2010, с. 20-25).

Також варто відзначити внесок М. Ожевана в дослідження комунікацій, зокрема використання стратегічних наративів як інструментів впливу. Під ними науковець розуміє засоби, які використовують політичні актори, щоб сформувати сенси та значення «великої політики». Тобто з допомогою таких наративів держави, корпорації, громадські організації артикулюють середовищу свою систему та набір

цінностей. На думку М. Ожевана, провідні наративи поширюються ключовими медіа *(mainstream media)*, які використовують передусім наративи для реалізації (фреймінгу), «окреслення пріоритетів» (праймінгу) та встановлення «порядку денного» *(agenda setting)* (Ожеван, 2016).

Питання державного суверенітету, зокрема інформаційного його виміру, вивчав О. Довгань. На його думку, в умовах глобалізації, стрімкої інформатизації та технологізації світу інститут державного суверенітету потребує адаптації до сучасних реалій. У цьому контексті важливим стає розвиток державою соціальних інформаційних комунікацій, насамперед тих, що вибудовуються на базі електронних технологій, які забезпечують обіг е-ресурсів і є самі по собі окремою мережею. Водночас держава зобов'язана подбати про інформаційну безпеку такої інфраструктури та комунікації, що стає одним з основних її завдань в рамках забезпечення державного інформаційного суверенітету (Довгань, 2014, с. 102-112).

Також варто відзначити напрацювання О. Курбана, який сконцентрував свою наукову діяльність на дослідженні феномену інформаційних війн. Зокрема, дослідник наголошує на ключовій ролі інформаційного простору у сучасному протиборстві держав. Так, О. Курбан дослідив історію інформаційних війн, визначив сучасні стратегії, тактики та прийоми її ведення. Зазначимо, що дослідник також наголосив на особливій ролі соціальних мереж у структурі сучасної гібридної війни. Саме вони часто-густо стають полем бою між ворогуючими сторонами, зокрема шляхом використання медіа-вірусів як інформаційної зброї (Курбан, 2016).

Вагомими є дослідження О. Литвиненка, присвячені теоретико-методологічним засадам спеціальних інформаційних операцій та пропагандистських кампаній у сучасному світі. Науковець підкреслює, що основою теорії інформаційної безпеки в частині поєднання з теорією «м'якої сили» є стратегія непрямих дій, яка, зокрема, пов`язана з використанням політичних, психологічних та інформаційних засобів тиску на супротивника. Ці дії діють повільніше, але системно підривають безпеку опонента. Також О. Литвиненко виокремив типи пропагандистських технологій в інформаційних операціях, серед

яких «м'які» (не суперечать системі сталих установок суспільства) та «жорсткі» (передбачають кардинальну модифікацію/руйнування наявних установок). Виходячи з цього автор виділяв спеціальні інформаційні операції проти лідерів держав, операції, спрямовані на дестабілізацію ситуації в країні, та операції проти громадських лідерів (Литвиненко, 2003).

На прикладі російського пропагандистського ЗМІ *Russia Today* дослідники Б. Юськів, Н. Карпчук та С. Хомич демонструють, як Кремль використовує медіа у веденні гібридної війни проти Заходу. Зокрема, науковці наголошують, що на операційному рівні ціллю медіа пропаганди Росії є не стільки намагання переконати цільову аудиторію в своїй правоті чи спонукати її до певних дій, як створити ситуацію інформаційної розгубленості в інфопросторі, ситуацію, коли цільова аудиторія постійно сумнівається в достовірності інформації, яку отримує. Також Б. Юськів, Н. Карпчук та С. Хомич підкреслюють, що діяльність такого медіа чітко продиктована завданнями стратегії гібридної війни Росії проти України та Заходу, тобто будь-які зміни в конфігурації, інтенсивності та направленості стратегії знаходять своє миттєве відображення в адаптації медійної роботи (Yuskiv, Karpchuk & Khomych, 2021, с. 235-258).

Водночас, на думку дослідників Б. Юськіва та Н. Карпчук, Україна є тільки «демонстраційним експонатом» потенціалу Росії в частині ведення гібридної війни, зокрема реалізації її інформаційної компоненти. Так, Кремль, використовуючи інформаційні приводи та інформаційний супровід, виходить далеко за межі України, перетворюючи локальну стратегію гібридної війни у глобальну. Для створення наративів, які відповідають цілям стратегії РФ, використовуються сучасні медіаінструменти та методи, серед яких одним із головних є генерування кількох варіантів «реальності», які мають заплутати споживача інформації (Карпчук & Юськів, 2022, с. 71-85).

Дослідженням інформаційної безпеки в контексті глобальних геополітичних процесів, зокрема його кібер складової, відзначився Д. Дубов. У своїй науковій праці «Кіберпростір як новий вимір геополітичного суперництва» (2014), він дослідив генезу наукової думки щодо вивчення поняття кіберпростору в контексті

геополітики. Також значну увагу в праці було приділено дослідженню поняття «кібермогутності» і його співвідношення з системою національної безпеки держави. Також Д. Дубов акцентує на важливості відстоювання національних інтересів держави в кіберпросторі як ще одного виміру геополітичного протиборства. Зокрема, для цього дослідник навів приклад протистояння США та Китаю, де кібернетична складова є одним із ключових секторів протиборства (Дубов, 2014).

Також Д. Дубов у своїх роботах акцентує на триваючому процесі трансформації методів інформаційного впливу в умовах технологічної еволюції. Прикладом може стати класичне «приховане мовлення», яке раніше було можливо послухати за допомогою «піратського радіо» сьогодні замінюється міжнародними соціальними платформами. Фактично різні онлайн платформи, такі як *WikiLeaks*, *Telegram*, *X* тощо, стали заміною для преси як основного майданчика поширення дезінформації. Ба більше, нові майданчики мають значно більше охоплення, а доступ до них максимально спрощений (Дубов, 2019).

Слід звернути увагу на дослідження С. Даниленка концепції «розумної сили» в контексті протистояння України та Росії. Зокрема, для розробки української версії стратегії С. Даниленко та група дослідників використовують інтегративний підхід, який охоплює взаємодію соціальної філософії, історії, політології, інформаціології, соціології, психології тощо. Науковець наголошує, що одним із дієвих елементів «розумної сили» у протидії ідеології «русского мира» та деструктивним впливам інформаційно-психологічної агресії Росії є українознавча компетентність. Саме тому врахування дієвості українознавчої компетентності наших громадян є одним із ключових факторів стратегії перемоги в інформаційній війні з Росією (С. Даниленко, Авер'янова, Воропаєва & Дроботенко, 2022, с. 43-53).

Окремо слід виділити науковий доробок Н. Піпченко, яка досліджує специфіку реалізації політики міжнародних акторів у інформаційному просторі, зокрема явище цифрової дипломатії. Так, дослідниця наголошує, що розвиток інформаційно-комунікаційних технологій змінив саму сутність комунікації зовнішньої політики. Можливість отримання інформаційного фідбеку перетворила

комунікацію держав з суспільством в інтерактивну комунікацію, де суспільство не тільки споживає і реагує, але й вступає у взаємодію з комунікатором. Тому Н. Піпченко наголошує, що високий рівень комунікаційних навичок в дипломатичних представництвах, володіння сучасними інформаційними технологіями, їх вдале використання в цифровій дипломатії є необхідною умовою ефективної зовнішньополітичної діяльності держав. На прикладах США та ЄС Н. Піпченко демонструє наскільки ефективною може бути цифрова дипломатія у глобальному просуванні позитивного образу держав та блоків, що безумовно створює сприятливі умови для реалізації зовнішньополітичного впливу зазначених акторів на міжнародне середовище (Pipchenko, 2020, с. 19-26).

Явище дезінформації та пропаганди, межі між цими поняттями у своїх працях активно досліджує Г. Почепцов. За словами науковця, дезінформація як системний інструментарій є сучаснішим винаходом, ніж пропаганда, яка до «зіпсування» її тоталітарними режимами була доволі почесним терміном. Так, пропаганда була пов'язана з Римською курією, де вона асоціювалася з місіонерською роботою з розповсюдження віри. «Сьогодні пропаганда пішла в тінь, нею пристойні люди не займаються, для них придумали тепер новий термін – стратегічні комунікації», – наголошує Почепцов (Почепцов, 2019).

Окремо слід відзначити наукові напрацювання О. Фролової, яка значну увагу приділяє міжнародному співробітництву в галузі забезпечення інформаційної безпеки. Дослідниця в своїх роботах акцентує на наднаціональних форматах забезпечення інформаційної безпеки, розробки її теоретико-методологічної основи. Йдеться про такі структури як ООН, НАТО та ЄС. На думку О. Фролової, транскордонний характер загроз інформаційній безпеці зумовлює необхідність кооперації міжнародних урядових і неурядових структур як необхідної умови для мінімізації шкоди від таких загроз (О. Фролова, 2019, с. 123-136).

Щодо джерельної бази дослідження, то її емпіричну основу склали:

- нормативні акти Франції, Німеччини та Великої Британії, Європейського Союзу, НАТО, інших міжнародних організацій, які регламентують сферу

інформаційної безпеки, зокрема Акт про цифрові послуги (*DSA*), Декларація Блечлі, Декларації за підсумками самітів НАТО тощо;

- концептуальні документи, наприклад Національна стратегія інформаційної безпеки Франції (2015 року), Міжнародна стратегія Франції в галузі інформаційних технологій (2017 року), які формують візію стратегії інформаційної безпеки, зокрема стратегії кібербезпеки, інформаційної безпеки вищезазначених суб'єктів;

- статистичні дані, що стосуються оцінки рівня цифровізації держав, їх кіберзахищеності, а також дані соцопитувань громадської думки в питаннях кібербезпеки та боротьби з дезінформацією.

Більшу частину джерельної бази складають документи англійською та французькою мовами: йдеться про національні та міжнародні документи, які регулюють безпекову інформаційну безпеку.

Підсумовуючи, слід зазначити, що теоретичні та методологічні засади інформаційної безпеки у різних її вимірах та конфігураціях активно досліджуються українською та закордонними науковими школами. Перманентна змінність інформаційних процесів у світі, поява нових технологій, що фактично свідчить про безмежний потенціал росту інформаційної компоненти міжнародних відносин, зумовлюють потребу у постійному осмисленні та переосмисленні ролі та впливу інформації на систему міжнародних відносин та міжнародну систему безпеки зокрема.

Висновки до Розділу 1

У сучасному світі інформаційна безпека стала необхідною умовою для захисту інтересів людини та соціуму в різних сферах, таких як економіка, оборона, політика та соціальна сфера. Загрози та небезпеки, що існують у сучасному світі, мають інформаційний характер і можуть впливати на людей через різні канали інформації.

Одним з ключових аспектів інформаційної безпеки є комп'ютерна безпека, яка включає заходи щодо захисту обладнання та інформації від стихійних лих, а також від умисних або випадкових пошкоджень. Соціально-інформаційна безпека є іншим важливим аспектом, оскільки багато техногенних загроз пов'язані з помилками у передачі інформації в соціальних відносинах.

Забезпечення інформаційної безпеки неможливе без покращення якості «людського фактору» в техногенних структурах. Участь держави у формуванні глобальної інформаційної єдності має велике значення для соціального розвитку.

На практиці інформаційна діяльність передбачає боротьбу з інформаційним забрудненням довкілля та недопущення використання інформації у протиправних цілях. Зростаюча роль інформації у суспільстві підкреслює актуальність проблем інформаційної безпеки.

Помилки та неточності в інформаційних системах можуть створити загрозу для економічної, соціальної та екологічної стійкості. Інформація стала ключовим ресурсом суспільного життя, і неперервний розвиток інформаційних технологій робить інформаційну безпеку дедалі важливішою.

Прогрес у сфері інформаційних технологій створює як нові можливості, так і нові загрози, з якими потрібно ефективно впоратися. Системи інформаційної безпеки виступають як ключовий елемент у забезпеченні інформаційної переваги та захисті від ризиків і загроз.

РОЗДІЛ 2
ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФРАНЦІЇ: ФОРМУВАННЯ ТА РЕАЛІЗАЦІЯ ЗА УМОВ МІЖНАРОДНО-ПОЛІТИЧНИХ ТРАНСФОРМАЦІЙ

2.1. Політико-правові засади Європейського Союзу з регулювання інфосфери як основа політики інформаційної безпеки Франції

Свій початок інформаційна політика Європейського Союзу бере з опублікованого в 1994 році звіту «Європа і глобальне інформаційне суспільство. Рекомендації Європейській Раді», який був підготовлений на замовлення Європейської Ради Мартіном Бангеманом, на той час комісаром Єврокомісії з питань внутрішнього ринку та промисловості (Bruggemann, 2010, с. 5-22).

У цьому звіті чітко наголошується, що в глобальному суспільстві настала «Інформаційна ера» і Європейський Союз має адаптувати свою політику до нової реальності, щоб не втратити свою конкурентну перевагу. Для цього в звіті пропонується конкретний «План Дій». Він передбачав сприяння лібералізації в інформаційній, телекомунікаційній та технологічній сферах; створення на рівні ЄС спільної регуляторної рамки, яка б стала основою для будівництва європейського інформаційного ринку. Водночас у звіті наголошується, що європейські держави мають відмовитися від монополії держави в інформаційній сфері та віддати ринок інформаційних послуг повністю у руки приватного сектору (Bangemann, 1995).

Оперативність створення таких документів пояснюється тим, що європейське суспільство на той час гостро потребувало рішень проблем, спричинених різким розвитком постіндустріального суспільства. Основні ідеї документу були спрямовані на створення інформаційного суспільства на засадах процесу європейської інтеграції для забезпечення економічної стабільності країн Європи; надання можливостей для вільного доступу до глобальних мереж, а також вирішення актуальних соціальних проблем.

У 1994 році Європейська комісія прийняла ще один важливий програмний документ під назвою «Шлях Європи до інформаційного суспільства». У цьому документі були визначені основні принципи розвитку інформаційного суспільства, серед яких важливими були гарантія вільного доступу до інформаційних систем, формування спільної колективної думки в європейській спільноті щодо розвитку інформаційного суспільства, розробка концепції інформаційної політики ЄС та сприяння розвитку європейської ідентичності (Бєлоусова, б. д., с. 45-54).

Вже наступного року ЄС перейшов до конкретних регуляторних рішень, коли прийняв у жовтні 1995 року Директиву про захист даних (95/46/ЕС) – революційного документу, яким блок фактично визнавав настання нової інформаційної реальності, в якій дані потребують додаткового захисту. Директива встановлювала чіткі принципи захисту даних, зокрема прозорість, підзвітність та пропорційність, а також визначала виняткові випадки, коли персональні дані могли бути передані без відома їх власника (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995). Фактично ця регуляторна рамка була базовою для сфери захисту даних до 2018 року, коли набув чинності Загальний регламент захисту даних (General Data Protection Regulation – GDPR), прийнятий в 2016 році. Він підсилив існуюче регулювання та адаптував його до сучасних інформаційних та технологічних реалій («General Data Protection Regulation», б. д.)

Безпосередньо до створення спеціалізованих інституційних базисів власної політики інформаційної безпеки, зокрема в частині захисту власного кіберпростору, ЄС перейшов у 2004 році. Так, регламентом від 10 березня 2004 року було створено Агентство з кібербезпеки Європейського Союзу (*European Union Agency for Cybersecurity — ENISA*). До сьогодні це основний орган ЄС, який відповідає за питання кібербезпеки, включаючи як технічний аспект, так і координацію сил та ресурсів, інформування населення («About ENISA - The European Union Agency for Cybersecurity», б. д.; Evaluation of the EU decentralised agencies in 2009, 2009).

Метою створення Агентства було підвищення здатності ЄС протидіяти загрозам інформаційної безпеки та реагувати на атаки в цифровому просторі. Початковий Регламент від 2004 року було доповнено Регламентом 2013 року, який визначає перед агентством такі завдання:

- підтримка високого рівня експертизи;
- допомога органам ЄС у формулюванні політики щодо мережевої та інформаційної безпеки;
- сприяння органам і країнам-членам ЄС у виконанні політики, необхідної для відповідності вимогам до мережевої та інформаційної безпеки в межах європейського законодавства;
- підтримка ЄС та країн-членів у підвищенні здатності та готовності до запобігання, виявлення та реагування на проблеми та інциденти, пов'язані з інформаційною безпекою;
- активна взаємодія з представниками громадського і приватного секторів (Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 Text with EEA relevance, 2013).

Зазначимо, що у 2019 році з прийняттям Акту про кібербезпеку ЄС мандат *ENISA* було розширено ще більше. Відтоді та до сьогодні агентство також відповідає за підготовку загальноєвропейських умов сертифікації інформаційно-комунікаційних продуктів, процесів та сервісів. Раніше подібна сертифікація проводилась виключно на національному рівні, а співпраця між державами на рівні ЄС обмежувалась виключно координацією («The EU Cybersecurity Act», 2019).

У 2013 році була оприлюднена Стратегія кібербезпеки ЄС, яка визначила пріоритети в сфері кібербезпеки, серед яких зміцнення стійкості кіберпростору, боротьба з кіберзлочинністю, розробка стратегії цифрової безпеки на основі «Загальної безпекової та оборонної політики», поліпшення цифрової інфраструктури та підтримка європейських цінностей. Цей документ також став одним із базисних у діяльності агентства *ENISA* («Joint communication to the

European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity strategy of the European Union: an Open, Safe and Secure Cyberspace Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace», 2013). Слід зазначити, що з 2007 року *ENISA* підтримує проєкти співпраці між країнами-членами ЄС у сфері інформаційної безпеки. Наприклад, *ENISA* підтримала проєкт між Болгарією та Угорщиною щодо створення болгарської групи реагування на кіберінциденти (*CERT*), проєкт між *CERT-FI* (Фінляндія) та *CSIR/MERAKA* (Південно-Африканська Республіка) щодо співпраці та обміну досвідом у сфері кібербезпеки, а також ініціативу зі створення Південно-Африканської групи швидкого реагування (*Computer Security Incident Response Team*).

Одним із векторів роботи *ENISA* є розбудова партнерства бізнесу і держави, зокрема у фінансовому секторі. Йдеться передусім про обмін інформацією про кіберзлочини за посередництва Центрів фінансової інформації та аналізу (*FI-ISAC*). Серед досягнень агентства на цьому напрямі – створення системи, здатної виявляти ризики інформаційної безпеки (*Emerging and Future Risks*); заснування Форуму з безпекових питань та запуск роботи експертних команд, які спеціалізуються на оцінці та аналізі інформаційних викликів та загроз («General Report», 2008).

З 2010 року *ENISA* кожні два роки проводить в межах ЄС та Європейської асоціації вільної торгівлі (далі – ЄАВТ) європейські навчання «Кібер Європа». Під час цих навчань відпрацьовується реагування на інциденти в кіберпросторі, які впливають на сферу публічного та приватного секторів («ENISA meets cyber-experts to plan Cyber Europe 2018», 2017).

ENISA активно працює також для захисту політичних процесів у Європі. Так, для захисту європейських виборів 2019 року агентство оприлюднило керівництво для країн-членів, щоб забезпечити належний рівень технічної безпеки. Це керівництво має рекомендаційний характер і включає аналіз конкретних випадків загроз електоральним системам (*Compendium on Cyber Security of Election Technology*, 2018). Необхідність таких дій *ENISA* викликали повідомлення про втручання у президентські вибори в США 2016 року з боку Росії, а також у вибори

у Франції у 2017 році. Під «втручанням» Європейська комісія розуміє різноманітні дії, включаючи злам поштових скриньок, обвалення вебсайтів за допомогою *DDoS* атак, втручання в електоральні системи і фінансування політичних сил (*European Cybersecurity Journal: strategic perspectives on cybersecurity management and public policies*, 2017).

Інституційну підтримку *ENISA* та загалом європейської політики інформаційної безпеки також надає створений у 2013 році Центр кіберзлочинності Європолу (*Europol's Cybercrime Centre – EC3*), основною функцією якого є боротьба з транскордонними кіберзлочинами. Зокрема, в рамках нього держави-члени ЄС можуть обмінюватися інформацією про кіберзагрози та ризики, координувати власні дії в кіберпросторі, а також використовувати *EC3* як майданчик для співпраці з бізнесом та громадськістю у протидії кібервикликам («EU cybersecurity initiatives: working towards a more secure online environment», 2017).

Суттєві корективи у європейську політику інформаційної безпеки внесла збройна агресія Росії проти України, розпочата у 2014 році. Використання Кремлем інструментів пропаганди, дезінформації, кібератак як проти України, так і проти колективного Заходу, змусило ЄС адаптувати власну політику інфобезпеки до нових викликів.

Одним із перших рішень на цьому напрямку стало створення у 2015 році Оперативної робочої групи зі стратегічних комунікацій (*East StratCom Task Force*, далі *East StratCom*). Її створення було передбачено висновками Європейської Ради від березня 2015 року, в яких протидія дезінформації з боку Росії була визначена одним із пріоритетів політики ЄС («European Council meeting (19 and 20 March 2015) – Conclusions», 2015).

План дій щодо стратегічних комунікацій, розроблений у червні 2015 року на виконання березневих висновків Єврокомісії, визначив основні напрямки діяльності для *East StratCom*:

- підвищення потенціалу ЄС у сфері стратегічних комунікацій;
- розвиток партнерських зв'язків та розширення можливостей взаємодії;

- здійснення комунікаційних заходів за програмами ЄС, управління проєктами та активностями в межах країн Східного партнерства;
- захист свободи ЗМІ та свободи висловлення;
- запровадження ініціатив громадянської дипломатії;
- розвиток професійного потенціалу журналістів та інших представників медіа;
- підтримка плюралізму в російськомовному медіапросторі;
- співпраця з громадянським суспільством;
- підвищення рівня обізнаності, розвиток критичного мислення та підтримка медіаграмотності;
- зміцнення співпраці між країнами-членами у сфері законодавчого регулювання медіапростору («Action plan on strategic communications», 2015).

Ця група зазначена також в інших документах, зокрема у резолюції Європарламенту, присвяченій протидії пропаганді третіх сторін («European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties», 2016). У тій самій резолюції російські установи та ЗМІ, такі як *Sputnik*, Россотрудничество, Русский мир, а також державні ЗМІ, були визначені як основні джерела пропаганди та дезінформації.

Основними інструментами *East StratCom* є взаємодія з пресою, комунікації у мережі Інтернет, написання статей та створення аудіовізуальних матеріалів («Strategic communications», б. д.). *East StratCom* займається моніторингом проурядових російських ЗМІ і надає спростування, якщо це необхідно, систематизуючи всі випадки. Інформація, яку готує *East StratCom*, часто цитується в різних ЗМІ, зокрема *The Guardian*, *Welt*, *Zeit*, *Independent*, *USA Today* тощо («EUvsDisinfo», б. д.).

Хоча початково *East StratCom* був заснований для боротьби з російською дезінформацією, наразі підрозділ став важливою структурою для просування комунікацій Європейського Союзу у країнах Східного партнерства та підтримки незалежних ЗМІ. В жовтні 2019 року було проведено оцінку ефективності роботи відомства. За підрахунками, група опублікувала понад 6500 випадків спростування

новин на понад 20 мовах («EUvsDisinfo: how to debunk over 6,500 disinformation cases in four years?», 2019).

Наступне оновлення європейської системи інформаційної безпеки включало в себе підготовку та оприлюднення Єврокомісією у квітні 2016 року Спільного плану з протидії гібридним атакам. У документі зазначається, що виникла нова загроза гібридних атак у країнах Східного та Південного партнерств, у вирішенні якої ЄС має виступити посередником. Наприклад, у плані відповіді на гібридні загрози за 2016 рік у розділі стратегічних комунікацій зазначається про одну із таких загроз – таргетовані кампанії, спрямовані на соціальну дестабілізацію («Joint communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response», 2016).

У документі висвітлено ще один важливий аспект – впровадження системи моніторингу за повідомленнями в Інтернеті. Зокрема, план рекомендує поглибити співпрацю з Групами протидії загрозам комп'ютерної безпеки (*CSIRTs*), які були утворені відповідно до Директиви ЄС 2016 року про заходи щодо підвищення рівня мережевої та інформаційної безпеки в ЄС (DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 2016). Згідно з тією ж Директивою було засновано Групу взаємодії у сфері безпеки мережі та інформації, яка призначена для координації дій у кіберпросторі між країнами, включаючи взаємодію з *CSIRTs* та сприяння обміну інформацією між представниками відповідних міністерств («NIS Cooperation Group», 2023). Згідно зі Спільним планом з протидії гібридним атакам, пізніше було засновано Центр передових технологій у протидії гібридним загрозам, який тісно взаємодіє з НАТО (необхідність такої співпраці відзначена у плані окремо).

Загалом, на основі цього плану можна виділити два основні напрямки діяльності ЄС у сучасній інформаційній політиці:

- стратегічні комунікації та боротьба з дезінформацією;
- кібербезпека.

Того ж 2016 року ЄС прийняв власну Глобальну стратегію зовнішньої та безпекової політики, де інформаційній безпеці відводилось чільне місце. Так, стратегія вказує, що одним із ключових факторів розвитку ЄС має стати забезпечення вільного руху інформації, головним для чого є вільний та безпечний Інтернет. Також в стратегії зазначається, що Євросоюз повинен бути завжди готовим прийти на допомогу державам-членам, які стикнулись з безпосередніми кіберзагрозами, сприяти розвитку інформаційних технологій з врахуванням важливості збереження приватності користувачів, а також ініціювати співпрацю всередині ЄС в питаннях кібербезпеки. Окремим напрямком роботи ЄС, згідно документу, має стати поглиблення співпраці з США та НАТО у сфері кібербезпеки. Окрім наднаціонального та національного рівнів, ЄС акцентує в стратегії на важливості кооперації з бізнесом та громадськістю у протидії кіберзагрозам (*Convention on cybercrime*, 2022). Ці цілі та принципи згодом, в 2020 році, були деталізовані та розширені в опублікованій Єврокомісією Кіберстратегії ЄС, яка концентрується безпосередньо на політиці захисту ЄС в кіберпросторі (Дубов & Ожеван, 2012).

У квітні 2018 року ЄС оприлюднив «Повідомлення щодо боротьби з дезінформацією в Інтернеті», підготовлене на основі громадських опитувань та досліджень від *Eurobarometer*. У цьому документі наголошується, що Інтернет набуває дедалі більшого значення як джерело новин. Водночас відзначається постійне зростання кількості дезінформації від різних внутрішніх та зовнішніх акторів, що порушує демократичні принципи та обмежує здатність європейського населення здійснювати свідомий вибір. Сама ж дезінформація розглядається як складова гібридної війни, а кампанії дезінформації з Росії – як основна загроза. Одні з можливих наслідків дезінформації проявляються в зниженні довіри до науки та емпіричних доказів («COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Tackling online disinformation: a European Approach», 2018).

Напередодні європейських виборів, у 2018 році, було також прийнято ще один важливий документ – «Зведення правил боротьби з дезінформацією». Це перший випадок, коли представники бізнесу вирішили добровільно впровадити стандарти саморегулювання з метою протидії дезінформації. Цей документ був створений для виконання завдань, визначених у «Повідомленні про боротьбу з дезінформацією в Інтернеті» 2018 року. Прозорість рекламних політичних кампаній, припинення дії фейкових облікових записів та демонетизація для поширювачів дезінформації були обрані як основні методи. *Facebook*, *Google*, *Twitter*, *Mozilla* та інші платформи приєдналися до цієї ініціативи. Пізніше учасники надавали звіти Європейській комісії щодо випадків дезінформації та заблокованих акаунтів.

Станом на сьогодні Європейський Союз у співпраці з приватним сектором розробили і впровадили уже оновлену версію «Зведення правил боротьби з дезінформацією», яка була презентована Єврокомісією у 2022 році і уже підписана 34 великими компаніями, серед яких *Google*, *Adobe* та *TikTok*. Вона враховує досвід, отриманий під час протидії російській дезінформаційній машині, та враховує інформаційні виклики та загрози, які створила для світу пандемія COVID-19. Серед нововведень: впровадження інструментів позбавлення доходів тих, хто поширює дезінформацію в соцмережах, підтримка факт-чекингових ініціатив, забезпечення прозорості політичної реклами та посилення захисту споживачів інформації.

Узагальнюючи, можна виділити такі ключові принципи, які об’єднують нормативно-правові акти Євросоюзу, що стосуються протидії дезінформації:

- поліпшення захисту персональних даних;
- контроль політичної реклами шляхом публікації інформації щодо замовників;
- створення мережі факт-чекерів;
- обмін досвідом у боротьбі із поширенням дезінформації;
- прозорість інтернет-платформ;
- підтримка професійної та якісної журналістики (С. Даниленко & Фурсай, 2020, с. 25-30).

Інституційно реалізацію «Зведення правил боротьби з дезінформацією» забезпечують Центр прозорості та Робоча група, завдання яких полягає у моніторингу ефективності впровадження правил та адаптація їх у відповідності до сучасних тенденцій у світі інформаційних технологій («The 2022 Code of Practice on Disinformation», 2022).

З метою втілення положень «Повідомлення 2018 року» Європейська комісія також запровадила Наглядовий центр за соціальними мережами *(SOMA).* Цей центр є платформою для моніторингу ЗМІ та виявлення дезінформації. Будь-яка особа чи організація в ЄС може приєднатися до цього центру, чия діяльність спрямована на перевірку достовірності фактів. Платформа надає різноманітні технологічні інструменти і можливість обмінюватися інформацією щодо випадків дезінформації. Основні завдання цієї організації включають моніторинг, надання освітніх послуг, експертні рекомендації, оцінку результатів і координацію зусиль («SOMA - About us», 2024).

Європейська комісія зробила ключовий крок у рамках стратегії протидії дезінформації, прийнявши у грудні 2018 року «План дій проти дезінформації» («JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Report on the implementation of the Action Plan Against Disinformation», 2019). План визначає дезінформацію як інформацію, яка є досить неправдивою або спотвореною і розповсюджується з метою отримання економічної вигоди або навмисного введення громадськості в оману, що може завдати шкоди суспільству. Особливий акцент у Плані робиться на загрозах для демократичних процесів. «План дій проти дезінформації» визнає боротьбу з гібридними загрозами, включаючи стратегічні комунікації, як один із пріоритетів у сфері забезпечення безпеки. В тексті вказується на хімічну атаку в Солсбері як на приклад гібридної загрози, що підкреслює необхідність багаторівневої безпекової політики в контексті російської загрози. План робить акцент на роботі *East StratCom* та Європейської служби зовнішньої дії в східному напрямку в рамках стратегії боротьби з гібридною

війною, де дезінформаційні кампанії пов'язані з кібератаками та проникненням у комп'ютерні мережі.

У «Плані дій проти дезінформації» вказується, що вперше загроза дезінформації з російського боку в онлайн-середовищі з'явилася у 2015 році. Навіть якщо Європейська комісія визнає, що кампанії дезінформації проводять понад тридцять країн, Росія виступає лідером в цьому напрямі, надаючи всім іншим можливість взяти на замітку її успішний досвід. Згідно з «Планом дій проти дезінформації», країни-члени та інститути ЄС повинні брати участь у різних аспектах спільної роботи, таких як протидія гібридним загрозам, кіберзагрозам, розвідка та стратегічні комунікації, захист даних, безпека виборів та взаємодія зі ЗМІ. Загалом пропоновані заходи Плану дій базуються на 4-х основних принципах:

- підвищення здатності ЄС виявляти та спростовувати дезінформацію;
- зміцнення можливостей спільного реагування на небезпеки;
- мобілізація приватного сектора;
- інформування громадян та підвищення стійкості населення до загроз.

План передбачає впровадження всіх необхідних заходів до травневих виборів до Європарламенту 2019 року. Саме ці вибори повинні були стати «лакмусовим папірцем» спроможностей ЄС з протидії дезінформації.

У рамках підготовки до цих виборів у лютому 2019 року Рада Європейського Союзу опублікувала рішення, в якому висвітлено важливість запобігання кіберзагрозам з метою забезпечення чесних та прозорих виборів. Документ визначає важливість проведення тижня медіаграмотності перед виборами, а також наголошує на необхідності співпраці з *G7* та НАТО у протидії дезінформації («Securing free and fair European elections: Council adopts conclusions», 2019). У червні 2019 року, після виборів, був опублікований звіт про виконання Плану дій («JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Report on the implementation of the Action Plan Against Disinformation», 2019). Цей документ став

підсумковим для всього процесу розвитку системи стратегічних комунікацій та боротьби з дезінформацією під час європейських виборів.

В документі акцентується, що вжиті заходи перед європейськими виборами для протидії дезінформації виявилися ефективними. З січня по червень *East StratCom* виявив та спростував 1000 випадків дезінформації, що вдвічі більше, ніж у порівнянні з аналогічним періодом попереднього року. Попри те, що *East StratCom* не виявив закордонних дезінформаційних кампаній, спрямованих на європейські вибори, звіт вказує на активність дезінформації з боку Росії. У звіті зазначається про введену в березні 2019 року «Систему швидкого реагування», призначену для оперативної взаємодії з *G7*, НАТО та онлайн-платформами щодо виявлення випадків дезінформації. Наразі ця система використовується для виявлення неправдивої інформації, що поширюється в Інтернеті щодо коронавірусу, зокрема неправильних методів лікування, які можуть призвести до серйозних наслідків для здоров'я (Stolton, 2020).

Ключовий акцент робиться на протидії дезінформації та фейкам, ціллю яких є дискредитація європейських інституцій та загалом стратегій ЄС та його держав-членів щодо протидії *COVID-19*. Зокрема, за оцінкою Європейської служби зовнішніх справ, такі міжнародні актори як Росія та Китай використовують для такої шкідливої діяльності державні ЗМІ та соціальні мережі, зокрема *X, Facebook* та інші. Слід зазначити, що результатом таких дій є не тільки інформаційна дезорієнтація громадян держав-членів ЄС, але й генерування глобального образу держав Заходу як «сповнених внутрішніх конфліктів» та «хаотичних». Протидія ЄС на цьому напрямі є не тільки частиною комплексної роботи з підтримки інформаційної гігієни в європейському інформаційному просторі, але й зосереджена на захисті західних ліберально-демократичних цінностей та стратегічної привабливості ЄС як успішної моделі колективної співпраці (Danylenko & Fursai, 2022, с. 19-45).

Також, згідно зі звітом, *Google* вжив заходів щодо більш ніж 130 тис. європейських акаунтів, щодо яких було зафіксовано порушення правил розміщення реклами. *Facebook* зафіксував 1,2 млн таких випадків і заблокував 2,2 млрд

фейкових акаунтів, а також перешкоджав роботі 1,5 тис. неєвропейських та 658 європейських сторінок, груп та акаунтів, націлених на європейців, та підвищив прозорість рекламних кампаній. Соцмережа *X* відхилила понад 16 тис. рекламних оголошень, націлених на громадян Європейського Союзу (*The EU's Cybersecurity Strategy for the Digital Decade*, 2020).

Серед інших ініціатив, які мають підтримку ЄС у протидії дезінформації, слід відзначити *SOMA* та Міжнародну мережу перевірки фактів (*International Fact-Checking Network*), яка нещодавно розпочала роботу європейського відділення. Також слід відмітити створення Євросоюзом системи швидкого оповіщення (*RAS*), яка представляє собою ключовий елемент загального підходу ЄС до протидії дезінформації. Ця система є конкретною реалізацією одного з чотирьох основних напрямків, визначених у «Плані протидії дезінформації», що був затверджений Європейською Радою у грудні 2018 року. *RAS* – це цифрова платформа, яка надає можливість членам ЄС обговорювати випадки дезінформації, реагувати на них та взаємодіяти з представниками влади кожної країни («Factsheet: Rapid Alert System», 2019).

Беззаперечно революційним кроком ЄС у впровадженні власної політики інформаційної безпеки стало прийняття у 2022 році Акту про цифрові послуги (*Digital Services Act – DSA*). Його основна мета: забезпечення для власних громадян більш безпечного цифрового простору шляхом суворішого регулювання роботи інформаційно-технологічних компаній, таких як *Google*, *Facebook* чи *TikTok*. Зокрема, тепер компанії, які мають щомісячну аудиторію у щонайменше 45 млн користувачів, зобов'язані посилювати контроль за поширенням дезінформації, мови ворожнечі або пропаганди тероризму. За невиконання цих зобов'язань компанії ризикують отримати штраф у розмірі 6% загального світового доходу або ж їх діяльність може бути взагалі заборонена в ЄС. Уже з лютого 2024 року ці зобов'язання поширюються на компанії з меншою за 45 млн користувачів аудиторією.

До того ж компанії тепер зобов'язані зробити публічною інформацію про те, як вони технічно протидіють дезінформації, надавати доступ незалежним

аудиторам для перевірки своєї роботи. Серед нововведень також запровадження механізму відмови користувача від використання соцмережею алгоритму рекомендацій, заснованому на оцінці релігійних, політичних вподобань чи на основі раси (Freedman, 2023).

Слід зазначити, що Єврокомісія уже задіює механізми *DSA* на практиці. Зокрема, у 2023 році запущено формальну процедуру оцінки дій соцмережі *X* щодо боротьби з дезінформацією та поширення нелегального контенту. Так, попередні висновки свідчать, що соцмережа не здійснила обов'язкових кроків з видалення незаконного в ЄС контенту руху ХАМАС, а також має проблеми із забезпеченням прозорості власної роботи («Commission opens formal proceedings against X under the Digital Services Act», 2023). У разі доведення провини соцмережі загрожує заборона роботи у всіх державах-членах ЄС (O'Carroll, 2023).

Підсилює *DSA* прийнятий того ж року Акт про цифрові ринки (*Digital Markets Act – DMA*). За допомогою цього документу ЄС планує забезпечити рівні та справедливі умови для розвитку інновацій та конкурентоспроможності через регулювання так званих «брамників» (*gatekeepers*), тобто онлайн-платформ, які стали основним каналом для своїх бізнес-користувачів в охопленні споживачів. Цей набір правил фактично розмежовує, що дозволено і що заборонено робити «брамникам» стосовно рекламних послуг, пошукових систем. Наприклад, «брамники» будуть зобов'язані утриматись від надання преференцій власним продуктам перед подібними конкуруючими продуктами, надавати можливість видалити попередньо встановленні застосунки чи зробити таргетовану рекламу прозорою та не поширювати її на дітей («Акт про цифрові послуги (DSA) та Акт про цифрові ринки (DMA): нові підходи ЄС до регулювання Інтернет-посередників», 2022).

Як ми бачимо, ЄС вдалося розбудувати потужний механізм інформаційної діяльності, що підкріплюється стратегічними документами, такими як «План дій з боротьби з дезінформацією» та «Зведення правил щодо протидії дезінформації». З'явилися нові міжурядові та неурядові установи, такі як *SOMA*, *RAS* і Центр

передових технологій, які спроможні вживати заходи для інформаційного захисту. *East StratCom* успішно виявляє значну кількість випадків дезінформації.

Також ЄС реалізує свою політику в сферах інформації та комунікацій через спеціалізовані структури, такі як Європейська Рада, Генеральний Директорат з інформаційного суспільства, Європейська комісія, Форум інформаційного суспільства ЄС, Генеральний Директорат з освіти та культури, а також через спеціалізовані інформаційні центри як у країнах-членах організації, так і поза її межами. ЄС має свій регульований інформаційний простір, який в основному наповнюється контентом національних ЗМІ, що діють як національно, так і на загальноєвропейському рівні, а також матеріалами, розміщеними у соціальних мережах. Проте, окрім регулювання інформаційного простору в межах єдиної аудіовізуальної політики, ЄС проводить заходи в інформаційному просторі з метою забезпечення безпеки своїх громадян і підтримки ліберально-демократичних цінностей. Це охоплює діяльність терористичних організацій, а також внутрішні та зовнішні загрози з боку інших країн та політичних сил.

Однак, результати вимагають об'єктивної оцінки, оскільки представники бізнесу та органів ЄС оцінюють ефективність нової системи співпраці по-різному. Головна мета – створення системи захисту європейських громадян та демократії від дезінформації – була досягнута, проте важливо провести критичний аналіз отриманих результатів.

Фонд Карнегі проводить оцінку заходів з боротьби з дезінформацією в рамках своєї програми партнерства з протидії кампаніям щодо впливу («Countering Influence Operations», 2024). Дослідження Фонду спрямовані на розробку рекомендацій з інформаційної політики, вивчення принципів операцій з впливу та зміцнення партнерства з урядовими та неурядовими установами. У травні 2018 року, перед виборами в Європарламент, Фонд оприлюднив дослідження щодо російського втручання та реакції Європи на фейкові новини та кібератаки (Brattberg & Maurer, 2018). У дослідженні акцентується увага на тому, що виборчу систему слід розглядати як критичну інфраструктуру, а також висвітлені п'ять випадків російського впливу на вибори в різних країнах. Дослідження вказує на різні рівні

впливу, такі як формування переваг виборців, вплив на процес голосування та явку виборців. Об'єктами впливу є ЗМІ, соціальні мережі, бази даних, канали передачі, організації та відповідальні особи. Дослідження також наголошує на тому, що система кібербезпеки повинна бути розроблена за участю урядових та неурядових організацій, спрямована на ці напрямки. Сучасна система інформаційної безпеки ЄС дозволяє вживати ці заходи, уникаючи необхідності відмовлятися від електронних носіїв, як це сталося у Нідерландах, коли під час парламентських виборів, які були проведені в березні 2017 року, виборчі комісії, побоюючись атак хакерів, підраховували результати голосування вручну (Chan, 2017).

У березні 2020 року Фонд Карнегі також випустив дослідження щодо ефективності «Зведення правил боротьби з дезінформацією», опубліковане Євросоюзом у 2018 році (Pamment, 2020). У ньому повідомляється, що цей документ привів до неоднозначних результатів, тому не всі учасники залишилися ними задоволені, а довіра між урядами, підприємствами, громадянським та науковим товариствами не була розбудована.

Досягнуті позитивні ефекти не вимагали значних зусиль. Серед них: розпізнавання та збір політичної реклами з даними про кампанії; відкритість даних; розпізнавання неточної інформації; розвиток практики з перевірки фактів; підготовка журналістів за програмами комерційних платформ; підвищення медіаграмотності завдяки діяльності платформ.

Фонд Маршалла також досліджував цю тему. Він пропонує десять принципів, які слід прийняти європейцям для боротьби з інформаційними загрозами:

- посилення взаємодії з НАТО для розробки заходів щодо спільної протидії іноземному втручанню;
- захист принципів та інститутів демократії, залучення громадян до участі у політичному процесі;
- посилення заходів протидії інформаційним загрозам;

- підвищення прозорості та підзвітності в інформаційно-технологічному секторі, але за обов'язкової умови збереження анонімності даних про користувачів;
- поглиблення взаємодії з приватним сектором;
- посилення контролю над фінансовою активністю та запобігання спонсоруванню операцій дезінформації в Європі;
- контроль за іноземним інвестуванням у критичні сектори європейської економіки;
- підтримка місцевих та незалежних ЗМІ;
- інформування населення про іноземне втручання;
- деполітизація підходу боротьби з іноземним втручанням (Berzina, Kovalčíková & Salvo, 2019).

Не слід забувати про когнітивну стійкість, тобто здатність населення критично і грамотно сприймати інформацію. Згідно дослідження *Eurobarometer*, проведеного у 2022 році, тільки 2/3 населення ЄС вважають, що здатні розпізнати дезінформацію (див. Додаток В). Традиційні ЗМІ також переживають кризу довіри споживачів через засилля фейків – так, державне телебачення та радіостанції користуються найбільшою довірою європейців серед інших ЗМІ, але водночас їм довіряють тільки половина європейців (див. Додаток Г) («Media & News Survey 2022», 2022).

У контексті цього важливо відзначити, що через виявлення та спростування дезінформації населенню та підвищення медіаграмотності можна сформувати здатність самостійно відокремлювати правдиві новини від хибних. Водночас не слід проводити диктаторську політику і забороняти будь-які інформаційні канали, оскільки це підриває довіру до влади, якщо не йдеться про екстрені заходи. Потік інформації має бути відкритим, але вона вся має проходити перевірку на правдивість у структурах ЄС та безпосередньо самими громадянами. Для ЄС довгий час існували загрози з боку російських урядових ЗМІ, перш за все, каналу *Russia Today*. Проте у цій сфері оцінка результатів – дуже складний процес. Поки що можна спиратися лише на опитування та кількість виявлених випадків

дезінформації. Наразі мовлення каналу *Russia Today* на території ЄС обмежене в рамках відповідного санкційного режиму Єросоюзу щодо Росії за її протиправні інформаційні операції, спрямовані на дестабілізацію ситуації в Європі.

Як зазначається у звітах, для ЄС виникали складні ситуації з російським інформаційним впливом: незаконна анексія Криму, навчання НАТО у державах Балтії, «справа Скрипалів», міграційна криза, катастрофа *MH17*. Завдяки ним можна дати оцінку ефективності стратегічних комунікацій ЄС та його здатності відповідати на загрози («CHAPTER 3 HEARTS AND MINDS: Enhancing societal resilience against disinformation», 2019).

Загалом механізми роботи в інформаційному просторі високорозвинені в ЄС, проте їхня ефективність могла б зрости за більш централізованої координації – наразі ініціативи мають ситуативний характер. Відповідно до цього законодавчо побудована і система інформаційної безпеки – вона спрямована на захист виборів та демократії, що не відповідає усім потребам у довгостроковій стратегії. Зокрема, один із факторів, який видозмінює стратегічну візію розвитку політики інформаційної безпеки ЄС, є повномасштабне вторгнення Росії в Україну та збільшення масштабів гібридної війни Кремля проти Заходу.

Враховуючи це та беручи до уваги євроінтеграційний поступ України, важливим в контексті руху України до членства в ЄС є акцентування на інформаційній безпеці як однієї з базових сфер співпраці. Уже сьогодні це можна відобразити шляхом вдосконалення Угоди про асоціацію, підписаної в 2014 році, що зумовлює потребує її адаптації до сучасних викликів та загроз.

2.2. Безпекова політика НАТО в сфері протидії деструктивному інформаційному впливу

Кіберзагрози для безпеки Альянсу є складними та руйнівними, і вони стають все більш поширеними. Кіберпростір завжди є ареною боротьби і щоденно ми стаємо свідками зловмисних кіберподій, починаючи від простих атак до

технологічно вишуканих. НАТО та її члени активно посилюють здатність Альянсу виявляти, запобігати та реагувати на зловмисну кібердіяльність. Організація розглядає кіберзахист як ключовий елемент для виконання трьох основних завдань. А саме:

1) оборона та стримування;

2) запобігання і врегулювання різноманітних криз;

3) забезпечення спільної безпеки.

Альянс прагне бути готовим захищати свої мережі та операції від дедалі складніших кіберзагроз, з якими він стикається.

Вперше Північноатлантичний альянс позиціонував питання кіберзахисту як один з напрямків своєї роботи на саміті Альянсу в Празі в 2002 році. Це було зумовлено різким загостренням міжнародної ситуації, викликаної подіями 11 вересня 2001 року, коли терористи угруповання «Аль-Каїда» атакували Всесвітній торговий центр в Нью-Йорку (США). Необхідність посилення безпекової складової НАТО, зокрема здатності Альянсу протидіяти кіберзагрозам, була безальтернативною в нових умовах («Prague Summit Declaration», 2002). Уже в рамках саміту 2006 року в Ризі союзники наголосили, що захист інформаційних систем потребує підсилення. Проте, ці два саміти стали тільки початком декларування Альянсом акценту на кіберзахисті («Riga Summit Declaration», 2006).

Безпосередньо до систематизації цієї роботи союзники перейшли в січні 2008 року, коли вони вперше затвердили Політику щодо кіберзахисту. Кібератаки на державні та приватні установи Естонії в 2007 році лише посприяли активізації роботи в цьому напрямку.

Уже в 2010 році на саміті в Лісабоні Альянс прийняв Стратегічну концепцію, яка вперше визначила, що кібератаки можуть досягти порогу, який загрожує національному та євроатлантичному процвітанню, безпеці та стабільності. Також, в рамках саміту союзники НАТО підкреслили свій намір удосконалити стратегічне партнерство з ЄС. Стратегічна концепція 2010 року зобов'язала Альянс більш тісно співпрацювати з іншими міжнародними організаціями у запобіганні кризам, врегулюванні конфліктів та стабілізації ситуацій після закінчення конфліктів.

Кожен наступний саміт НАТО ще більше збагачував цю співпрацю («Lisbon Summit Declaration», 2010).

У квітні 2012 року кіберзахист було включено до процесу оборонного планування НАТО. Відповідні вимоги до кіберзахисту було визначено та пріоритезовано в процесі оборонного планування («Strategic Concept 2010», 2010). Важливим для переосмислення кіберзахисту на рівні НАТО став саміт в Уельсі в 2014 році (Larsen, 2014). Саме тоді кіберзахист було визнано частиною основного завдання НАТО щодо колективної оборони, що означає, що кібератака може бути підставою для застосування Статті 5 установчого договору НАТО. Союзники також визнали, що міжнародне право застосовується в кіберпросторі («Collective defence and Article 5», 2023).

Робота НАТО на напрямку кібербезпеки не обмежується внутрішньоблоковими процесами. У вересні 2014 року НАТО запустила ініціативу «Промислове кіберпартнерство НАТО» (*NATO Industry Cyber Partnership (NICP*) для посилення співпраці з приватним сектором щодо кіберзагроз і викликів. *NICP* визнає важливість співпраці з галузевими партнерами, щоб Альянс міг досягти своїх цілей кіберзахисту («NATO launches Industry Cyber Partnership», 2014).

Щодо нормативного регулювання, то сьогодні ключовим документом, який визначає стратегію кіберзахисту НАТО є прийнята на саміті в Брюсселі в 2021 році «Комплексна політика кіберзахисту» (*Comprehensive Cyber Defence Policy*) для підтримки трьох основних завдань НАТО, а також його загальної позиції стримування та оборони. Зокрема, згідно цієї політики, НАТО має активно стримувати, захищатися та протидіяти повному спектру кіберзагроз у будь-який час – у мирний час, у кризі та конфлікті – на політичному, військовому та технічному рівнях. Члени Альянсу визнали, що вплив значної зловмисної сукупної кібератівності за певних обставин може розглядатися як збройний напад. Члени Альянсу також погодилися ширше використовувати НАТО як платформу для політичних консультацій між членами Альянсу, поділяючи занепокоєння щодо зловмисної кібератівності та обмінюючись національними підходами та відповідями, а також розглядаючи можливі колективні відповіді.

За останні роки НАТО та ЄС ще більше розширили свою співпрацю, зосередивши увагу на конкретних результатах та підвищенні безпеки громадян європейських країн. Важливість цього унікального та важливого партнерства ще більшою мірою була відзначена на Брюссельському саміті, де, окрім вище зазначеного, лідери країн Альянсу показали конкретні результати спільних дій щодо гібридних загроз та загроз у кібепросторі, стратегічних комунікацій та оперативного планування. Були продемонстровані також результати спільної діяльності з таких напрямків як проведення досліджень та навчань, боротьба з тероризмом та оборона, а також підвищення можливостей у сфері безпеки. Створення злагоджених, взаємодоповнюючих та оперативно сумісних оборонних можливостей залишається ключовим напрямом спільних зусиль двох організацій, спрямованих на підвищення безпеки. ЄС, як і раніше, є унікальним та найважливішим партнером НАТО. Стратегічне партнерство НАТО та ЄС є надзвичайно важливим для безпеки та процвітання європейських країн та євроатлантичного регіону («Brussels Summit Communiqué», 2021).

Також союзники працюють над тим, щоб посилити кіберзахист не тільки Альянсу, але й його держав-членів. На саміті у Вільнюсі в 2023 році НАТО також запустила ініціативу «Спроможність підтримки віртуальних кіберінцидентів» (*VCISC*) для підтримки національних зусиль із пом’якшення наслідків у відповідь на значні зловмисні кіберактивності. На тому ж саміті члени Альянсу ухвалили нову концепцію, яка акцентує важливість внеску кіберзахисту у загальну стратегію стримування та оборони НАТО. Ця концепція додатково інтегрує три рівні кіберзахисту в НАТО – політичний, військовий і технічний. Крім того, вона передбачає взаємодію з приватним сектором у випадках, коли це необхідно («Vilnius Summit Communiqué», 2023).

Сьогодні ключовою інституцією НАТО в питанні кібербезпеки є Центр кібербезпеки НАТО, розташований в Монсі (Бельгія). Альянс створив центр у 2018 році з метою захисту власної мережі, забезпечуючи централізовану та цілодобову підтримку з кіберзахисту. Ця здатність постійно розвивається, враховуючи швидкі

зміни у сфері загроз і технологічного середовища («New leader for NATO's Cyber Security Centre», 2023).

Також в Монсі в 2018 році Альянс відкрив Центр операцій в кіберпросторі (*Cyberspace Operations Centre*). Центр надає військовим командирам підтримку в ситуаційній обізнаності для інформування про операції та місії Альянсу. Він також координує оперативну діяльність НАТО в кіберпросторі, забезпечуючи свободу дій у цій сфері та роблячи операції більш стійкими до кіберзагроз. Центр також забезпечує ситуаційну обізнаність і координує оперативну діяльність НАТО в кіберпросторі. Також в системі НАТО працюють спеціалізовані Групи швидкого кіберреагування, які знаходяться у цілодобовій готовності, щоб в разі необхідності допомогти членам Альянсу («Cyber defence», 2023).

НАТО використовує різноманітні інструменти для поліпшення ситуаційної обізнаності та підтримки обміну інформацією між державними органами кіберзахисту в державах НАТО. Спеціальний Меморандум про взаєморозуміння встановлює механізми обміну різноманітною інформацією, пов'язаною з кіберзахистом, і надає допомогу для покращення запобігання кіберінцидентам, стійкості та можливостей реагування («NATO Agency, Oracle sign cyber information sharing agreement», 2019).

Також в структурі НАТО функціонує низка аналітичних установ, ціллю яких є дослідження існуючих кібервикликів та загроз, а також розробка рішень для їх усунення. Серед таких установ:

- Кооперативний центр передового досвіду кіберзахисту НАТО (*CCDCOE*) у Таллінні (Естонія) – акредитований багатонаціональний і міждисциплінарний центр кіберзахисту. Цей центр спеціалізується в питаннях освіти щодо кіберзахисту, на консультаціях, вивченні отриманого досвіду, а також на дослідженнях і розробках в цій сфері. Слід зазначити, що в *CCDCOE* функціонує «кіберполігон» на основі апаратно-програмних комплексів НАТО *Cyber Range CR14* і естонського *Cyber Range CR14.* Його завдання – розробка нових технологічних та інформаційних рішень для захисту інфосистем НАТО та збільшення кіберпотенціалу Альянсу для проведення власних кібероперацій.

- Академія зв'язку та інформації НАТО (*NCI*) в Оейрасі (Португалія) забезпечує підготовку персоналу країн-членів (а також країн, що не входять до НАТО) з експлуатації та обслуговування систем зв'язку та інформації НАТО.

- Школа НАТО в Обераммергау (Німеччина), що проводить різні тренінги та навчання з кіберзахисту.

- Коледж з питань оборони НАТО в Римі працює над формуванням стратегічної візії щодо військово-політичних питань, зокрема і щодо питань кіберзахисту («Cyber defence», 2023).

Окремо слід відзначити вплив повномасштабного вторгнення Росії в Україну як один із факторів переосмислення Альянсом власної кіберполітики. Це переосмислення знайшло своє відображення в прийнятому на саміті НАТО в Мадриді в червні 2022 року Стратегічного концепту (*Strategic Concept*). Цей документ визначає Росію найбільшою загрозою безпеці НАТО. Зокрема, зазначається, що Кремль активно використовує кіберпростір для атак на інформаційні системи держав-членів НАТО («NATO 2030 and the new Strategic Concept», 2022).

У відповідь НАТО проголосило курс на цифрову трансформацію, адаптацію командної структури НАТО до інформаційної ери та посилення кіберзахисту, мереж та інфраструктури. Зокрема, йдеться про підтримку інновацій та збільшення інвестицій у розвиток нових та революційних технологій, щоб зберегти взаємосумісність і військову перевагу країн-членів Альянсу. Також йдеться про спільну роботу та інтеграцію нових технологій, співпрацю з приватним сектором, захист інноваційних екосистем, формування стандартів та дотримання принципів, які відображають демократичні цінності та права людини («NATO 2022: Strategic Concept», 2022).

Від початку свого становлення у 1949 році НАТО постійно веде боротьбу з дезінформацією, яка є невід’ємною складовою стратегій та щоденних операцій організації. НАТО розглядає дезінформацію як навмисне створення та поширення неправдивої чи спотвореної інформації з метою введення в оману. Термін «дезінформація» використовується для охоплення різноманітних тактик, методів і

процедур, які відомі як «ворожа інформаційна діяльність». Ця діяльність націлена на збільшення розбіжностей усередині країн-членів НАТО, а також на ослаблення Альянсу в цілому (Paul & Matthews, 2016).

Діяльність Альянсу по протидії дезінформації включає низку операцій. А саме: моніторинг ЗМІ, аналіз інформаційного простору та активну комунікацію. У 2019 році НАТО затвердило оновлений і систематизований набір цілей та заходів для боротьби з дезінформацією. Так, наприклад, відповідь на дезінформацію щодо *COVID-19* була викладена в Плані дій, опублікованому Генеральним секретарем для членів Альянсу. Цей план був спрямований на об'єднання зусиль у протидії ворожій дезінформації навколо *COVID-19*, що свого часу охопила весь інформаційний простір (Chłoń, 2022).

У 2021 році був розроблений інструментарій НАТО для протидії ворожій інформаційній діяльності, який дотримується двох основних складових: взаємодія та розуміння. Цей інструментарій допомагає членам Альянсу оцінити ворожу інформаційну діяльність, включно з дезінформацією, та визначити шляхи дій. Крім того, НАТО регулярно брифінгує членів на військово-політичних комітетах щодо російської та іншої дезінформаційної діяльності.

Для успішного протистояння дезінформації важливо мати глибоке розуміння інформаційного середовища. З цією метою Альянс постійно відслідковує та аналізує інформацію, пов'язану з його діяльністю, відстежує та виявляє джерела дезінформації, аналізує ворожі наративи. Потенціал НАТО в оцінці інформаційного середовища базується на здібностях та професіоналізмі фахівців, використанні відтворюваних процесів та технологій, які спрямовані на використання загальнодоступної інформації для планування повідомлень, а також формування адекватної реакції на інформаційні загрози. Окрім аналізу дезінформації, цей потенціал дозволяє НАТО оцінювати ефективність своїх публічних повідомлень. Регулярний моніторинг та аналіз ЗМІ є одним із засобів, яким Альянс вдосконалює своє розуміння інформаційного середовища. Цей потенціал дозволяє НАТО не лише аналізувати дезінформацію, але й оцінювати ефективність публічних повідомлень. Постійний моніторинг та аналіз ЗМІ – один

із інструментів, завдяки якому НАТО покращує своє розуміння інформаційного середовища (Paul & Matthews, 2016).

Одним з ефективних засобів протидії дезінформації для НАТО – регулярний обмін інформацією. Шляхом відкритих, прозорих та чітких публічних повідомлень Альянс може своєчасно розкривати потенційну та фактичну дезінформацію, передбачати дезінформаційні наративи та запобігати їх поширенню. НАТО активно комунікує з громадськістю через різноманітні канали, включно з соціальними мережами, зв'язками з журналістами та власним офіційним сайтом. Альянс суворо дотримується принципу прозорості та регулярно публікує інформацію про свою діяльність. Наприклад, графік навчань НАТО та її країн-членів публікується заздалегідь (Exercises & Training, б. д.). Так, у НАТО було запущено інформаційну ініціативу щодо розвінчування російської дезінформації «Спростування російської дезінформації щодо НАТО». Вся інформація постійно оновлюється та публікується на офіційному сайті НАТО чотирма мовами, зокрема і російською («Зіставлення з реальними фактами: Спростування російської дезінформації щодо НАТО», 2024).

Також НАТО реалізує спеціальні комунікаційні ініціативи для привернення уваги аудиторії, яка не схильна відслідковувати діяльність Альянсу. Так, у межах кампанії «Захисти майбутнє» НАТО взаємодіє з молодими «контент-творцями», надаючи їм можливість побувати за лаштунками штаб-квартири, поспілкуватися з експертами та дізнатися з перших вуст про діяльність організації. Комунікаційні кампанії відіграють важливу, якщо не ключову роль у виявленні дезінформації («Protect The Future», 2024).

На додаток до цифрових та медійних повідомлень, НАТО веде пряму взаємодію з представниками країн-членів НАТО та країнами-партнерами (без членства в НАТО) з метою покращення розуміння громадськістю мети, цілей та політики діяльності Альянсу. Організація активно співпрацює з ЄС для використання переваг Системи швидкого оповіщення ЄС, розробленої для протидії дезінформації. Успіх колективного оборонного союзу НАТО напряму залежить від сили та рішучості країн-членів та союзників. Будь-які спроби маніпулювання чи

втручання в іноземну інформацію з метою послаблення союзників НАТО, а, отже, зниження здатності Альянсу захищати своїх членів, є великим викликом для Альянсу (Chłoń, 2022).

Втім, не дивлячись на ефективну політику інформаційної та кібербезпеки НАТО і країн ЄС, Росія посилює кампанії з дезінформації. З травня 2022 року і до сьогодні Росія проводить у країнах Європи, зокрема Україні, Німеччині, Франції, Великій Британії, Італії, державах Балтії масштабну дезінформаційну кампанію, яка має назву *Doppelgänger* (з нім. – «двійник»). Її ціль – дискредитація України в очах її європейських партнерів і, як наслідок, зниження рівня підтримки Києва у його протидії російській агресії (Alaphilippe, Machado, Raquel & Poldi, 2022).

Ключовий інформаційний метод, який Москва використовує для цього, – створення фейкових клонів вебсайтів авторитетних видань країн Європи. Зафіксовано уже як мінімум 18 сайтів-клонів таких видань, як *Bild* (Німеччина), *20minutes* (Франція), *Ansa* (Італія), *The Guardian* (Велика Британія), РБК-Україна (Україна). Для інформаційної підтримки таких клонів, Росія через такі структури як *Struktura* та *Social Media Agency* створила мережу фейкових аккаунтів в *Facebook*, *Instagram* та *X*, ціллю яких було поширення контенту з фейкових «сайтів-клонів» і, як підсумок, збільшення їх охоплення та інформаційного впливу. Також Росія створює мережу фейкових урядових сторінок (включно зі сторінкою НАТО), проросійських та антиукраїнських вебсайтів («Doppelganger operation», 2023).

Зазнала дезінформаційної атаки й інформаційна система Франції. Так, в червні 2023 року французький орган протидії іноземному впливу *Viginum* виявив ворожу інформаційну кампанію «*Doppelgänger*», яка ґрунтується на створенні клонів сайтів ЗМІ та урядових органів. Зокрема, було «клоновано» вебсторінку Міністерства Європи та закордонних справ Франції. Так, на ньому було опубліковано фейкове комюніке, в якому зазначалось, що Франція ввела так званий «безпековий податок» на значну кількість транзакцій, спрямованих на фінансову підтримку України. У такий спосіб Кремль намагався знизити рівень підтримки України французьким суспільством (*RRN. A complex and persistent information manipulation campaign*, 2023).

10 лютого 2023 року генеральний секретар НАТО Єнс Столтенберг, голова Європейської ради Шарль Мішель та голова Європейської комісії Урсула фон дер Ляйєн підписали спільну декларацію зі зміцнення співробітництва, зокрема для того, щоб протистояти загрозам з боку Росії. У спільній декларації Китай також названий викликом для безпеки. Єнс Столтенберг підкреслює, що нова декларація знаменує тіснішу співпрацю між НАТО та інститутами ЄС. До того ж нова декларація 2023 року розглядає питання щодо зовнішньої політики, розвитку космічних програм та захисту від дезінформації («Joint press conference by NATO Secretary General Jens Stoltenberg, President of the European Council Charles Michel and President of the European Commission, Ursula von der Leyen», 2023; «NATO and European Union leadership sign third joint declaration», 2023).

Так, ми бачимо, що Захід повинен розробити послідовну, комплексну та скоординовану стратегію для ефективної відповіді на російську дезінформацію. Країни повинні повністю використати потенціал НАТО, хоча національні відмінності у історії, регіональній безпеці, багатстві, освіті, якості медіа, політичній та правовій культурі, а також у поточному стані відносин з Росією можуть впливати на підходи різних країн. Практика реагування на дезінформацію вже існує і частково успішна в окремих країнах та євроатлантичних інституціях, але вона ще не перетворена на спільну політику чи стратегію. Національні політичні декларації та узгоджені плани дій не завжди виконуються повністю (Chłoń, 2022).

Протидія дезінформації стає більш актуальною в ЄС, і це відображається в Європейському плані дій для демократії та нових правилах для цифрових послуг. Акт про цифрові послуги (*DSA*) визначає нові правила для онлайн-платформ і встановлює обов'язки, які є більш вимогливими, ніж попередні добровільні зобов'язання. *DSA* передбачає співпрацю платформ з незалежними дослідниками, обов'язкові консультації з громадськістю, інститут довірених інформаторів і створення спеціальних органів для вирішення питань. Також передбачено встановлення спеціальної ради інформаційних послуг для координації заходів

національних координаторів цифрових послуг («The Digital Services Act (DSA)», б. д.).

В контексті сьогоднішньої безпекової ситуації важливо зазначити, що традиційні загрози залишаються пріоритетом, і колективна оборона залишається основною місією НАТО. Однак, з урахуванням еволюції загроз, нових ризиків, таких як дезінформація, слід приділяти належну увагу. Учасники переговорів щодо нової Стратегічної концепції НАТО повинні розробити повний спектр інструментів для нейтралізації цих нових загроз (Chłoń, 2022).

Для забезпечення ефективної відповіді на дезінформацію, учасники мають бути гнучкими під час розробки контрзаходів, оскільки загрози постійно змінюються. Ключовим завданням є забезпечення громадянської стійкості, наступальної і оборонної спроможності, а також мінімізація відмінностей в підходах країн-членів до протидії дезінформації.

Основні рекомендації для НАТО та інших організацій такі:

1. Громадянська стійкість: зосередження на підвищенні обізнаності громадян щодо дезінформації, надання освітніх ресурсів і навчання для виявлення та протидії дезінформації. Розвиток медіаграмотності серед громадян є важливим елементом.

2. Спроможність відповідати наступально і оборонно: зміцнення кіберспроможностей та здатності реагувати на кіберзагрози, включно з дезінформацією. Розробка та вдосконалення технічних інструментів для виявлення та аналізу дезінформації.

3. Мінімізація відмінностей: співпраця між країнами-членами НАТО та країнами ЄС для вироблення єдиної стратегії протидії дезінформації. Регулярні консультації та обмін досвідом можуть сприяти створенню єдиної лінії дій.

4. Міжнародна співпраця: посилення співпраці з іншими міжнародними організаціями та партнерами для обміну інформацією, координації контрзаходів і спільної реакції на дезінформацію.

Зазначена вище стратегія має забезпечити більш ефективний та координований підхід для протидії дезінформації. НАТО та ЄС, як міжнародні

організації, можуть відігравати важливу роль у протидії дезінформації, і це має бути відображено в їхніх стратегіях та політиках.

Окрім необхідності протистояти російським гібридним загрозам, НАТО також особливу увагу має приділяти внутрішній згуртованості блоку як фактору стабільності в євроатлантичному просторі. У цьому контексті чи не ключовим наразі є опрацювання Альянсом сценаріїв власного розвитку за умов ймовірного виходу з НАТО Сполучених Штатів Америки після перемоги Д. Трампа. Про високу ймовірність такого розвитку подій говорить колишній помічник президента США з питань національної безпеки Д. Болтон, який обіймав цю посаду в період президентства Д. Трампа. За його словами, екс-президент США, у разі свого обрання вдруге очільником США, «спробує вийти з НАТО», а саме НАТО «буде у значній небезпеці» у зв'язку з таким рішенням (Sciutto, 2024). Варто зазначити, що вихід з НАТО не є новою ідеєю Д. Трампа – ще у 2018 році, бувши президентом США, він активно обговорював зі своєю командою таку можливість як відповідь на недостатнє фінансування іншими державами-членами НАТО власного оборонного розвитку (Barnes & Cooper, 2019).

Враховуючи це та наявні статистичні опитування, які демонструють електоральну перевагу Д. Трампа над Д. Байденом (Wren & Allison, 2024), слід розглядати ймовірність виходу Штатів з Альянсу як серйозний ризик, реалізація якого здатна створити системні загрози для безпеки євроатлантичного простору. Для розуміння, частка американського фінансування військового, цивільного та інвестиційного бюджетів НАТО становить понад 16%, що є найвищим показником серед усіх держав-членів Альянсу («Funding NATO», 2024).

Також США безсумнівно є найпотужнішою військовою одиницею Альянсу, адже військовий бюджет Штатів у 2023 році склав майже 877 млрд доларів, що є найвищим показником у світі і становить 3,5% ВВП. Водночас найбільші європейські держави-члени НАТО – Велика Британія, Франція та Німеччина – разом витратили в 2023 році на оборону 178 млрд доларів, що майже в 5 разів менше витрат США («Military Spending by Country», 2024). Також, крім витрат на оборону, слід звернути увагу на присутність американських військових у Європі як

засіб стримування Росії та як гарантію безпеки партнерів, а також лідерство США у підтримці України як геополітичного форпосту оборони Європи. Усі ці фактори чітко демонструють, що будь-який рух США в напрямку від НАТО стане екзистенційним викликом для існування блоку та безпеки Європи зокрема.

Узагальнюючи, можна говорити про реальні ризики виходу США з НАТО, що напевне призведе до серйозних наслідків для Європи. А саме:

1. Зниження обороноздатності: США роблять один з найбільших внесків до оборонного потенціалу НАТО. Їх відсутність може призвести до зниження здатності Альянсу протистояти загрозам.

2. Послаблення об'єднаної підтримки: з виходом США може порушитися внутрішня солідарність НАТО, що послабить здатність Альянсу реагувати на загрози та конфлікти.

3. Збільшення впливу Росії: послаблення НАТО може створити простір для зростання впливу Росії в Європі та збільшення загрози для безпеки регіону.

4. Занепокоєння серед членів Альянсу: вихід США може викликати неспокій серед інших країн-членів НАТО, які розраховують на американську підтримку у випадку загрози, особливо в умовах активної фази російської агресії проти України.

Ймовірність такого розвитку подій актуалізує необхідність посилення геополітичної та безпекової суб’єктності Європи як компенсаторного фактору у випадку виходу США з НАТО. Лідерство у цьому процесі уже демонструє Париж, який прагне перехопити естафету у Вашингтона та стати новим ідейним безпековим лідером Європи. Зокрема, під час візиту у Китай в квітні 2023 року Е. Макрон наголосив, що Європа має уникати надмірної залежності від США та прагнути здобуття стратегічної автономності в геополітичній площині (Anderlini & Caulcutt, 2023).

Протестувати цю автономність європейці на чолі з Францією мають змогу уже зараз в контексті підтримки України у відбитті нею агресії Росії. Так, гальмування процесу виділення Україні 60 млрд доларів військової допомоги США прискорило роботу Європи з нарощування власного військового потенціалу та

збільшення своєї частки у військовій підтримці України. Зокрема, держави «Веймарського трикутника» – Франція, Німеччина та Польща – уже домовилися про спільне збільшення виробництва зброї для потреб України як відповідь на проблеми з наданням зброї Сполученими Штатами (Moulson & Gera, 2024).

Щодо ролі Франції, то її збільшення може мати багато важливих переваг не тільки для членів Альянсу, але й для усієї Європи. Насамперед це збільшення свого внеску у військові операції, адже Франція має один з найбільших потенціалів та досвід у цій сфері серед країн-членів Альянсу.

Також Франція відома своїм високим рівнем технологічного розвитку у різних сферах, зокрема в оборонній промисловості, протидії дезінформації та розвитку «штучного інтелекту». Уряд країни давно визначив ці напрямки як пріоритетні і докладає значних зусиль та інвестує кошти у розвиток відповідних технологій та інновацій. У сфері оборонної промисловості Франція виробляє високоякісну військову техніку та зброю, а також літаки, танки, кораблі та інше військове обладнання. Її оборонні технології широко визнані поза межами країни. Щодо протидії дезінформації, Франція активно розвиває методи та технології, зокрема і «штучний інтелект», для виявлення та боротьби з недостовірною інформацією та кіберзагрозами.

Отже, досвід П’ятої Республіки може посприяти впровадженню новітніх технологій та інновацій у військовій сфері НАТО, а сама держава може цілком впоратися з роллю лідера серед інших країн Європи в цьому напрямі.

Тому Україні слід максимально використовувати наявні в НАТО можливості для посилення власної спроможності захищати себе в інформаційному просторі. Робота у цьому напрямі уже ведеться. Так, у 2023 році Україна офіційно приєдналася до Кооперативного центру передового досвіду кіберзахисту НАТО («Україна офіційно приєдналася до Центру кіберзахисту НАТО», 2023), що дозволить налагодити більш тісну співпрацю з партнерами з Альянсу та обмінюватися досвідом реагування та протидії кіберзагрозам. Таке співробітництво критично важливе в умовах повномасштабної агресії Росії проти

України та незмінного курсу України на здобуття членства в Північноатлантичному альянсі.

2.3. Особливості та імплементація національних моделей політики інформаційної безпеки в Європі

Провідні держави Європи, які мають значний вплив на міжнародні відносини та встановлюють стандарти поведінки держав у різних сферах, активно ведуть політику в галузі інформаційної безпеки. Враховуючи систематичний інформаційний тиск з боку Росії, забезпечення інформаційної безпеки є стратегічним завданням для кожної країни Європи. Водночас європейські держави вживають заходів для захисту свого внутрішнього інформаційного простору від негативного втручання з боку Росії.

В умовах сучасного розвитку інформаційного суспільства, де проведення ефективної інформаційної політики є важливим завданням для всіх країн, які приділяють увагу своїй інформаційній безпеці, виникає необхідність розкрити її зміст, сутність та особливості проведення, взявши за основу досвід провідних країн світу. Це необхідно для вивчення найкращих практик та розробки ефективних механізмів забезпечення інформаційної безпеки в Україні.

Метою даного розділу є детальне дослідження пріоритетних напрямків політики інформаційної безпеки та механізмів їх впровадження на національному рівні, зокрема на прикладі досвіду Німеччини та Великої Британії.

Під час вибору цих країн для детальнішого дослідження ми спиралися насамперед на Індекс глобальної потужності (*GPI*), який був розроблений *Pareto Economics*. *GPI* – це індекс, який представляє рейтинг країн на основі їх деталізованого аналізу і який містить низку показників, зокрема оцінку споживацького ринку країн, військову та технологічну потужність, геостратегічне позиціювання, наявність системоутворюючих природніх ресурсів та фінансову силу. Вважається, що *GPI* є найбільш повним і актуальним аналізом глобалізованої

сили країни, який можна використовувати для прогнозування майбутнього розвитку країн і регіонів. Він призначений для надання допомоги інвесторам, компаніям та політикам у відстеженні та розумінні динаміки світової влади в реальному часі («Pareto Economics: About us», 2024). Відповідно до Індексу глобальної потужності, такі країни як Франція, Німеччина та Велика Британія у 2023 році увійшли у топ-10 країн світу з найвищим показником *GPI* («Global Power Index 2023 Report», 2024).

Слід відзначити й опубліковане у вересні 2022 року дослідження центру Белфера при Гарвардському університеті. За його результатами було систематизовано країни відповідно до Національного індексу кіберпотужності (*NCPI*). У проміжок з 2020 по 2022 роки *NCPI* акумулював в собі проаналізовані розмови та дебати між політиками, академічними колами та експертами галузі промисловості щодо концепції кіберпотужності та того, як держави можуть і будуть далі використовувати свої можливості для підвищення загальної здатності досягати національних цілей. Використання кіберпотужності держави вимагає загальнонаціонального підходу. Національні уряди повинні бути стурбовані не лише деструктивними операціями, шпигунством або підвищенням своєї кіберстійкості, а й зусиллями інших держав щодо стеження, контролю інформації, технологічної конкуренції, фінансових мотивів і формування того, що є прийнятним і можливим за допомогою норм і стандартів. Відповідно до *NCPI*, у 2020 році Франція, Німеччина та Велика Британія займають провідні позиції. У 2022 році ця тенденція залишається незмінною для Франції та Великої Британії (Voo, J., Hemani, I., & Cassidy, D., 2022).

Структура, яку забезпечує *NCPI*, є такою, що дозволяє нам обрати країну для дослідження та розглянути більш повний спектр викликів і загроз, а також ефективних практик та тенденцій. Об’єднання як якісних, так і кількісних моделей із більш ніж 1000 існуючими джерелами даних і 29 індикаторами для вимірювання спроможності держави є комплексним і являє собою якісний та більш точний показник кіберпотужності кожної країни.

Керуючись сучасними тенденціями та вище зазначеними метричними системами, дослідженнями, рейтингом Індексу глобальної потужності (*GPI*) та Національним індексом кіберпотужності (*NCPI*), ми обрали дві країни Європи для аналізу та порівняння, а саме Німеччину та Велику Британію, які будуть детальніше досліджено в цьому підрозділі.

Сьогодні Федеративна Республіка Німеччина, як і практично всі держави ЄС, стикається із суттєвими викликами інформаційній безпеці. Ці виклики мають тенденцію до трансформації в безпосередні загрози національній безпеці Німеччини, які федеральний уряд не може ігнорувати. Так, звіт про стан кібербезпеки в Німеччині за 2023 рік, підготовлений Федеральним відомством з інформаційної безпеки (*BSI*), свідчить про те, що загрози в кіберпросторі є надзвичайно складними. Зокрема, в 2023 році *BSI* фіксувало щодня понад 250 тис. нових варіантів шкідливого програмного забезпечення (ПЗ), а також щомісяця понад 2 тис. вразливостей в ПЗ, 15% з яких були критичними. Крім того, відомство щодня фіксувало понад 21 тис. інфікованих IT-систем державного та приватного сектору («The State of IT Security in Germany in 2023 at a Glance», 2023). Це вказує на постійне зростання рівня кіберзагроз та необхідність активних заходів для захисту інформаційної інфраструктури та забезпечення кібербезпеки («The State of IT Security in Germany», 2023).

Зокрема, програми-вимагачі залишаються найбільшою загрозою в сфері кібератак. Так, в 2023 році щомісяця реєструвалось щонайменше 2 атаки з допомогою програм-вимагачів на ресурси місцевого самоврядування та локального бізнесу (див. Додаток Г) («The State of IT Security in Germany in 2023 at a Glance», 2023). *BSI* виявляє зміни в характері атак: тепер у центрі уваги переважно вже не великі компанії з великими фінансовими резервами, а частіше малі та середні підприємства, установи місцевого самоврядування та муніципальні організації. У звіті зазначено, що успішні кібератаки на органи місцевого самоврядування та муніципальні підприємства можуть безпосередньо впливати на громадян, зокрема призводити до тимчасової недоступності соціальних сервісів або потрапляння особистих даних у руки зловмисників.

Так, наприкінці жовтня 2023 року невідома хакерська група атакувала інфраструктуру провайдера IT-послуг *Südwestfalen IT*, який оперує в західній Німеччині. Щоб унеможливити розповсюдження шкідливого програмного забезпечення в клієнтські системи, провайдер змушений був відключити доступ до мережі для понад 70 муніципалітетів, зокрема на території землі Північний Рейн – Вестфалія. Внаслідок цього низка муніципалітетів зупинили надання послуг для громадян, зокрема місто Зіген зупинило прийом усіх громадян, а більшість онлайн послуг були заблоковані для користувачів. Показово, що атака була здійснена в чутливий для муніципалітетів період – саме наприкінці місяця органи місцевого самоврядування Німеччини закривають власні фінансові транзакції (Antoniuk, 2023).

Крім цього, *BSI* відзначає, що кіберзлочинність стає дедалі більш професійною, використовуючи концепцію розподілу праці, зростаючу потребу в наданні послуг і тісну мережу між національними та галузевими кордонами. Із застосуванням підходу «кіберзлочинність як послуга» кіберзлочинці діють чимраз більш професійно, оскільки спеціалізація на конкретних послугах дозволяє їм цілеспрямовано розробляти та впроваджувати свої «послуги».

Також *BSI* зазначає, що уразливості програмного забезпечення знаходяться на чутливому рівні. Ці уразливості часто слугують точкою входу для кіберзлочинців у процесі компрометації систем та мереж. Щодня в середньому реєструється майже 70 нових уразливостей у програмному забезпеченні, що на чверть перевищує попередній звітний період. Зростає не лише кількість, а й потенційний негативний вплив цих уразливостей, приблизно кожна шоста з яких класифікується як критична.

Окремо *BSI* акцентує увагу на ризиках, які створює розвиток технологій генеративного штучного інтелекту (ШІ), зокрема таких сервісів як *ChatGPT*, *Bard* і *LlaMa*. Такі прості в користуванні інструменти відкрили можливості для використання ШІ в широких сферах, зокрема і в менш технічно орієнтованих користувачів. Однак, разом із цим виникає загроза їх використання зі злочинною метою. Наприклад, інструменти ШІ можуть створювати дедалі більш автентичні

дипфейки, ускладнюючи їх виявлення («The State of IT Security in Germany», 2023). Яскравим прикладом використання ШІ в таких цілях є створення та поширення в листопаді 2023 року невідомими зловмисниками відео дипфейку канцлера Німеччини Олафа Шольца. На цьому відео він начебто оголошує про рішення заборонити німецьку націоналістичну партію «Альтернатива для Німеччини» (*AfD*). Ціллю цієї публікації була дестабілізація соціально-політичної ситуації в Німеччині та дискредитація самого канцлера та його уряду («Deepfake video of German chancellor sparks angry reaction», 2023).

Також ШІ може підвищити рівень реалістичності фішингових електронних листів, сприяти кампаніям дезінформації в соціальних мережах або створювати шкідливий програмний код. Водночас сам штучний інтелект може стати об'єктом атаки та використовуватися для несанкціонованих цілей, що створює унікальні виклики для компаній і урядових структур («The State of IT Security in Germany», 2023).

Очевидно, що такі тенденції в німецькому кіберпросторі безпосередньо на собі відчуває суспільство. Зокрема, згідно з дослідженням міжнародної страхової компанії Hiscox, проведеного в 2023 році, 58% німецьких компаній зазнавали минулого року однієї або декількох хакерських атак, що на 12 відсоткових пунктів більше, ніж у 2022 році. Близько 43% цих компаній відчували фінансові труднощі через ворожі кібердії, зокрема їх кошти переводилися на рахунки зловмисників («Survey finds more than 50% of German companies victim of cyberattacks», 2023). Жертвами кібератак стають також прості громадяни Німеччини. Зокрема, показовим є кейс кібератаки на IT-систему Університетської лікарні в Дюссельдорфі в 2020 році. Паралізування електронних сервісів лікарні змусило її персонал зупинити прийняття викликів на надання невідкладної допомоги, а також реєстрацію нових пацієнтів, які звернулися за невідкладною допомогою. Внаслідок таких дій одна з громадянок ФРН, яка потребувала невідкладної допомоги, була перенаправлена до іншої лікарні, яка знаходилася за 32 км від Університетської клініки. Як наслідок, втрата дорогоцінного часу для надання допомоги призвела до смерті цієї людини. Цей приклад яскраво демонструє наскільки руйнівними

можуть бути кібератаки на соціальну інфраструктуру для пересічних громадян (Silomon, 2020).

Ще одним фактором, який характеризує сучасну інформаційну ситуацію в ФРН, є вплив російської загарбницької війни проти України на систему інформаційно-технологічної безпеки Німеччини. Варто відзначити, що *DDoS*-атаки, які були проведені проросійськими активістами і зареєстровані *BSI*, поки що майже не завдали значної шкоди. Як приклад можна навести минулорічну *DDoS*-кібератаку проросійської групи *Killnet* на сайти урядових структур, аеропортів, банків. Атака була відповіддю на рішення федерального уряду надати Україні танки *Leopard*. Незважаючи на масованість та складність атаки, вона змогла внести збій у роботу ресурсів тільки на кілька годин, що не створило критичних системних проблем для Німеччини (див. Додаток Ґ) (CONSTANTINESCU, 2023).

Наразі *BSI* класифікує переважну більшість інформаційних інцидентів з боку Росії як пропаганду, спрямовану на створення невизначеності та підрив довіри до державних інституцій («The State of IT Security in Germany», 2023). Прикладом такої дезінформаційної, пропагандистської операції була кампанія «*Doppelgänger*» в соцмережі *X*, яка проводилася з грудня 2023 року по січень 2024 року. Зокрема, проросійські ботоферми створили понад 50 тис. фейкових аккаунтів, які поширювали неправдиву інформацію про допомогу Україні та критикували офіційний Берлін за підтримку України. Ціллю цієї кампанії був зрив німецької допомоги та дестабілізація ситуація в самій Німеччині (див. Додаток Д) (Conolly, 2024).

У суспільстві, яке дедалі більш переплетене мережею, не може існувати абсолютного захисту від атак на IT-інфраструктури та пристрої, що використовують програмне забезпечення. Однак, найкращим засобом захисту від таких атак є кіберстійкість, яка передбачає підвищення стійкості IT і здатність більш ефективно протистояти атакам. Щоб зробити IT-системи більш стійкими та відбивати атаки, а також пом'якшувати наслідки успішних атак, необхідні кваліфіковані експерти з безпеки. Професіоналізація в сфері кіберзахисту, через стандартизацію, централізацію та автоматизацію, відіграє ключову роль у

підвищенні захисту. Держава та громадянське суспільство не є беззахисними перед різноманітними кіберзагрозами, але зможуть успішно протистояти їм завдяки підтримці Федерального відомства з інформаційної безпеки (*BSI*) («The State of IT Security in Germany», 2023).

Якщо говорити безпосередньо про регулювання Німеччиною протидії інформаційним загрозам, то базовим законодавчим інструментом боротьби федерального уряду з дезінформацією є прийнятий у 2017 році «Закон про захист прав у мережі» (*Netzwerkdurchsetzungsgesetz – NetzDG*), який ще також називають «Закон про *Facebook*». Він встановлює чіткий механізм видалення з соцмереж фейкових новин та іншого незаконного контенту. Йдеться про матеріали, які містять мову ненависті, закликають до насилля. Зокрема, такі соцмережі як *Facebook*, *Google*, *Instagram* зобов'язані прибрати такий контент протягом 24 годин з моменту подання скарги користувачем. Це правило також поширено на соцмережу *Telegram*. У випадку, якщо незаконність контенту не є очевидною, соціальній мережі надається 7 днів на проведення розслідування та видалення його. Невиконання цих вимог може призвести до накладення штрафу на соціальну мережу на суму до 50 млн євро («Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)», 2017).

Посилює цей закон Міжземельна угода про медіа, яку підписали у квітні 2020 року очільники усіх земель ФРН. Вона встановлює чітку регуляторну рамку для сфери телемовлення, ключовим принципом якої є плюралізм думок та відкритість, доступність ринку. В ній, зокрема, наголошується на рівних можливостях для роботи громадських і приватних медіа, встановлюється механізм боротьби з фейками тощо. Цей документ є важливим ще й тому, що сфера ліцензування медіа у Німеччині децентралізована, що викликано федеративним устроєм держави – в кожної землі можуть бути свої правила. Саме тому вкрай важливою є координація та синхронізація правил між різними землями, що дозволить створити уніфікований підхід до боротьби з інформаційними загрозами («Interstate Media Treaty (Medienstaatsvertrag)», 2020).

Додатковим юридичним інструментом є використання статті Кримінального кодексу, спрямованої проти розпалювання ненависті. Ця стаття дозволяє судити тих, хто поширює дезінформацію та антисемітизм, враховуючи також заперечення Голокосту («Strafgesetzbuch», б. д.).

Іншим важливим документом є прийнятий у грудні 2022 року закон, який впроваджує Європейську директиву про захист викривачів (ЄС 2019/1937 – «Директива про викривачі» та що стосується захисту викривачів («WHISTLEBLOWING: THE GERMAN PARLIAMENT PASSES THE WHISTLEBLOWER PROTECTION ACT», 2022). Проте, деякі організації винесли справу до суду після того, як федеральний парламент Німеччини в червні минулого року, в рамках реформи Закону про захист конституції, дав дозвіл усім спецслужбам використовувати шпигунське програмне забезпечення для вторгнення в смартфони та комп'ютери (Biselli, 2023). Це дозволило їм записувати зашифровані повідомлення та дзвінки через популярні месенджери, такі як *Signal*, *Telegram*, *WhatsApp* і інші, що може суперечити захисту інформаторів.

Щодо кібербезпеки, то найновішим базовим на сьогодні регулюючим документом в ФРН є Акт ІТ-безпеки сфери (*German IT Security Act 2.0*), прийнятий в травні 2021 року. Він підсилює та допомагає *BSI* в реалізації політики інформаційної безпеки. Зокрема, він розширив можливості *BSI* з моніторингу федеральних інформаційних систем на предмет їх вразливості. Також організація отримала функцію захисту споживачів, що означає перетворення *BSI* в незалежний, консультативний орган для бізнесу та громадськості у питаннях ІТ-безпеки («Second act on increasing the security of IT systems (German IT Security Act 2.0)», 2021).

German IT Security Act 2.0 також спрямований на посилення роботи безпеки ІТ-систем та гармонізацію інших законів для протидії постійно зростаючому ландшафту цифрових загроз, таких як атаки програм-вимагачів. Він встановлює чіткі вимоги до федеральних органів та приватних компаній щодо захисту своїх ІТ-мереж, захисту конфіденційної інформації споживачів. Однак, компаніям і організаціям може бути важко виконувати цей комплекс правил і вимог

кібербезпеки. Штрафи за порушення можуть сягати до 20 млн євро або 4% річного світового обороту. Нещодавно такий штраф був накладений на *H&M* в розмірі 35 млн євро за незаконну обробку конфіденційних даних співробітників (Chin, 2023).

Як вже було зазначено вище, ключовим державним органом, відповідальним за інформаційну безпеку Німеччини, є Федеральне відомство з інформаційної безпеки (*BSI*), яке було створено у 1991 році. Воно відповідає за забезпечення інформаційної безпеки держави та бізнесу. А з прийняттям *German IT Security Act 2.0 BSI* також стало відповідальним за захист прав споживачів цифрової продукції, що фактично універсалізувало відомство.

Окрім цього, Федеральне відомство з інформаційної безпеки володіє компетенцією для аудиту компаній, які обслуговують державні IT-системи. У такий спосіб федеральний уряд створює додатковий інструмент фільтрації роботи кібербезпекових організацій на предмет їх якості надання послуг з покращення захисту державних IT-мереж.

На тлі агресії Росії проти України додатковою зоною відповідальності *BSI* став аналіз інформаційного простору щодо наявності загроз та ризиків внаслідок російської підривної діяльності. У разі виявлення таких *BSI* надає державним та приватним організаціям рекомендації щодо того, як убезпечити себе в кіберпросторі. Окрім цього, у схожих ситуаціях *BSI* покладається на міжвідомчу співпрацю та міжнародне партнерство («Timeline», 2022).

Іншою важливою інституцією є Національний центр кіберреагування (*Cyber-AZ*), заснований в 2011 році. Фактично цей центр є координаційною платформою для усіх федеральних інституцій, які відповідають за кібербезпеку, де вони можуть обмінюватися інформацією про кіберзагрози та, як наслідок, превентивно протидіяти їм («The National Cyber Response Centre», б. д.).

Також в федеральній системі функціонують спеціальні Команди реагування на кіберзагрози (*CERT-Bund*), які в режимі 24/7 відстежують ситуацію в кіберпросторі, здійснюють першу фіксацію кіберінцидентів та оперативно передають інформацію *BSI* та іншим відповідальним федеральним інституціям («Germany (DE)», 2021).

Окремо слід відзначити, що за мілітарну складову кібербезпеки Німеччини відповідають Збройні сили ФРН (Бундесвер) і Міністерство оборони, які своєю чергою тісно співпрацюють зі своїми союзниками, такими як Центр передового досвіду спільного кіберзахисту НАТО (*NATO Cooperative Cyber Defense Centre of Excellence*) («Federal Office for Information Security», б. д.).

Щодо оперативної боротьби з актами дезінформації або поширенням мови ворожнечі на інституційному рівні в Німеччині діє федеральна робоча група, завдання якої – боротьба з мовою ненависті в соцмережах. Оперативна група швидко розробила добровільні зобов'язання для різних соціальних мереж, таких як *Facebook*, *Google*, *X*, *Microsoft*, які приєдналися до Спільного Кодексу поведінки. Цей Кодекс закликає платформи вживати заходів для реагування на повідомлення про ненависть протягом 24 годин (Jankowicz & Pierson, 2020).

Варто зауважити, що федеральний уряд Німеччини у співпраці з приватним сектором та громадськістю розвинув розгалужену мережу фактчекінгових організацій, покликаних протидіяти дезінформації та спростовувати фейки. Серед таких організацій варто виділити:

- *CORRECTIV* – одна з провідних німецьких компаній з перевірки фактів, яка поєднує розкриття фейків із журналістськими розслідуваннями. Компанія підписала Кодекс принципів Міжнародної мережі перевірки фактів (*IFCN*) («Commit to transparency — sign up for the International Fact-Checking Network's code of principles», 2024). З моменту заснування у 2014 році *CORRECTIV* отримала понад 30 нагород за високоякісну журналістську роботу («CORRECTIV - Über uns», б. д.);

- *DPA-FACTCHECKING* – це підрозділ перевірки фактів провідного інформаційного агентства Німеччини *Deutsche Presse-Agentur* (*DPA*). Головна мета *DPA-FACTCHECKING* – сприяння впровадженню журналістського формату перевірки фактів як методу протидії дестабілізуючим суспільним подіям. Також *DPA-FACTCHECKING* має незалежну редакційну команду, яка професійно перевіряє факти, аналізуючи можливі неправдиві твердження. Редакція сама приймає рішення про публікацію – без редакторського впливу ззовні. *DPA-FACTCHECKING* також є перевіреним підписантом Кодексу принципів *IFCN*, що

вказує на високі стандарти відділу *DPA* у галузі перевірки фактів і розкриттю інформаційних міфів («Faktencheck bei dpa», б. д.).

- *ARD-Faktenfinder* є підрозділом німецького громадського мовника *ARD* з перевірки фактів. Хоча він не є членом Міжнародної мережі фактчекерів *IFCN*, загалом підрозділ дотримується високих стандартів і публікує матеріали про дезінформаційні наративи в Німеччині («ARD-FAKTENFINDER», б. д.);

- *BR24 #Faktenfuchs* – підрозділ перевірки фактів баварського громадського мовника BR, який також є членом Міжнародної мережі фактчекерів (*IFCN*) («#FAKTENFUCHS», б. д.);

- *AFP – Faktencheck* базується в Австрії, але також розвінчує дезінформацію, яка поширюється в Німеччині. *AFP – Faktencheck* також є членом Міжнародної мережі фактчекерів (*IFCN*) та має німецькомовний підрозділ перевірки фактів у французькому інформаційному агентстві *AFP* («AFP Faktencheck», б. д.).

Також в Німеччині існують спеціалізовані організації, які вивчають явище дезінформації, виокремлюючи ключові тренди та інформаційні загрози, виклики, які стоять перед Німеччиною. Зокрема, слід відзначити:

- *CeMAS* – центр моніторингу, аналізу та стратегії, який об'єднує міждисциплінарну експертизу щодо ідеологій змови, дезінформації, антисемітизму та правого екстремізму. Ця некомерційна організація активно стежить за актуальними подіями в різних тематичних сферах в режимі онлайн, використовуючи систематичний моніторинг центральних цифрових платформ з допомогою сучасних методів досліджень. Мета *CeMAS* – надавати інноваційний аналіз та рекомендації для подальших дій. Організація також надає консультації представникам громадянського суспільства, ЗМІ та політики, сприяючи прийняттю обґрунтованих рішень. Враховуючи свою експертизу, *CeMAS* виконує важливу роль у боротьбі з різними формами негативного впливу в онлайн-середовищі («About CeMAS», б. д.);

- *ISD Germany* – Інститут стратегічного діалогу – незалежна некомерційна організація, яка займається захистом прав людини та протидією тенденції зростання поляризації, екстремізму та дезінформації в усьому світі. Інститут

аналізує соціальні та політичні тенденції в німецькомовному світі з глобальної точки зору, зосереджуючись на «аналізі, порадах, діях» («ISD Geschichte», б. д.);

- *NEWSGUARD GERMANY* є німецьким підрозділом компанії NewsGuard, яка володіє журналістським та технологічним інструментарієм для оцінки довіри до новинних та інформаційних вебсайтів. Ця організація також відстежує дезінформацію в Інтернеті, працюючи в кількох країнах («About NewsGuard», б. д.).

Як ми бачимо, Федеративна Республіка Німеччина має розвинуту нормативну та інституційну базу в питаннях протидії кібервикликам та дезінформації. Водночас одна з провідних позицій ФРН у Європі, лідерство Берліну у загальноєвропейській стратегії з підтримки України у війні з Росією роблять Німеччину однією з ключових цілей ворожих інформаційних кампаній Кремля, що зобов'язує офіційний Берлін постійно вдосконалювати свою систему інформаційної безпеки та шукати нові рішення як для оборони, так і для контратакувальних дій щодо інформаційних агресорів.

Велика Британія, як і Німеччина та багато інших держав Європи, стикається з проблемою поширення фейкових новин і дезінформації. Згідно з дослідженням, проведеним британським медіа агентством *Newsworks*, 8 з 10 мешканців Великої Британії стикаються з фейковими новинами щодня, а понад половина (52%) зізнається, що була введена в оману хоча б один раз. 9% респондентів стверджують, що ніколи не були обмануті фейковими новинами (див. Додаток Е). Важливо, що кожен 10-ий респондент не перевіряє надійність онлайн-контенту, і це не може не турбувати, особливо з урахуванням загрози, яку становлять фейкові новини.

Щодо методів перевірки інформації, майже половина респондентів (46%) намагаються знайти схожі статті в медіапросторі, 35% – звертають увагу на авторитетність видання, і лише 31% – шукають інші ознаки достовірного повідомлення новин, наприклад ім'я автора новини або популярність новинного видання. Це підкреслює важливість медіа брендів та довіри до них в очах споживачів («Study: Over 80% of people in the UK regularly come across fake news», 2022).

Відповідно до офіційної статистики, підготовленої урядом Великої Британії у 2023 році щодо ситуації з кібербезпекою, приблизно третина компаній (32%) і чверть благодійних організацій (24%) стикалися з порушенням кібербезпеки або атаками за останні 12 місяців (див. Додаток Є). Великі підприємства найчастіше фіксують кіберпорушення чи кібератаки проти них, ніж малі підприємства – це стабільна ситуація, як показує щорічне опитування. Благодійні організації з високим рівнем доходу (56% з тих, чиї доходи становлять 500 тис. фунтів стерлінгів або більше) та з дуже високими доходами (76% тих, хто має 5 млн фунтів стерлінгів або більше) також мають значно більшу ймовірність реєструвати будь-які порушення чи кібератаки.

Щодо частоти кіберпорушень та кібератак, то дослідження показує, що за попередні 12 місяців 4 з 10-ти підприємств (40%) і така ж частка благодійних організацій (38%) зазнавали атак раз на місяць або частіше, а п’ята частина підприємств (21%), благодійних організацій (19%) стикаються з порушеннями чи нападами принаймні раз на тиждень. Останні 3 роки стабільна кожен третій бізнес стикався з кібератаками і кожна четверта благодійна організація (див. Додаток Ж) («Cyber security breaches survey 2023», 2023).

Як показує досвід Великої Британії в контексті протидії кіберзагрозам, такі кібератаки можуть мати катастрофічні наслідки. Наприклад, в липні 2017 року британська компанія з роздрібного продажу електро- та телеком-обладнання *Dixons Carphone* (сучасна назва – *Currys*) зазнала потужної кібератаки, внаслідок якої хакери отримали несанкціонований доступ до близько 10 млн персональних даних і майже 6 млн платіжних карток британців. Серед даних, до яких отримали доступ хакери: прізвище та ім’я покупців, їх фізична адреса проживання, номери кредитних карток тощо. Як згодом продемонструвало розслідування влади Британії, компанія не приділяла достатньої уваги посиленню власного кіберзахисту і не усувала існуючі уразливості в своїх IT-системах (Chin, 2024).

Окрім цієї атаки, з 2015 року Велика Британія піддавалась системним кібератакам на інформаційні ресурси політиків, державних та приватних інституцій, які здійснював «Центр 18» Федеральної служби безпеки Росії. В рамках

неї Росія використовувала інструменти фішингу, зламу сайтів, викрадення конфіденційної інформації з ціллю проникнення в політичну систему Великої Британії. Внаслідок цих атак російська сторона отримала доступ до значного обсягу конфіденційної інформації, зокрема торгівельних документів США та Великої Британії, які згодом «зливала» в інфопростір для соціально-політичного тиску на британську владу та загалом дестабілізації ситуації у Сполученому Королівстві (див. Додаток Ґ) («UK exposes attempted Russian cyber interference in politics and democratic processes», 2023).

Розуміючи всю складність наслідків неефективної політики інформаційної безпеки, Велика Британія активно продовжує розробку та вдосконалення комплексу заходів щодо протидії загрозам в інформаційному середовищі та посиленню своєї інституційної спроможності у сфері захисту інформаційної безпеки. Ще в 2011 році на Мюнхенській конференції з безпеки глава Форін Офіса У. Хейг заявив, що Велика Британія має намір активно сприяти пошуку відповідей на глобальні кіберзагрози і з цією метою співпрацюватиме з союзниками у Вашингтоні, Берліні, Парижі та Канберрі (Hague, 2011).

Національна кіберстратегія, прийнята у 2022 році, є базовим нормативним документом Великої Британії, який визначає основи політики інформаційної безпеки Сполученого Королівства. Зазначений стратегічний документ встановлює ключові напрямки та завдання для роботи у кіберпросторі з метою забезпечення безпеки та захисту національних інтересів.

Вперше національну кіберстратегію було прийнято у листопаді 2011 року, і кожні 5 років стратегія оновлюється відповідно до світових тенденцій та загроз («Cyber Security Strategy», 2011). Варто зазначити, що кожна кіберстратегія визначає кібератаки як найбільшу загрозу національній безпеці у всіх її аспектах, включно з економікою («National Cyber Security Strategy 2016 to 2021», 2016). У документі від 2016 року сформульовано амбітну мету – зробити Велику Британію невразливою щодо сучасних загроз у цифровому середовищі, а британські ініціативи – моделлю для глобальних зусиль з кіберзахисту.

Основний вектор роботи, який визначений у оновленій стратегії 2022 року, підкреслює намір Сполученого Королівства залишатися провідною кібердержавою, демократичною та відповідальною. Спрямованість на захист та просування власних інтересів у кіберпросторі визначається як ключовий компонент досягнення національних цілей. Це може містити заходи щодо кібербезпеки, посилення кібервійськових можливостей, захисту критичної інфраструктури та реагування на кіберзагрози. Ці цілі відображають стратегічні пріоритети для розвитку та безпеки країни, враховуючи сучасні технологічні, економічні та геополітичні виклики. Серед них такі:

1. Безпека та стійкість
   - створення більш безпечної та стійкої нації, орієнтованої на підготовку до нових загроз і ризиків;
   - використання кіберможливостей для захисту громадян від злочинності, шахрайства та державних загроз.
2. Цифрова економіка
   - розвиток інноваційної та процвітаючої цифрової економіки;
   - розподіл можливостей більш рівномірно по всій країні та серед різноманітного населення.
3. Науково-технічна наддержава
   - становлення науково-технічної наддержави, що використовує трансформаційні технології;
   - підтримка розвитку більш екологічного та здорового суспільства.
4. Глобальний вплив та партнерство
   - зміцнення впливу на глобальній арені;
   - активна участь у формуванні майбутніх меж відкритого та стабільного міжнародного порядку;
   - збереження свободи дій у кіберпросторі («National Cyber Strategy 2022», 2022).

Стратегія інформаційної безпеки, прийнята у 2022 році, ґрунтується на великому прогресі, досягнутому в рамках Національної стратегії кібербезпеки за

період 2016-2021 років. В інтегрованому огляді цієї стратегії викладено п'ять «першочергових дій», які Велика Британія використовує як основні цілі стратегічного плану. Вони визначають напрям і організацію конкретних дій, яких країна має намір досягти до 2025 року:

- зміцнення кібернетичної екосистеми Сполученого Королівства, інвестиції в людей і підготовку кваліфікованих кадрів, поглиблення партнерських відносин між урядом, науковими колами та галуззю;

- побудова у Сполученому Королівстві стійкої і процвітаючої цифрової економіки, зниження кіберризиків, що дозволить компаніям отримувати максимальні економічні вигоди від використання цифрових технологій, підвищення безпеки громадян в інтернеті і зміцнення їх впевненості в захищеності їх персональних даних;

- досягнення лідерства в галузі технологій, життєво важливих для кібердержави, нарощування промислового потенціалу та розробка механізмів, що забезпечують доступ до майбутніх технологій;

- зміцнення світового лідерства та впливу Сполученого Королівства з метою формування більш надійного та відкритого міжнародного порядку, співпраця з урядовими та галузевими партнерами, обмін досвідом і знаннями, на які спирається кіберпотужність Сполученого Королівства;

- виявлення, дезорганізація та стримування супротивників з метою зміцнення безпеки Сполученого Королівства в кіберпросторі та більш комплексне, креативне та рутинне використання всього спектру важелів, наявних у розпорядженні Сполученого Королівства («National Cyber Strategy 2022: Policy Paper», 2022).

Щодо боротьби з дезінформацією та фейками, то тут Велика Британія робить акцент на розвитку медіаграмотності серед населення. Так, згідно Стратегії онлайн медіаграмотності, прийнятої британським урядом в 2021 році, спеціальне навчання методам та інструментам розвінчування фейків пройдуть вчителі та інші працівники освітньої сфери, які згодом зможуть передати ці знання молодшому поколінню, яке є найбільш вразливим до дезінформації. Потреба в такій стратегії

викликана тим, що згідно соцопитування *Ofcom*, 40% дорослого населення Великої Британії не володіє навиками для розпізнавання фейків. Ще гірша ситуація з дітьми віком до 15 років. Британський уряд вбачає, що стратегічним рішенням цієї проблеми, окрім безпосередньо роботи з онлайн-платформами, де з'являються фейки, є розвиток у дітей критичного мислення як ключового фільтра від пропаганди («Minister launches new strategy to fight online disinformation», 2021).

Щодо безпосереднього регулювання сфери поширення інформації онлайн та боротьби з дезінформацією, то тут ключовим є Закон Великої Британії про онлайн безпеку (*Online Safety Bill*), який був прийнятий у 2023 році. Він посилює відповідальність великих інформаційних платформ, таких як *Google, X*, *Facebook*, *TikTok* тощо, за поширення неправдивого або шкідливого контенту.

Окрім очевидних «плюсів», зокрема примус компаній-адміністраторів таких платформ видаляти шкідливий контент (порнографія, фейки, пропаганда, контент з мовою ворожнечі, зображення знущань над людьми та тваринами тощо), закон містить і низку контроверсійних позицій. Так, він зобов'язує компанії-адміністратори месенджерів, таких як *Facebook Messenger*, *WhatsApp*, *Viber* тощо, інспектувати зашифровані приватні повідомлення користувачів на предмет виявлення контенту з жорстоким поводженням з дітьми. Така вимога закону ставить питання про збереження приватності користувачів, на чому наголошують компанії. Низка компаній уже заявили, що вони радше покинуть ринок Великої Британії, ніж змінять власну політику конфіденційності.

Водночас за системні порушення вимог *Online Safety Bill* великим компаніям загрожує штраф у розмірі 10% їх глобального доходу або фіксований штраф у розмірі 18 млн фунтів стерлінгів. Ба більше, керівництво компаній-адміністраторів онлайн- платформ може бути ув'язнене за особливо значні порушення вимог британського закону (Rahman-Jones & Vallance, 2023).

Ключовою інституцією Сполученого Королівства з питань забезпечення інформаційної безпеки, зокрема виміру кібербезпеки, є Національний центр кібербезпеки (*NCSC*), головною ціллю якого є кіберзахист критично важливих для Британії суб'єктів як державної, так і приватної форм власності. *NCSC* був

заснований в 2016 році та має свою штаб-квартиру в Лондоні («National Cyber Strategy 2022: Policy Paper», 2022; «About the NCSC», б. д.).

Центр об’єднує в собі досвід таких організацій:

- *CESG* (*Communications-Electronics Security Group*) – національний технічний орган з питань забезпечення безпеки інформації уряду Великої Британії. Його головна функція полягає в консультуванні організацій щодо методів захисту їхньої інформації та інформаційних систем від сучасних загроз. *CESG* відомий своїм експертним підходом до кібербезпеки та використовує свій технічний досвід для надання порад та рекомендацій щодо захисту інформації в урядових та комерційних секторах («CESG», б. д.);

- *CERT-UK* (*Computer Emergency Response Team – UK*) – це національна команда реагування на комп'ютерні надзвичайні ситуації у Великій Британії. Основні функції *CERT-UK* включають управління національними інцидентами кібербезпеки та готовність до реагування на них. Ця команда забезпечує координацію та взаємодію між різними суб'єктами у випадку кібератак чи інших надзвичайних подій в інформаційній сфері. *CERT-UK* спрямована на швидку та ефективну протидію кіберзагрозам та надання підтримки організаціям та урядовим структурам у реагуванні на кіберінциденти («UK launches first national CERT», 2014);

- Центру захисту національної інфраструктури, який у березні 2023 року став Національним органом захисту та безпеки (*NPSA*) («National Protective Security Authority», б. д.).

Серед основних функцій *NCSC* слід відзначити такі:

- забезпечення єдиної точки контакту для різних суб'єктів, таких як малі і середні підприємства, великі організації, державні установи, громадськість і департаменти;

- співпраця з іншими правоохоронними органами, оборонними органами, розвідувальними службами та службами безпеки Великої Британії, а також з міжнародними партнерами («About the NCSC», б. д.).

Одним із нових напрямків роботи *NCSC* стало дослідження можливих наслідків розвитку технологій «штучного інтелекту» та їх впливу на кібербезпеку Великої Британії. Згідно оцінки Національного центру кібербезпеки, опублікованої в січні 2024 року, «штучний інтелект» найімовірніше збільшить кількість та потужність кібератак в найближчі 2 роки. Однією з причин цього є те, що державні та недержавні суб'єкти, які систематично створюють загрози в кіберпросторі, уже активно використовують ШІ у власних операціях. Також у цьому контексті *NCSC* називає 2025 рік переломним, адже до цього року, за оцінкою центру, жоден суб'єкт не зможе використати ШІ для надскладної, комплексної кібератаки, проте уже в 2025 році і після нього розвиток технологій уже зможе дати користувачам ШІ суттєву перевагу під час кібероперацій («The near-term impact of AI on the cyber threat», 2024).

Також в структурі інституцій кібербезпеки Великої Британії варто звернути увагу на Національні сили кібербезпеки (*The National Cyber Force, NCF*) як інституцію, яка безпосередньо протидіє кібератакам. Заснована у 2020 році, організація відповідає за проведення операцій у кіберпросторі, спрямованих на протидію, підрив, ослаблення та боротьбу з діями тих, хто може завдати шкоди Сполученому Королівству або його союзникам, з метою зміцнення безпеки країни, а також захисту та просування інтересів Сполученого Королівства всередині країни та за її межами. До складу *NCF* входить персонал сил оборони та розвідки приблизно в рівному співвідношенні, що дозволяє об'єднати їхній досвід, ресурси та повноваження в рамках єдиної структури.

NCF забезпечують досягнення високих результатів діяльності в інтересах національної безпеки, таких як сприяння обороні, підвищення економічного благополуччя Сполученого Королівства та запобігання серйозним злочинам. Діяльність *NCF* охоплює широкий діапазон заходів – від тактичних дій до стратегічних заходів боротьби як з державними, так і з недержавними суб'єктами. Їхня діяльність поділяється на три основні категорії:

1) протидія загрозам з боку терористів, злочинців та держав, які використовують Інтернет для проведення транскордонних операцій з метою

заподіяння шкоди Сполученому Королівству та іншим демократичним суспільствам;

2) протидія загрозам порушення конфіденційності, цілісності та доступності даних та послуг у кіберпросторі;

3) підтримка британських оборонних операцій та допомога у здійсненні зовнішньої політики Сполученого Королівства (наприклад, реагування на гуманітарні кризи з метою захисту цивільного населення).

Операції *NCF* можуть використовуватися для впливу на окремих людей та груп, підриву онлайнових та комунікаційних систем та порушення функціональності фізичних систем. Цей вид діяльності часто називають наступальними кіберопераціями («National Cyber Strategy 2022», 2022).

До прикладу, Центр урядового зв'язку Великої Британії (*GCHQ*) вперше підтвердив факт проведення наступальних кібероперацій спеціалістами *NCF*. Попри те, що у звіті *GCHQ* не було уточнено, проти кого саме були проведені операції, проте у відомстві наголосили, що *NCF* підтримує військові операції проти терористичних угруповань, а також здійснює контрзаходи проти ворожих дезінформаційних кампаній, ціллю яких є втручання в демократичний процес всередині Британії. Щодо неназваних цілей операцій, то тут варто акцентувати увагу, що *GCHQ* виділила Іран та Росію як держави, які регулярно проводять операції з поширення дезінформації.

В контексті цього директор Центру урядового зв'язку Великої Британії Джеремі Флемінг заявив: «Щоб стати справді відповідальною кібердержавою у світі, що стає все більш нестабільним і взаємопов'язаним, держави повинні мати можливість змагатися та конкурувати з супротивниками в кіберпросторі». Це свідчить про готовність Лондона не тільки захищати власний інформаційний простір від зовнішніх та внутрішніх загроз, але й атакувати превентивно ворожі інформаційні сили (Gooding, 2023).

Слід зазначити, що операції *NCF* здійснюються відповідно до загальновизнаних правових норм, включно з Законом 1994 року про розвідувальні служби та Законом 2016 року про регулювання повноважень слідчих органів.

Сполучене Королівство раніше чітко заявляло, що воно розробляє та розгортає можливості відповідно до міжнародного права. Діяльність *NCF* підлягає затвердженню на міністерському рівні, судовому та парламентському нагляду, тому британський режим управління кібероперaціями – один із найсуворіших у світі («National Cyber Strategy 2022», 2022).

У серпні 2019 року у британських ЗМІ було оприлюднено дані про спеціальний підрозділ британської армії, до завдань якого увійшла боротьба з гібридними загрозами та кібератаками, які походять від різних терористичних угруповань. Діяльність нового підрозділу спеціальних кібероперацій, або 6-ої Дивізії (*6 Div*), виходить за межі звичайних кібероперацій у військовому контексті і зосереджується на повноцінній «інформаційній війні» в соціальних мережах. І тут основним супротивником є Росія, яка перетворила поширення фейкових новин і політичної пропаганди через основні соціальні медіа-платформи на стратегічний елемент національної безпеки.

Цей новий кібервідділ включає експертів з існуючих підрозділів спецназу з сильними кібернавичками, об'єднує ресурси наявних підрозділів, зокрема 1-ї та 11-ї бригад зв’язку та 1-ї бригади спостереження та розвідки. Тут використовується поєднання сил спеціального призначення та розвідувальних ресурсів, спрямованих на розвиток атак в кіберпросторі. Окрім того, *6 Div* також розширює свою мережу, намагаючись залучити нове покоління фахівців в сфері соціальних медіа (Doffman, 2019).

Ще однією організацією, яка займається протидією кіберзлочинам, є Національна мережа правоохоронних органів боротьби з кіберзлочинністю (*Law Enforcement’s National Cyber Crime Network*). Створена в період дії Національної стратегії кібербезпеки 2016–2021 року, організація розробила плани повномасштабного комплексного реагування на кіберзлочини і готова до розгортання заходів реагування на основі розвідувальних даних у відповідь на будь-які форми кібератак, які націлені проти людей, організацій та цілих секторів. Це національна система, що діє на національному, регіональному та місцевому рівнях. У її завдання входять надання підтримки постраждалим, надання допомоги

юридичним та фізичним особам у забезпеченні своєї безпеки та здатності до швидкого відновлення, а також підвищення дієвості кримінального правосуддя щодо злочинців.

Національний підрозділ боротьби з кіберзлочинністю (*NCCU*) у структурі Національного агентства боротьби зі злочинністю (*NCA*) виступає у ролі національного керівника та координатора діяльності з реагування на кіберзлочини. Він спирається на підтримку мережі спеціалізованих регіональних підрозділів з боротьби з кіберзлочинністю (*RCCU*), створених у кожному з 9-ти поліцейських територіальних округів Англії та Уельсу, та діє у партнерстві з колегами зі Служб поліції Шотландії та Північної Ірландії, підрозділом по боротьбі з кіберзлочинністю Служби поліції Лондона. До мережі також входять спеціалізовані місцеві підрозділи боротьби з кіберзлочинністю (*LCCU*), які є у складі кожної з 43 поліцейських служб, діяльність яких синхронізує регіональний координатор. Ці регіональні та місцеві підрозділи уповноважені здійснювати розслідування та переслідування правопорушників, допомагати компаніям та потерпілим захищати себе від кібератак, а також спільно з партнерами запобігати залученню вразливих осіб до злочинної кібердіяльності.

Поєднуючи системи з інноваційними можливостями криміналістичної експертизи, розвідки та обміну даними, Велика Британія створює єдину платформу, яка об’єднає усі регіональні та національні органи у сфері кібербезпеки. Ця платформа надає національним та регіональним підрозділам доступ до всіх спеціалізованих високотехнологічних засобів та інструментів, що перебувають у розробці. Серед можливостей – ефективне співробітництво з партнерами в структурах безпеки та розвідки, зокрема у сфері реагування на змішані кримінальні державні загрози. Керуючись принципом «створити один раз і назавжди, розробити національний рівень на користь всієї мережі боротьби з кіберзлочинністю», Велика Британія надає доступ місцевим підрозділам з боротьби з кіберзлочинністю через регіональних координаторів. Цей комплексний підхід вже забезпечує значно ефективнішу реакцію на кіберзагрози.

Мережа правоохоронних органів, що бореться з кіберзлочинністю, продовжить сприяти зміцненню кримінально-правових заходів проти кіберзлочинності на різних рівнях – міжнародному, національному, регіональному та місцевому. Окрім цього, будуть використовуватись різноманітні деструктивні методи, такі як:

- розробка спеціалізованих високотехнологічних розвідувальних та деструктивних кіберможливостей;
- використання широкої міжнародної мережі *NCA* для підтримки заходів, проведених партнерськими країнами, шляхом надання розвідувальних даних та фактичної інформації;
- перешкоджання отриманню кримінальними угрупованнями прибутку від їхньої діяльності шляхом позбавлення їх можливості користуватися кримінальними ринковими каналами та допоміжними сервісами;
- захист країн від кіберзлочинів шляхом порушення функціональності та руйнування інфраструктури, яку використовують для здійснення кіберзлочинів;
- конфіскація криптовалюти та інших активів, які є доходами від кіберзлочинів («National Cyber Strategy 2022», 2022).

В останні роки уряд Великої Британії активно впроваджує ініціативи з кібербезпеки, що спрямовані на підвищення кібергігієни та протидію кіберзагрозам. Серед цих ініціатив варто виділити «Інструкцію з 10 кроків», *Cyber Essentials* та *CISP*, що містять основні заходи, які різні організації можуть вживати для захисту своєї кібернетичної безпеки. *Industry 100* – ініціатива, яка сприяє взаємодії між громадськістю та приватним сектором для вирішення проблем та викликів у сфері кібербезпеки. *Exercise in a Box* – це онлайн-інструмент, призначений для визначення готовності та стійкості організацій до кібератак. Він також дозволяє практикувати реагування в безпечному оточенні.

Враховуючи сьогоднішні реалії, надзвичайно важливо, щоб як фахівці з безпеки, так і звичайні користувачі проходили навчання з кібербезпеки. Уряд Великої Британії запустив достатньо ефективних та робочих ініціатив та розробив

інструкції для надання допомоги окремим особам і організаціям у захисті їхньої кібербезпеки в Інтернеті (див. Додаток З) (Odebade & Benkhelifa, б. д.).

Дискурс, який використовує Лондон щодо протидії недостовірній інформації у традиційних та соціальних медіа, допомагає Великій Британії об'єднати навколо себе союзників на глобальному рівні (США, Канаду, Австралію та ін.) у рамках ініціатив із захисту ліберального світового порядку. Такі кроки відповідають курсу Лондона на «Глобальну Британію», здатну, за задумом «брекзитерів», забезпечити Сполученому Королівству провідні міжнародні позиції поза межами ЄС («Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy», 2021).

Новий прем'єр-міністр Британії Ріші Сунак, очевидно, продовжить лінію попереднього уряду щодо регулювання інформаційного контенту та заходів з посилення кібербезпеки Британії та її стратегічних партнерів. Так, наприклад, 12 січня 2023 року Велика Британія та Україна підписали Угоду про співробітництво у сфері безпеки. Основні положення документу стосуються співпраці між обома країнами з впровадження заходів для стримування інформаційної агресії та розкриття дезінформації, сприяння обміну розвідувальними даними та напрацювання спільного протоколу стримування та реагування на кібератаки з боку РФ, а також підвищення медіаграмотності серед громадян («Угода про співробітництво у сфері безпеки між Україною та Сполученим Королівством Великої Британії і Північної Ірландії», 2024).

Значна увага приділяється і регулюванню сфери розвитку та використання технології «штучного інтелекту». У листопаді 2023 року Велика Британія, США, ЄС та Китай, а також ще 25 держав світу підписали першу декларацію про небезпеку ШІ. Країни-підписанти погодилися з тим, що ШІ становить потенційну небезпеку для людства. Двадцять вісім країн підписали Декларацію Блетчлі під час саміту з безпеки кіберпростору, який було проведено в Лондоні. Угода передбачає спільні дослідження в галузі кібербезпеки, навіть за умови конкуренції між США та Великою Британією за лідерство в цій галузі. Окрім цього, декларація визначає безпечне, людиноцентричне та відповідальне використання ШІ як базовий

принцип розвитку і використання технології. Для цього держави взаємодіятимуть з бізнесом, науковим середовищем, громадськістю, а сам процес розвитку технології має бути прозорим та інклюзивним («The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023», 2023).

У грудні 2023 року, в британському ЗМІ було опубліковано інформацію про наміри уряду країни розробити «надійні механізми», щоб зупинити поширення дезінформації за допомогою ШІ вже до початку наступних загальних виборів, проведення яких заплановане не пізніше січня 2025 року (Landi, 2023).

Як ми можемо спостерігати, попри наявність доволі розгалуженої мережі державних інституцій для боротьби з кіберзагрозами та дезінформацією, а також розвинуту нормативно-правову базу щодо регулювання цих сфер, Берлін та Лондон продовжують працювати над адаптацією політики інформаційної безпеки до сучасних інформаційно-технологічний реалій. Зокрема, одним із ключових рушіїв процесу адаптації є агресія Росії проти України, активне використання Кремлем інформаційного простору для проведення своїх кібероперацій та пропагандистських кампаній. Крім того, Велика Британія та Німеччина спільно працюють над унеможливленням використання сучасних технологій, зокрема ШІ в створенні та просуванні ворожих інформаційних операцій, ціллю яких є дестабілізація соціально-політичної ситуації в Європі. Зазначимо, що у вдосконаленні безпекової інформаційної політики обидві держави активно співпрацюють з Францією, виступаючи єдиним фронтом у боротьбі з дезінформаційними наративами та кібератаками.

Висновки до Розділу 2

Інформаційна безпека стала критичним аспектом як національної, так і міжнародної безпеки в сучасному цифровому світі. Її значення зросло через розвиток інформаційних технологій, збільшення кількості даних, що обробляються, і загальний вплив цифрового середовища на всі сфери життя.

Серед ключових аспектів інформаційної безпеки на рівні національної політики можна виокремити такі:

- кіберзахист – захист інформаційних систем та мереж від кібератак, що є першочерговим завданням національної інформаційної безпеки. Розвиток та впровадження ефективних кіберзахисних стратегій стають критичними для запобігання кіберзагрозам;
- легісляція та регулювання – розробка та прийняття законів та політик, що регулюють обробку, зберігання та передачу інформації, сприяє створенню правової бази для інформаційної безпеки. Це містить в собі заходи щодо конфіденційності, доступу та карного переслідування за порушення правил;
- громадянська обізнаність – підвищення обізнаності громадян щодо інформаційних загроз та кібербезпеки відіграє важливу роль у виявленні та запобіганні соціальним інженерним атакам та дезінформації.

Серед ключових аспектів інформаційної безпеки на рівні міжнародної політики можна виділити:

- міжнародне співробітництво – загальні стандарти та механізми співробітництва в галузі кібербезпеки сприяють обміну інформацією та спільним заходам протидії кіберзагрозам між країнами;
- кібердипломатія – становлення дипломатичних відносин в кіберпросторі стає важливим аспектом міжнародних відносин. Розробка міжнародних норм та правил для кіберпростору може сприяти уникненню конфліктів;
- міжнародні організації – організації, такі як ЄС, НАТО та ООН відіграють ключову роль у формуванні міжнародних стандартів щодо інформаційної безпеки та сприяють розробці спільних стратегій.

В сучасних умовах розробка та розширення арсеналу інформаційно-технологічної та інформаційно-психологічної зброї зумовлює зміни балансу сил у міжнародних відносинах, формуючи загрози національній та глобальній безпеці, перешкоджаючи реалізації як зовнішньополітичних, так і внутрішніх інтересів держав, та їх сталого розвитку.

У таких умовах інформаційна безпека стає ключовим чинником успішного здійснення зовнішньополітичної стратегії держави та забезпечення безпеки держави від зовнішніх загроз загалом, встановлюючи нові орієнтири її зовнішньополітичної поведінки, трансформуючи звичні критерії оцінки ролі та співвідношення військової могутності та політичних можливостей у реалізації на світовій арені геополітичних інтересів, зіткнення яких перетворює інформаційне протиборство за лідерство на інформаційну війну.

РОЗДІЛ 3
ІНФОРМАЦІЙНИЙ ПРОСТІР ФРАНЦУЗЬКОЇ РЕСПУБЛІКИ В КОНТЕКСТІ ЄВРОПЕЙСЬКИХ БЕЗПЕКОВИХ ІНІЦІАТИВ

3.1. Нормативні та інституційні контури безпекової політики Франції в європейському інформаційному просторі

Інформаційна безпека має велике значення у забезпеченні захисту конфіденційності, цілісності та доступності інформації. У контексті держави це стає критичним елементом національної безпеки в частині захисту від зовнішніх та внутрішніх загроз. Інформаційна безпека є передумовою для ефективного функціонування урядових установ, підприємств та інших організацій, а також для запобігання кібератакам, витокам інформації та іншим формам кіберзагроз. Крім того, інформаційна безпека важлива для збереження довіри громадськості до інститутів держави та підтримки суспільства загалом. Забезпечення надійної та безпечної інформаційної інфраструктури є ключовим аспектом сучасного управління та функціонування різних сфер життєдіяльності. Враховуючи важливість та пріоритетність розвитку даних напрямків, уряд Франції активно нарощує «інформаційні м’язи» з метою набуття статусу одного з лідерів в інформаційній сфері на геополітичній арені.

Сьогодні ми можемо спостерігати, як у кіберпросторі розвивається нова руйнівна практика: використання Інтернету у злочинних цілях (кіберзлочинність), зокрема терористичних; поширення хибної інформації та маніпулювання; шпигунство в політичних або економічних цілях; атаки на критичну інфраструктуру (транспорт, енергетика, зв'язок тощо) у цілях саботажу.

Національна стратегія інформаційної безпеки Франції, яка була прийнята в 2015 році, характеризує кібератаки, що виходять від державних чи недержавних груп таким чином:

- не залежать від кордонів та відстаней;

- складно відстежуються (злочинці часто використовують у своїх цілях проміжні системи – ботнети чи проксі);
- відносно прості у здійсненні та пов'язані для злочинця з незначними витратами та ризиком. Кібератаки спрямовані на те, щоб поставити під загрозу безперебійну роботу інформаційних систем та систем зв'язку, що використовуються населенням, підприємствами та адміністративними структурами, а також фізичну цілісність інфраструктури, яка має ключове значення для безпеки держави.

Кібербезпека містить всі дії, які можуть бути використані для захисту від цих атак. Постійне підвищення рівня та інтенсивності кібератак змусило останніми роками більшість розвинених країн зміцнювати свою здатність протистояти їм та затвердити національні стратегії в галузі кібербезпеки.

Інформаційна політика безпеки Франції спрямована на захист інформаційного простору країни. Франція визнає важливість здатності держави самостійно приймати рішення та вживати заходів щодо захисту національної безпеки в умовах глобальної цифрової та інформаційної сфер. Політика акцентується на цілях кібербезпеки, зокрема на захисті інформаційної інфраструктури від кіберзагроз, які можуть становити небезпеку критичним сферам функціонування держави. Така стратегія визначає конкретні заходи та пріоритети для забезпечення безпеки в цифровому середовищі країни (French National Digital Security Strategy, 2015).

До пріоритетів інформаційної безпеки Франції належить поняття «цифровий суверенітет», що в даному контексті визначається як здатність держави приймати автономні рішення та вживати захисних заходів з метою забезпечення національної безпеки в умовах глобалізації та інформатизації суспільства. Також велика увага приділяється захисту інформаційної інфраструктури та інформаційного середовища країни. Це важливо у зв’язку з постійним впливом деструктивної проросійської пропаганди і не тільки на інформаційний простір держави та маніпулюванням зовнішніми силами масовою свідомістю французької громадськості.

Прикладом може бути кампанія з дезінформації, наративи якої йшли з Азербайджану, а метою було підірвати здатність Франції провести Олімпійські ігри в 2024 році. Кампанія проводилася з 26 по 27 липня 2023 року в соціальній мережі *X* з посиланнями на президентську партію Азербайджану. За результатами розслідування, французький орган протидії іноземному впливу *Viginum* виявив, що суб'єкти, близькі до Азербайджану, діяли з метою завдати шкоди репутації Франції шляхом її звинувачення у неспроможності провести Олімпійські та Паралімпійські ігри у 2024 році. Кампанія, яка включала фотографії та відео зіткнень між французькою поліцією та протестувальниками, які бачили мільйони людей, проходила під гаслом *#boycottparis2024*.

У контексті цього слід зазначити, що відносини між Парижем і Баку були напруженими в останні місяці і погіршилися після того, як Баку взяв під контроль регіон Нагірного Карабаху. Під час кампанії Франція неодноразово критикувала азербайджанську владу за блокування Лачинського коридору, ключової дороги, яка з'єднує Вірменію зі спірним анклавом Нагірного Карабаху («French report flags Azeri-linked disinformation campaign targeting 2024 Olympics», 2023).

Серед основних ризиків для інформаційної безпеки П'ятої Республіки слід виділити кіберзагрози. Це пояснюється тим, що кіберзлочинність, інтернет-шпигунство та хакерські атаки на інфраструктурні об'єкти розглядаються як потенційні загрози для критично важливих сфер життєдіяльності країни. Прикладом такої атаки на критично важливі бази даних може слугувати кібератака, здійснена в лютому 2023 року проти медичних закладів та лабораторій Франції, які використовували програмне забезпечення компанії *Dedalus.* Як наслідок, хакери отримали доступ до понад 500 тис. медичних справ громадян Франції, зокрема до особистих даних пацієнтів, їх адрес, телефонних номерів, імейлів, поштових адрес, номерів соціального захисту, інформації про тип крові, результатів тестів на виявлення *COVID-19* тощо. Незважаючи на те, що компанія *Dedalus* була оштрафована за недотримання європейських положень *GDPR* про захист даних, це не знімає питання про вразливість критичної інфраструктури, зокрема медичних баз даних, для зовнішнього хакерського втручання (Chin, 2024b).

Розуміння критичності кіберзагроз існує й на суспільному рівні – опитування *Ipsos*, проведене у 2022 році, показало, що 66% французів занепокоєні, що значний ядерний або промисловий техногенний інцидент може трапитися у Франції саме через кібератаку на критичну інфраструктуру. Більше половини опитаних вважають реальною загрозу перебоїв енергопостачання, проблеми з наданням адміністративних послуг саме через злочинні дії в кіберпросторі (Додаток И). Водночас дослідження показало, що 48% громадян Франції вже зазнали хакерських атак, а 31% – зазнали успішних кібератак. Проблемою є й те, що більше половини жителів Франції вважають себе слабко поінформованими щодо того, як їх інформація захищена в Інтернеті (див. Додаток І). Водночас французьке суспільство має дуже низький рівень довіри до соцмереж та пошукових систем в Інтернеті (див. Додаток Ї) («82% of French people say they are worried about the global risks of cyber-attacks», 2022).

Окрім цього, зазначена вище Національна стратегія інформаційної безпеки визначає шляхи розвитку і практики забезпечення інформаційної безпеки в державі. Ця стратегія була призначена для супроводу суспільства країни у перехідному процесі до використання цифрових технологій, а також для захисту від нових викликів та загроз, пов'язаних із зміною у використанні цих технологій.

У цій Стратегії виділено 5 векторів діяльності:

- гарантування суверенітету держави;
- успішне реагування на зловмисні дії в комп'ютерних системах та мережах;
- інформування широкого загалу;
- перетворення інформаційної безпеки на конкурентну перевагу французьких підприємств;
- підвищення впливу Франції на міжнародній арені («La France et la cybersécurité», 2022).

Цю стратегію доповнили:

- Міжнародна стратегія Франції в галузі інформаційних технологій, яка була презентована міністром Європи та закордонних справ наприкінці 2017 року. У ній узагальнено всі стратегічні цілі, які Франція підтримує в галузі інформаційних

технологій у трьох основних сферах: управління, економіка та безпека («Stratégie internationale de la France pour le numérique», 2015).

- Стратегічний огляд з питань кіберзахисту (Біла книга) – огляд, складений Генеральним секретарем з питань оборони та національної безпеки за дорученням Прем'єр-міністра, був представлений на початку 2018 року. Він, серед іншого, визначає доктрину управління кризами в сфері кібербезпеки, а також роз'яснює цілі національної стратегії в галузі кіберзахисту, підтверджує ефективність французької моделі та покладає основну відповідальність у цій галузі на державу («Revue stratégique de cyberdéfense», 2018).

Окремо слід відзначити візіонерський характер іншого базового документу Французької Республіки, який визначає бачення Парижем процесів в кіберпросторі – відповідь Франції на резолюцію Генасамблеї ООН 73/27 «Розвиток в сферах інформації та телекомунікацій в контексті міжнародної безпеки» та резолюцію 73/266 «Просування відповідальної поведінки держав в кіберпросторі в контексті міжнародної безпеки».

Згідно з цією відповіддю, Франція не вбачає потреби в створенні юридично зобов’язуючого міжнародного інструменту для регулювання процесів в кіберпросторі. Також Париж наполягає на застосуванні міжнародного гуманітарного права при проведенні кібероперацій в умовах збройних конфліктів. Зокрема, міжнародні актори, які проводять такі операції, на думку Франції, зобов’язані розрізняти військові та невійськові об’єкти та дотримуватися принципу гуманності (відмова від атак цивільної інфраструктури). Базовою ідеєю візії Франції є забезпечення для людей в Інтернеті дотримання прав та свобод тією чи іншою мірою, як у реальному фізичному світі («France’s response to Resolution 73/27 and Resolution 73/266», 2019).

Інформаційні технології дедалі глибше проникають у суспільні сфери, що спричиняє значне зростання різного роду кіберзагроз. Тепер уразливість чи захищеність інфраструктури ІКТ, можливість витоку даних стає умовою недружнього чи відверто ворожого інформаційного впливу на інших суб'єктів міжнародно-правових відносин. У зв'язку з цим на найближчу перспективу під

потреби кібербезпеки Франції закладено додаткові бюджетні асигнування, а також збільшено чисельність спеціалізованих кадрів. Як випливає з останнього «Закону про воєнне планування», до 2025 року на цифрову оборону П'ятої Республіки буде виділено 1,6 млрд євро (у період 2014–2019 рр. цей показник складав 1 млрд); кількість «кіберфахівців» у системі Міністерства збройних сил зросте приблизно з 2,5 до 4 тис. осіб. Основним реципієнтом стане командування *COMCYBER*, (поставлене у пряме підпорядкування начальнику Генерального штабу), а також зовнішня розвідка (*DGSE*) та Головне управління озброєнь (*DGA*) («POUR UNE COORDINATION DE LA CYBERDÉFENSE PLUS OFFENSIVE DANS LA LOI DE PROGRAMMATION MILITAIRE 2024-2030», б. д.).

Окрім цього, у 2021 році президент Франції оголосив про плани виділення 500 млн євро фінансової підтримки державним установам та приватним підприємствам для покращення власної кібербезпеки. Цю підтримку також планується використовувати для розробки сучасних рішень протидії кіберзагрозам (Nussbaum, 2021).

Робляться кроки назустріч інноваційним підприємствам. Влада розраховує використати потенціал майданчика *«French Tech»*, який об'єднує французькі стартапи (зокрема й у сфері ІКТ): у 2017 році Е. Макрон пообіцяв вкласти в його розвиток 5 млрд євро на 3 роки; для неї ж був побудований один із найбільших у світі бізнес-інкубаторів *«Station F».* Також за участю Президента Франції створено щорічну конференцію «Французький цифровий день», яка має на меті об'єднати підприємців, програмістів, ІТ-журналістів, тощо (Rolland, 2019). А у листопаді 2019 року уряд підписав трирічний пакт про поглиблення кіберспівпраці з лідерами національного військово-промислового комплексу — *Airbus*, *Dassault*, *Thales*, *Naval Group* та іншими (Filippone, 2019).

Знаковою подією стало прийняття у 2021 році Стратегії кібербезпеки Франції на 2021-2025 роки, яка тепер фактично є базовим документом для планування політики держави у кіберпросторі. Вона передбачає збільшення до 2025 року доходів французьких компаній, які спеціалізуються на кіберзахисті, до 25 млрд євро на рік (у 2019 році цей показник становив 7,3 млрд євро). Планується також

вдвічі збільшити кількість кіберфахівців – до 75 тис. та створити у Франції як мінімум 3 компанії-«єдинороги» у сфері кібербезпеки (стартапи, які за короткий проміжок часу досягли капіталізації у понад 1 млрд доларів) (Hentzen, 2021).

Уже на виконання цієї стратегії в лютому 2022 року в Парижі було відкрито Кіберкампус (*Campus Cyber*). Він об'єднав майже 1700 спеціалістів кібербезпеки з державної та приватної сфер, наукового середовища («Campus Cyber», б. д.). Їх ключове завдання – розробка та впровадження нових рішень з посилення кібербезпеки. Влада Франції розраховує, що об'єднання зусиль держави та приватного сектору дозволить зробити Францію одним із лідерів Європи в ефективності протидії кіберзагрозам («France launches «cyber city» to pool resources for better digital security», 2022).

На технічному та оперативному рівні ефективності французької системи інформаційної безпеки сприяє низка інституцій, серед яких варто виділити:

- Французьке агентство безпеки інформаційних систем (*ANSSI*), яке було створено у 2009 році. Агентство є національним органом, який відповідає за кібербезпеку, запобігання (у тому числі з нормативно-правової точки зору) та реагування на IT-інциденти в системах стратегічно важливих установ. Окрім цього, Агентство відпрацьовує управління у кризових ситуаціях на національному рівні. В агентстві працює 600 осіб і його штат продовжує зростати («Agence nationale de la sécurité des systèmes d'information», 2024).

- Міністерство збройних сил виконує подвійну місію із захисту мереж, що забезпечують його діяльність, та з інтеграції цифрової протидії у військові операції. З метою підтримки діяльності міністерства на початку 2017 року уряд Франції створив Штаб кіберзахисту (*COMCYBER*), переданий під командування начальника штабу озброєних сил («Le commandement de la cyberdéfense (COMCYBER)», б. д.).

- Міністерство внутрішніх справ веде боротьбу з усіма формами кіберзлочинності, спрямованої проти національних установ та інтересів, суб'єктів господарювання та фізичних осіб. Для цього міністерство опирається на центральні служби та територіальні мережі національної поліції, національної жандармерії та

сил внутрішньої безпеки. Їм доручено ведення слідчої діяльності з метою виявлення та притягнення до відповідальності кіберзловмисників. Ці служби також беруть участь у профілактичній та інформаційній роботі з відповідними категоріями громадян («Sur internet», б. д.).

Щодо Міністерства внутрішніх справ Франції та його діяльності з протидії кіберзагрозам, цікавою є робота так званих кіберпатрульних – спеціалістів з кібербезпеки. Так у 2022 році Е. Макрон заявив про створення при Міністерстві спеціальної школи з підготовки фахівців для протидії кібератакам, а також про створення 1500 посад кіберпатрульних. Завдяки цим крокам Президент Франції планує створити повноцінний фаховий клас спеціалістів, що дозволить значно посилити кібербезпеку держави. Окрім цього, в рамках цієї ж роботи з кіберреформи Міністерства внутрішніх справ планується створити «гарячу лінію», подзвонивши на яку люди, які постраждали від дій зловмисників в кіберпросторі, зможуть отримати консультацію щодо того, як їм діяти в їх конкретній ситуації. Такий підхід свідчить про намагання Е. Макрона створити таку систему інформаційної безпеки Франції, яка б враховувала як важливість захищеності державних інформаційних систем, так і була б ефективним щитом для безпосередньо громадян Французької Республіки («У Франції наберуть додатково 1500 «кіберпатрульних», 2022).

Як ми вже зазначали раніше, серед стратегічних ризиків інформаційної безпеки в Франції виокремлюється кібертероризм, оскільки через вебсайти реалізується пропаганда тероризму, здійснюються психологічні впливи на французьке суспільство, проводиться вербування прихильників терористичних організацій, ведеться пошук фінансових ресурсів і плануються терористичні акції. Фахівці підкреслюють, що терористи активно поширюють деструктивну інформацію через мас-медіа, яка детально висвітлює теракти, ситуації з захопленням заручників, реакцію влади на заяви терористичних угруповань, у такий спосіб збільшуючи обсяг негативного контенту та підсилюючи присутність терористичних груп в інформаційному середовищі країни.

Одним із прикладів використання терористами кіберінструментів для атаки на Францію стала масована кібератака на сайти відомих французьких медіа, серед яких *Le Parisien*, *Marianne* та *20 Minutes*, яка була здійснена в січні 2015 року. За даними французьких військових, за цією атакою стояли «ісламістські хакери», а, загалом, їх ціллю було близько 20 тис. французьких вебсайтів. Зазначається, що атака була проведена на тлі вшанування Францією жертв терористичних нападів у Парижі, які відбулись 7-9 січня 2015 року *(Rawlinson, 2015).*

До того ж експерти у галузі інформаційної та кібербезпеки Франції вказують не лише на зовнішні чинники впливу на інформаційну інфраструктуру, але також на деструктивну діяльність таких суб'єктів, як фабрики «ботів» та «тролів», пропаганду та гібридну війну. Вони рекомендують урядовим агенціям Франції створити централізований орган, який займатиметься боротьбою з «фейковими» новинами, проводитиме спростування та попереджатиме поширення маніпулятивних повідомлень в інформаційному просторі держави (Robin, 2023).

Прикладом такої ворожої дезінформаційної діяльності може слугувати спецоперація Росії в рамках інформаційної кампанії *«Doppelgänger»*, яка була проведена в 2023 році. В рамках неї прокремлівські групи створювали фейкові копії сайтів відомих французьких ЗМІ, урядових ресурсів та поширювали фейковий контент, розміщений на цих сайтах, з допомогою мережі ботів у таких соціальних мережах як *Facebook* та *X*. Серед видань, копії сайтів яких було створено, такі відомі медіа як *Le Parisien*, *Le Figaro*, *Le Monde*, *20 Minutes*, а також сайт Міністерства Європи та закордонних справ Франції. Зазначимо, що французька влада виявила, що для поширення дезінформації використовувались також офіційні ресурси посольства Росії у Франції, а також сторінки російських культурних центрів.

За словами речника Міністерства Європи і закордонних справ Франції Анни-Клер Лежандр: «… ця кампанія демонструє гібридну стратегію Росії, спрямовану на підрив демократичного процесу та французьких демократичних інституцій. Ці дії негідні постійного члена Ради Безпеки ООН» (Dönmez, 2023).

Не можна не згадати основні інституції з протидії дезінформації у Франції. Слід відмітити відділ цифрових розслідувань *Agence France Presse (AFP)*, заснований у 2017 році, який з часом розвинувся у найбільшу в світі мережу журналістів-фактчекерів. Зараз у *AFP* працює понад 140 фактчекерів на 5 континентах, які охоплюють більше 30 країн і використовують 24 мови. Ці фактчекери постійно взаємодіють з іншими журналістами в мережі *AFP*. Наприклад, у 2022 році було проведено понад 1236 фактчеків, включаючи неупереджені, дидактичні і джерельні розслідування різноманітних форматів, зокрема фотографії, відео та інших джерел, в результаті яких було виявлено вірусний контекст, що стосувався війни в Україні та інших подій («AFP Factuel», 2024).

Не менш важливу роль відіграє Управління з регулювання аудіовізуальних та цифрових комунікацій (*ARCOM*), яке було створене у 2022 році шляхом об'єднання Вищої ради аудіовізуалу (*CSA*) і Вищого органу з розповсюдження інформації та захисту прав в Інтернеті (*HADOPI*). Управління здійснює розподіл ліцензій, забезпечує дотримання прав авторів та виконання законодавства, зокрема законів, спрямованих на боротьбу з маніпулюванням інформацією, ненависницьким вмістом, зміцненням принципів Республіки і протидією насильству проти жінок. Також було запропоновано, щоб *ARCOM* став основою для онлайн-платформ з метою впровадження Акту про цифрові послуги (*DSA*) у Франції («ARCOM», 2024).

Рада журналістської етики та посередництва (*CDJM*) виступає посередником між журналістами, медіа, інформаційними агентствами та громадськістю у всіх питаннях, пов'язаних з журналістською етикою, включно з достовірністю фактів. Її члени поділяються на три колегії, які порівну представлені в керівних органах: журналісти, ЗМІ та громадськість. Так, будь-який громадянин може звернутися до Ради *CDJM*, яка ухвалює рішення незалежно від політичних чи економічних впливів («CONSEIL DE DÉONTOLOGIE JOURNALISTIQUE ET DE MÉDIATION», 2024).

Неурядова організація «Між рядками» (*Entre les lignes*) представляє собою асоціацію інформаційної та медіаграмотності (*IML*), яка була заснована ще у 2010 році журналістами *Agence France-Presse* та *Reuters*. Асоціація покладається на мережу з понад 200 журналістів-волонтерів для проведення семінарів у Франції та за кордоном. Щороку «Між рядками» проводить кілька сотень воркшопів, в яких беруть участь тисячі молодих людей («ASSOCIATION D'ÉDUCATION AUX MÉDIAS ET À L'INFORMATION», 2024).

Фонд Декарта (*Fondation Descartes*) – це незалежний багатодисциплінарний дослідницький інститут, що спеціалізується на питаннях, пов'язаних з інформацією та публічними дебатами в епоху Інтернету та соціальних мереж. Фонд має внутрішню команду, яка проводить дослідження для більш глибокого розуміння процесів виробництва, розповсюдження та отримання інформації («Fondation Descartes», 2024).

Важливе місце в забезпеченні інформаційної безпеки та попередженні дезінформаційних впливів у французькому медіапросторі посідає Міжнародна фактчекінгова мережа (*IFCN*). Список членів *IFCN* у Франції, окрім *AFP Factuel*, включає такі організації:

- *20 Minutes Fake off*, яка є дочірньою компанією безкоштовної щоденної газети *20 Minutes*;
- *Check News/Libération*, пов'язана з лівоцентристською щоденною газетою *Libération*;
- *France 24 Observers*, що прикріплена до закордонного громадського телеканалу *France 24*;
- *Franceinfo.fr*, пов'язаний з державним радіоконсорціумом *Radio France*;
- *Les Décodeurs/Le Monde*, приєднаний до провідної щоденної газети *Le Monde*;
- *Les Surligneurs*, неурядова організація, що спеціалізується на корекції закону;

- *Les Vérificateurs/LCI-TF1*, афілійований з приватним телеканалом *TF1* та його дочірньою компанією новин («DISINFORMATION LANDSCAPE IN FRANCE», 2023).

Також слід згадати про *Viginum* – це французький спеціальний державний орган протидії іноземному впливу, що діє від липня 2021 року під егідою Генерального секретаріату з питань оборони та національної безпеки (*SGDSN*). Основна мета *Viginum* полягає у виявленні та типологізації підозрілого розповсюдження оманливого чи ворожого контенту на цифрових платформах, яке може стосуватися іноземних акторів, що мають намір завдати шкоди Франції та її інтересам. Важливою особливістю *Viginum* є наявність етичного і наукового комітету, який дотримується суворих норм законодавства («Service de vigilance et protection contre les ingérences numériques étrangères», 2022).

Серед прикладів ефективної роботи *Viginum* стало виявлення в лютому цього року ознак підготовки нової російської дезінформаційної кампанії, яка має назву «*Portal Kombat*». Спрямована проти Німеччини, Франції, Польщі та інших європейських держав, вона передбачала створення на фіктивних вебсайтах фейкового контенту, який згодом мав бути поширений російськими ботами в соцмережах. Для цього Росія створила 197 сайтів французькою, німецькою, польською та англійською мовами. Попри те, що значна частина цих сайтів має низький трафік відвідувань, але, за оцінкою *Viginum*, в будь-який момент ці сторінки можуть бути активовані Росією для форсування поширення дезінформації. Це особливо актуально в умовах підготовки європейських країн до виборів в Європарламент, які заплановані на червень 2024 року («France uncovers a vast Russian disinformation campaign in Europe», 2024).

Інший успішний кейс роботи *Viginum* стосується виявлення та реагування на російську дезінформаційну кампанію «*Doppelgänger*», запущену Росією у 2022 році для дестабілізації соціально-політичної ситуації в країнах Заходу. Так, на тлі посилення збройного конфлікту між Ізраїлем та Палестиною у 2023 році Росія інформаційно атакувала Францію шляхом масованого розповсюдження графіті зі зображенням зірок Давида на будівлях у Парижі. За результатами розслідування

Viginum, відповідальною за ці акції є Росія, яка публікувала фотографій графіті та поширювала їх в соціальних мережах. Зокрема, було виявлено мережу з понад 1000 ботів в соцмережі *X*, які зробили понад 2500 публікацій з тегом *#StarsOfDavid*. Правоохоронними органами Франції було затримано 4 осіб, з яких 2-є громадян Молдови, за підозрою у розповсюдженні понад 250 графіті зірок Давида. Такі дії можуть розпалити заворушення у Франції на тлі сплеску антисемітських дій з початку війни Ізраїлю та ХАМАС.

Міністерство закордонних справ Франції висловило жаль та засудження таких дій, визнавши їх «цифровим втручанням проти Франції». МЗС вважає це спробою Росії використовувати «міжнародну кризу» для розпалювання напруженості та внесення плутанини всередині країни (Caulcutt, 2023).

Однак, Франція веде активну роботу у боротьбі з дезінформацією та наданням об'єктивної інформації громадськості на тлі війни між Ізраїлем та Палестиною. Процес виявлення та розкриття фейків включає роботу фактчекерів, аналіз медійних джерел та співпрацю з міжнародними партнерами. Так, наприклад експерти *AFP* виявляють низку дезінформаційних наративів у висвітленні військових дій з боку Ізраїлю та Палестини. Відео масових ракетних ударів по Палестині, яке нещодавно було розповсюджено, виявилося фальшивим, з використанням анімаційних кадрів з відеогри *Arma 3* («Video game clips misleadingly shared amid Israel-Hamas war», 2023).

Францію не оминула хвиля дезінформації, що охопила нещодавно Європу у зв'язку з пандемією *COVID-19*, війною в Україні, загостренням конфлікту між Ізраїлем та Палестиною, змінами клімату тощо. Актори дезінформації швидко переходять від однієї теми до іншої, реагуючи на розгортання національних та міжнародних криз. Наприклад, криза «жовтих жилетів» стала певним каталізатором для поляризації громадської думки.

З феноменом «жовтих жилетів» Франція вперше зіткнулася наприкінці 2018 року. До цього руху входили переважно прості мешканці Франції та громадяни із матеріальним станом нижчим за середній клас. Приводом до протестів став різкий ріст цін на паливо у зв’язку зі збільшенням акцизу. Однак рух «жовтих жилетів»

досить швидко змінив вектор з протидії намірам уряду підвищити акцизи на бензин, дизельне пальне та мастило на вимогу протестувальників підвищити купівельну спроможність середнього класу та дійшло навіть до спроб відставки чинного Президента Е. Макрона, рейтинг якого зазнав негативних наслідків внаслідок протестів. Деякі дослідники припускають, що протести французів представляють собою ніщо інше, як ілюстрацію однієї з глобальних криз ліберальної демократії, локальними проявами якої є праві сили в Угорщині та Польщі, Брекзіт у Великій Британії, популісти в Греції, Італії та Австрії (Schifrin, 2017).

Якщо подивитися на цей феномен з організаційної та технічної сторін, то можна помітити, що рух «жовтих жилетів» розвивався подібно до апробованої схеми «арабської весни» 2011 року. А саме використання флешмобів, соціальних мереж, мітингів, які проходять одночасно в різних місцях. У Франції досі розслідують можливу причетність Росії до організації акцій протесту «жовтих жилетів». Цим питанням займається Генеральний секретаріат з оборони та національної безпеки – міжвідомча структура, яка підзвітна прем'єр-міністру. Через повідомлення про численні фейкові акаунти в соціальних мережах, які були використані для підтримки демонстрантів, почалося розслідування. Раніше британська газета *Times*, посилаючись на дослідження компанії *New Knowledge*, повідомила про тисячі акаунтів, особливо в соцмережі *X*, які висловлювали підтримку «жовтим жилетам». Дослідники не виключають, що ці акаунти можуть бути пов'язані з Росією («У Франції вивчають причетність РФ до руху «Жовті жилети», 2018).

Журналіст українського видання «Українська правда» Олексій Братущак вважає, що Росія використовувала фейкові акаунти. На його думку, головною метою інформаційної спецоперації для Кремля було:

- у рамках підготовки виявити шляхи розповсюдження інформації. Важливо знати, що є найбільш ефективним для поширення пропаганди та фейків. Росіяни мали змогу знайти слабкі ланки українського інформаційного простору

використовуючи «Офіційний маніфест» від «жовтих жилетів» та ствердитися, яким чином ЗМІ знаходять та поширюють інформацію;

- повне або часткове проведення медіа-операції. Частина громадян України, що «інфікувались» цією інформацією, були впевнені у бажанні мітингувальників виходу Франції з ЄС та НАТО. Наслідками цього стала спотворена думка в головах українців про те, що французькому населенню нібито набридло, що їх країна є членом міждержавних об'єднань. Наступним кроком є поширення тези: «Нащо Україні приєднуватися до НАТО та ЄС, якщо французькі громадяни хочуть виходити звідти?» (Кисельов & Кордун, 2019).

Франція зіткнулася з серйозними викликами в сфері дезінформації та маніпуляції недостовірною інформацію під час руху «жовтих жилетів». Влада та інші суб'єкти застосовували різноманітні заходи для боротьби з цим явищем. Національні та міжнародні фактчекерські організації вивчали розповсюдження інформації та перевіряли її на достовірність. Ретельний аналіз та публікації фактчеків допомагали розкривати неправдиві твердження. Французькі владні структури та представництва намагалися активно спілкуватися з громадськістю через офіційні заяви, пресконференції та інші комунікаційні канали для пояснення ситуації та роз'яснення правдивої інформації. Співпраця з медіа та соціальними платформами була невід'ємною частиною процесу. Залучення міжнародних партнерів та стейкхолдерів для виявлення та припинення розповсюдження дезінформації в мережі допомагало ефективно контролювати інформаційне середовище.

Було проведено низку інформаційних кампаній, спрямованих на підвищення рівня грамотності громадськості щодо методів дезінформації та маніпуляції, що і стало ключовим аспектом відповіді на це явище. Всі ці заходи були спрямовані на підтримку об'єктивної та правдивої інформації, яка є важливою для забезпечення стабільності та об'єктивності в суспільстві.

Іншим фундаментальним викликом для інформаційної безпеки Франції, яка змусила адаптовувати власну політику до нових реалій, стала пандемія *COVID-19*. Багато наративів, пов'язаних із цією кризою, були антивакцинальними та

конспірологічними, а сама ж дезінформація про *COVID-19* спиралася на антисистемний дискурс. Наприклад, кілька представників ЗМІ з руху «жовтих жилетів» стали розповсюджувачами дезінформації про пандемію («DISINFORMATION LANDSCAPE IN FRANCE», 2023).

Дезінформація навколо пандемії *COVID-19* плавно перетікала в дезінформацію навколо вакцинації проти *COVID-19* – «вакцинодемію». «Вакцинодемія» виступила як новий етап багатоступеневого інформаційного протистояння, що, на наш погляд, слід розглядати як черговий крок у глобальній когнітивній війні (Danylenko & Fursai, 2022, с. 19-45). Так, уряд Франції звинуватив Росію в поширенні разом із вакциною своєї «пропаганди та агресивної дипломатії» («France Slams Russia's Sputnik Vaccine as «Propaganda» Tool», 2021). Е. Макрон зазначив, що через пандемію коронавірусу і спроби Росії та Китаю політично вплинути на постачання вакцин, європейські країни опинилися на порозі світової війни нового типу («Covid-19 : le vaccin, un nouvel enjeu de pouvoir à l'échelle mondiale», 2021).

Саме для протидії зовнішньому інформаційному втручанню задля дестабілізації Франції у 2021 році Е. Макрон оголосив про створення спеціального органу для боротьби з іноземним втручанням *Viginum*, який офіційно запрацював в жовтні 2022 року. Знаходячись в прямому підпорядкуванні уряду Франції, офіс опирається на інформацію розвідок, медіа та регуляторів (Laudrain, 2021).

Завдяки таким діям громадянське суспільство сьогодні демонструє певний рівень інформаційної стійкості. Це підтверджується, наприклад, невеликим впливом витоків інформації про Е. Макрона на суспільну позицію. Франція має розвинену мережу фахівців з перевірки фактів та різноманітні ініціативи з медіаграмотності. Але ми хотіли б закцентувати увагу та детальніше розглянути кілька законів, спрямованих на адаптацію відповіді на дезінформацію, якими сьогодні активно послуговується Франція.

Так, наприклад, згідно із Законом про свободу преси від 29 липня 1881 року в Франції, який визначає права та обов'язки ЗМІ, установлена законодавча база для регулювання публікацій, публічних повідомлень, хокінгу та вуличної торгівлі.

Пізніше цей закон був розширений поняттями правопорушення, наклеп і расистські заяви. Спочатку він передбачав відповідальність за «неправдиві новини» (згідно зі статтею 27), але рідко використовується у зв’язку з обуреннями щодо можливості обмеження свободи слова. Поняття «неправдивих новин», які зазвичай виносяться на судовий розгляд, містить порушення законодавства про фондовий ринок (згідно зі статтею L. 465-1 Валютно-фінансового кодексу) та чесності голосування (згідно зі статтею L. 97 Виборчого кодексу) («Loi du 29 juillet 1881 sur la liberté de la presse», б. д.).

Відповідно до Закону № 2004-575 від 21 червня 2004 року про довіру до цифрової економіки, власники публічних онлайн-інформаційних служб мають певні обов'язки, в рамках яких вони можуть бути притягнуті до відповідальності за нездатність видалити незаконний контент («Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1)»., 2004).

Згідно із Законом № 2010-1 від 4 січня 2010 року про охорону таємниці журналістських джерел, порушення таємниці джерел можливе лише у випадках, коли існує переважний суспільний інтерес і застосування заходів є суворо необхідним та пропорційним законній меті, яку ставлять перед собою («Loi n° 2010-1 du 4 janvier 2010 relative à la protection du secret des sources des journalistes (1)», 2010).

Згідно із Законом № 2018-1202 від 22 грудня 2018 року про маніпулювання інформацією, спрямованим на захист демократії від неправдивої інформації, яка може вплинути на чесність голосування, платформи, які відвідують більше 5 млн унікальних відвідувачів на місяць або отримують 100 євро без урахування податків за рекламну кампанію за кожну публікацію, пов'язану з дискусією загального інтересу, підпадають під його дію. Протягом 3-х місяців перед національними виборами може бути запущене спрощене судове провадження для швидкого припинення трансляції публікації. Рішення щодо характеру інформації та можливості її видалення має бути ухвалено тимчасовим суддею протягом 48 годин. Закон передбачає обов'язок співпраці з платформами («Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information», 2018). Інший

закон, який варто згадати, – Закон № 2022-401 від 21 березня 2022 року, спрямований на поліпшення захисту інформаторів («Loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte», 2022).

Окремо слід зазначити, що в квітні 2023 року набули чинності зміни в Страховий кодекс Франції, які надають громадянам Республіки додатковий захист від наслідків кібератак. Зокрема, тепер жертви кібератак можуть протягом 72 годин подати скаргу, після розгляду якої уповноваженими органами влади, потерпілий зможе претендувати на страхову виплату (Apostle & Kawkabani, 2023).

Франція активно веде політику у сфері інформаційної безпеки, приділяючи велику увагу заходам щодо захисту від кіберзагроз, боротьби з дезінформацією та іншими викликами, пов'язаними з цифровим середовищем. П’ята Республіка приймає закони та стратегії, спрямовані на зміцнення її інформаційної безпеки та захист від сучасних кіберзагроз, враховуючи реалії сьогодення.

3.2. Вплив політики інформаційної безпеки Франції на безпекову ситуацію в Європі та світі

Зміцнення стратегічної стабільності та міжнародної безпеки у кіберпросторі є одним із пріоритетів Французької Республіки. Міністерство закордонних справ Франції координує діяльність у сфері «кібердипломатії». Ця робота проводиться у європейських та міжнародних вимірах.

У рамках ЄС Франція відстоює принцип «стратегічної незалежності ЄС у галузі інформаційних технологій», яка є запорукою колективної спроможності Франції до ініціативи та дій. Ця стратегія будується за трьома напрямками:

- Технологічний аспект: промислова політика ЄС спрямована на розвиток потенціалу в сфері новітніх наукових досліджень та розробок для впровадження технологій та служб забезпечення цифрової безпеки. Розробка цифрових компонентів з урахуванням критерію безпеки дозволить також забезпечити конкурентну перевагу європейських товарів та послуг;

- Нормативно-правовий аспект: зовнішньополітичні стратегії ЄС встановлюють норми, які враховують вимоги конкурентоспроможності та перспективи цифрових технологій. Важливо підкреслити, що водночас не порушуються принципи захисту громадян, компаній та держав-членів, і враховуються загальні цінності та принципи, які спільні з П'ятою Республікою. Серед цих принципів – забезпечення права на конфіденційність, захист персональних даних та критичної інфраструктури;

- Зміцнення потенціалу: ЄС покликаний відігравати важливу роль у заохоченні та підтримці розвитку можливостей щодо забезпечення кіберзахисту державних та приватних структур у державах-членах та в самих європейських організаціях. Він також може сприяти в сфері підготовки та навчання шляхом налагодження спільної діяльності та усунення дублювання інструментів.

Крім цих аспектів, на переконання Франції, необхідно зміцнити оперативну співпрацю між державами-членами ЄС. Її метою має стати створення у масштабах Європи майданчиків для обміну технічною інформацією про загрози, що дозволить попереджати кібератаки та оперативно реагувати на них. Створення у 2017 році механізму спільного дипломатичного реагування ЄС на зловмисні дії у комп'ютерних системах та мережах («Комплекс заходів кібердипломатії») повністю вписується у стратегію зміцнення співробітництва («La France et la cybersécurité», 2022).

Таке акцентування Франції на важливості посилення стратегічної незалежності ЄС у сфері інформаційної безпеки є частиною стратегії Е. Макрона з безпекового посилення Європи та зниження її залежності у захисті своєї безпеки від США та блоку НАТО. На думку Президента Франції, надмірна залежність ЄС від заокеанського партнера, який за умов існування «феномену Трампа» став значно менш прогнозованим для союзників та створює стратегічні ризики для безпеки Європи. Особливо це підкреслило повномасштабне вторгнення Росії в Україну, розпочате в лютому 2022 року, яке яскраво продемонструвало військову та безпекову неготовність Європи до тривалого воєнного протистояння.

«Ми більше не можемо покладатися на те, що інші годують нас, піклуються про нас, інформують нас, фінансують. Ми не можемо покладатися на те, що інші захистять нас, чи то на суші, на морі, під водою, у повітрі, у космосі чи кіберпросторі. У цьому відношенні наша європейська оборона повинна зробити новий крок вперед», – наголосив Е. Макрон в березні 2022 року у телезверненні до громадян Франції (Willsher, 2022).

Активною та принциповою також є візіонерська позиція Франції на глобальному рівні. Так, Паризький заклик до довіри та безпеки у кіберпросторі, оприлюднений Францією на Паризькому форумі світу 12 листопада 2018 року, свідчить про активну роль Франції у створенні безпечного, стабільного та відкритого кіберпростору. Ця політична декларація високого рівня знаменує собою подальшу мобілізацію зусиль щодо забезпечення стабільності у кіберпросторі. Декларація, яка базується на 9-ти принципах та загальних цінностях, спрямована на перетворення кіберпростору у вільний, безпечний та відкритий простір, а також передбачає активну взаємодію як національних, так і міжнародних акторів, бізнесу, громадськості для забезпечення базових демократичних цінностей в кіберпросторі.

Автори Паризького заклику зобов'язуються вести спільну роботу з метою забезпечення:

- захисту окремих осіб та найважливіших об'єктів інфраструктури від зловмисної кібердіяльності;
- захисту цілісності та доступності Інтернету;
- запобігання кібервтручанню, спрямованому на дестабілізацію виборчих процесів;
- захисту інтелектуальної власності за умов кіберзагроз;
- перешкоджання поширенню шкідливих комп'ютерних програм та методів;
- підвищення безпеки цифрової продукції та цифрових послуг;
- покращення загальної комп'ютерної гігієни;
- перешкоджання здійсненню дій щодо кіберреагування з боку недержавних суб'єктів, включно з приватним вектором;

- покращення міжнародних норм відповідальної поведінки та посилення заходів щодо зміцнення довіри.

Текст підтримали понад 1200 суб'єктів, зокрема 81 держава, 36 державних інституцій та органів місцевого самоврядування, 390 організацій та представників громадського сектору та 706 приватних компаній. Зазначимо, що в 2021 році до заклику приєдналися США та ЄС, що зробило ініціативу однією з базових для всієї світової громадськості («Paris Call», 2024).

Всеосяжний характер Паризького заклику наголошує на необхідності багатостороннього підходу для вироблення стандартів та належної практики, щоб надійно та безпечно використовувати можливості, які відкриває цифрова революція. Франція має намір разом з іншими державними партнерами, приватним сектором та громадськістю вивчати питання про роль та особливу відповідальність приватних учасників у зміцненні стабільності та міжнародної безпеки кіберпростору («Cybersécurité: Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans le cyberespace», 2018).

Лідируючу позицію у питанні кібербезпеки Франція демонструє також в інших міжнародних форматах. Зокрема, в квітні 2019 року на саміті *G7* Франція стала одним із авторів ініціативи *Cyber Norm*. Вона встановлює узагальнені принципи та правила, які регулюють поведінку держав у кіберпросторі з метою забезпечення кібербезпеки та стабільності. Йдеться про захист критичної інфраструктури, відповідальне використання кіберзброї, співпрацю в розслідуванні кібератак, інформаційну безпеку та захист прав людини у кіберпросторі.

Окрім цього, згідно з ініціативою *Cyber Norm*, її учасники зобов’язуються:

- сприяти активному та розширеному обміну інформацією всередині країни та між країнами ЄС;

- обмінюватися досвідом та найкращими практиками, які будуть визначені в результаті цього процесу, з широким колом держав та іншими зацікавленими сторонами;

- взаємодіяти з іншими державами з метою їх залучення до спільних зусиль з навчання, співпраці, прозорості та зміцнення довіри;

- активно співпрацювати з метою сприяння розвитку можливостей партнерів для впровадження вищезгаданих норм поведінки і рекомендацій («Cyber Norm Initiative: Synthesis of Lessons Learned and Best Practices», 2019).

6 квітня 2019 року міністри закордонних справ країн «Великої сімки» виступили на зустрічі в Дінарі з ініціативою щодо норм, що застосовуються до кіберпростору. Норми, викладені у цьому документі, були здебільшого розроблені групою урядових експертів ООН і є однією зі складових міжнародної системи забезпечення стабільності у кіберпросторі. Країни *G7* мають намір продовжувати цю роботу та узгоджувати свої позиції щодо широкого спектру важливих рекомендацій у галузі кібербезпеки («Communiqué des ministres des affaires étrangères du G7 sur leurs convergences de vue en matière de politique étrangère, le 6 avril 2019», 2019).

Ця ініціатива закріплює уже напрацьовані Францією в рамках ООН ідеї щодо покращення кібербезпеки в глобальному просторі. Зокрема, в рамках ООН з 2004 року 6 груп урядових експертів (*GGE*) і робоча група відкритого складу, в якій Франція брала активну участь, зосередилися на питаннях міжнародної кібербезпеки та зробили можливим просування дискусій щодо застосування міжнародного права щодо кіберпростору. Було створено нову робочу групу відкритого складу на період 2021-2025 років, у якій Франція бере активну участь, щоб захистити своє бачення міжнародного регулювання кіберпростору, зокрема просування принципів Паризького заклику. Крім того, зіткнувшись із зростанням загроз і ризиків нестабільності в кіберпросторі, Франція разом із 54 іншими державами та ЄС сприяють створенню Програми дій щодо кібербезпеки, метою якої є підвищення загального рівня кібербезпеки, підтримка зусиль держав з розбудови власного кіберпотенціалу та розвиток партнерства «держава – приватний сектор – громадськість».

У рамках НАТО з ініціативи Франції 28 держав прийняли на варшавському саміті в червні 2016 року «Зобов'язання з кіберзахисту». У ньому кіберпростір був визнаний зоною ведення операцій, що зобов'язує НАТО захищати себе в

кіберпросторі так само, як на суходолі, у повітрі та на воді («La France et la cybersécurité», 2022).

Зокрема, за ініціативи Франції кібербезпеку визначено одним із пріоритетів НАТО та ухвалено перелік конкретних кроків для побудови ефективного кіберзахисту Альянсу. Серед таких кроків:

- розробка найповнішого спектру можливостей для захисту національних інфраструктур і мереж;
- виділення необхідних ресурсів на національному рівні для зміцнення можливостей кіберзахисту;
- посилення взаємодії між відповідними національними зацікавленими сторонами кіберзахисту;
- обмін інформацією та оцінками щодо кіберзагроз;
- покращення навичок та обізнаності серед усіх зацікавлених сторін у сфері оборони на національному рівні: від кібергігієни до найскладнішого та надійного кіберзахисту;
- сприяння кібернавчанню, тренуванню, а також покращенню навчальних закладів для зміцнення довіри та знань в Альянсі;
- прискорення виконання узгоджених зобов’язань щодо кіберзахисту («Cyber Defence Pledge», 2016).

Також слід зазначити, що у травні 2018 року у Франції відбулася перша в історії конференція *Cyber Defence Pledge Conference*, присвячена зобов'язанню з кіберзахисту («La France et la cybersécurité», 2022).

На рівні Організації економічного співробітництва та розвитку ОЕСР у 2018 році Франція ініціювала щорічний Глобальний форум з цифрової безпеки для економічного процвітання (далі – Глобальний форум), спрямований на просування позиції Франції про те, що приватний сектор відіграє значну роль у безпеці та стабільності кіберпростору. Щорічно Глобальний форум проводить тематичні заходи, результати яких впливають на міжнародні обговорення у галузі публічної політики та можуть сприяти розвитку аналітичної роботи, формуванню принципів та рекомендацій у міжнародній політиці, як у ОЕСР, так і на інших міжнародних

форумах. Варто підкреслити, що у 2023 році форум відбувся саме у Парижі («The Global Forum on Digital Security for Prosperity», б. д.).

Активною є діяльність Франції і в інших форматах, покликаних забезпечити не тільки покращення кібербезпеки між державами, але й на глобальному рівні. Зокрема, у 2019 році Франція приєдналася до Нової Зеландії у запуску Крайстчерчського заклику до ліквідації терористичного та насильницького екстремістського контенту в Інтернеті («Déclaration conjointe du président de la République française Emmanuel Macron et de la Première ministre de Nouvelle-Zélande Jacinda Ardern à l'occasion du Sommet de l'Appel de Christchurch 2022», 2022). *L'Appel de Christchurch* – це спільнота понад 130 урядів, постачальників онлайн-послуг і організацій громадянського суспільства, які діють разом, щоб ліквідувати терористичний і насильницький екстремістський контент в Інтернеті («The Christchurch Call», 2024).

Також у лютому 2024 року Франція разом з Великою Британією та США стала однією з ініціаторок підписання 35 державами та декількома транснаціональними корпораціями, серед яких *Google*, *Microsoft* та *Meta*, декларації щодо боротьби з незаконним використанням кібершпигунських інструментів, зокрема йдеться про засоби прослуховування телефонних розмов та дистанційного управління відеокамерами та мікрофонами. Так, підписанти домовились використовувати ці інструменти відповідально та в законний спосіб, а також вибудувати прозорий обмін інформацією про такі інструменти з приватними компаніями. Одним із чинників, який зумовив ініціювання підписання цієї декларації став кейс використання державними та недержавними акторами ізраїльського шпигунського програмного забезпечення *Pegasus*, яке дозволяло непомітно проникати в мобільні телефони та відстежувати активність їх користувачів («Britain, France lead 35 nation agreement on controlling spyware, mercenary hackers», 2024).

Щодо національного рівня, то наразі урядом Франції обговорюється законодавча ініціатива, яка буде спрямована на впровадження важливого нормативного документу для країн ЄС, який міститиме в собі внесення нових

пропозицій щодо цифрового шахрайства, кібершпіонажу, захисту дітей, обмежень для ЗМІ та переходу до «хмарних» технологій.

Законопроєкт, спрямований на захист і регулювання цифрового простору (*Loi visant à sécuriser et réguler l'espace numérique – SREN*) містить положення про імплементацію європейських Актів про цифрові послуги та цифрові ринки в поєднанні з міжпартійними пропозиціями щодо захисту неповнолітніх від доступу до онлайн-порнографії та зміцнення цифрового суверенітету.

Міністр цифрових технологій Франції Жан-Ноель Барро, який і представляв законопроєкт, підкреслив, що цей нормативний документ був написаний таким чином, щоб всі положення відповідали чинному регулюванню впливу в соціальних мережах. Жан-Ноель Барро пропонує запровадити фільтр проти шахрайства для боротьби з «мафією без честі, яка […] перетворила наші планшети та смартфони на нову територію для рекету» (Hartmann, 2023).

Цей фільтр має запобігти, серед іншого, онлайн-шахрайству, яке є достатньо поширеним у Франції. Так, для прикладу, у лютому 2024 року дві страхові компанії Франції *Viamedis* та *Almerys* зазнали потужної кібератаки, внаслідок якої зловмисники отримали доступ до персональних даних французів, зокрема інформації про дату народження, номер соціального страхування тощо. За оцінкою Французького відомства із захисту даних *CNIL*, жертвами цієї атаки стали понад 33 млн громадян Франції, що становить майже половину населення країни. Також там наголосили, що ця інформація тепер може бути використана зловмисниками для онлайн-шахрайства, зокрема розсилки фішингових листів (Duboust, 2024).

Ба більше, новий законопроєкт передбачає надання ліцензії французькому органу, що регулює аудіовізуальні та цифрові комунікації (*ARCOM*) з метою деіндексувати порнографічні вебсайти, які не відповідають новим вимогам перевірки віку. Барро також хоче уповноважити *ARCOM*, французький медіарегулятор, призупинити доступ до вебсайтів, які потрапили під санкції ЄС, прямо посилаючись на афілійовані з Москвою видання *Russia Today France* та *Sputnik*. Ці ЗМІ були заборонені на початку агресії Росії проти України, оскільки їх вважали рупором Кремля, але їм вдавалося місяцями обходити санкції. Для

міністра цифрових технологій намір полягає в тому, щоб дати *ARCOM* можливість «ефективно та швидко протидіяти пропаганді ворогів демократії». Законопроєкт визначає *ARCOM* координатором цифрових послуг, національним органом, який забезпечуватиме дотримання Закону про цифрові послуги та відповідатиме за нагляд за відповідністю цифрових компаній, розташованих у Франції («Le Règlement européen sur les services numériques (DSA): protéger les droits des citoyens sur internet», 2023).

Франція докладає значних зусиль щодо розвитку і використання технології «штучного інтелекту», щоб стати центром ЄС в галузі ШІ. Уже зараз Франція є однією з держав-лідерок у розвитку ШІ – так, у 2020 році було подано 278 заявок на отримання патенту на технології, пов'язані зі «штучним інтелектом», що є 3-м показником у Європі (див. Додаток Й) («Annual patent applications related to artificial intelligence», б. д.).

Під час конференції *Viva Tech* Президент країни Е. Макрон, голова Мінфіну Брюно Ле Мер та міністр цифрових технологій Жан-Ноель Барро висловили підтримку ШІ-галузі. «Я думаю, що ми номер один [у сфері «штучного інтелекту»] у континентальній Європі, і нам потрібно прискоритися», – заявив Макрон. Він додав, що Франція має намір «інвестувати як божевільна» у навчання та дослідження. На його думку, Франція сподівається в найближчому майбутньому наздогнати конкурентів у сфері розвитку ШІ, зокрема шляхом створення кількох «великих глобальних гравців. «Повірте мені, це ясно, що США номер один. І не дарма, тому що це величезний внутрішній ринок. Я хочу, щоб ми скоротили розрив та інвестували, розвивалися та прискорювалися набагато швидше», – зазначив Президент (Kharpal, 2023).

Серед основних ініціатив Франції у цьому напрямку є:

- Стратегія розвитку «штучного інтелекту», яку презентовано у 2018 році. Стратегія спрямована на забезпечення того, щоб Франція займала визначальне положення в галузі ШІ як з технологічного, так і з етичного погляду («LA STRATÉGIE NATIONALE POUR L'INTELLIGENCE ARTIFICIELLE», 2018);

- Паризька стратегія зі «штучного інтелекту», яка покликана розвивати екосистему ШІ у Парижі та створювати сприятливі умови для стартапів і великих технологічних компаній у цій галузі («MANIFESTE POUR UNE ÉTHIQUE DU NUMÉRIQUE», 2021);

- Створення Комітету етики зі «штучного інтелекту» (*CNPEN*), метою якого є розробка рекомендацій та визначення принципів для ефективного та етичного використання цих технологій (Rinke, 2023).

У галузі ШІ Франція об’єднує зусилля з іншими країнами ЄС, прагнучи забезпечити сталий розвиток цієї галузі на користь суспільства. Німеччина, Франція та Італія досягли угоди щодо майбутнього регулювання ШІ. Уряди трьох країн підтримали обов'язкове саморегулювання через кодекси поведінки для базових моделей ШІ. У Берліні, Парижі та Римі вважають, що ризики, які властиві системам ШІ, пов'язані з їх застосуванням, а не з самою технологією. Згідно з планом урядів трьох країн, малі і великі постачальники технологій ШІ в ЄС, які добровільно беруть на себе умови європейців, зобов'язані їх виконувати. Тому правила поведінки та прозорості мають бути обов'язковими для всіх, вважають вони. Як йдеться у документі, на початковому етапі не передбачається запровадження будь-яких санкцій, лише обов'язкове саморегулювання. Однак, якщо з часом будуть виявлені порушення кодексу поведінки, то може бути створена система санкцій. Париж, Рим та Берлін припускають, що надалі контроль за дотриманням стандартів здійснюватиме певний європейський орган. Міністерство економіки Німеччини, що займається цією темою спільно з Міністерством цифрових технологій ФРН, заявило, що держави повинні регулювати не сам ШІ, а його застосування. Міністр цифрових технологій Фолькер Віссінг заявив, що він дуже радий тому, що Париж і Берлін на одній хвилі. «Якщо ми хочемо грати у вищій лізі світового ШІ, нам потрібно регулювати програми, що виходять на ринок, а не саму технологію», – сказав він (Piquard, 2024).

Окрім цього, Франція активно виступає за міжнародне регулювання сфери розвитку та використання технології «штучного інтелекту». Зокрема, Франція стала одним із розробників Декларації Блетчлі з безпеки використання ШІ,

підписаної в листопаді 2023 року 28 державами та Європейським Союзом. Її ключова ціль – зробити розвиток технології прозорим, підзвітним та стандартизованим, аби мінімізувати будь-які ризики використання технології у ворожих цілях. Водночас Франція та підписанти наполягають на тісній співпраці бізнесу, держав та громадськості у цьому питанні («The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023», 2023).

Зазначимо, що у цьому питанні Франція має особливу позицію, яка контрастує з багатьма європейськими партнерами. Наприклад, підтриманий Радою ЄС Акт про «штучний інтелект» (*Artificial Intelligence Act*), який наразі розглядається Європарламентом, став «яблуком розбрату» між Парижем та Брюсселем. Регуляторна рамка, яку пропонує цей акт, передбачає жорсткий контроль за розвитком цієї технології, зокрема надання розробниками ШІ інформації про свою роботу контролюючим органам ЄС – Агентству «штучного інтелекту», яке передбачається створити цим актом. Франція, як одна з держав-лідерів у розвитку технології, яка значну увагу приділяє підтримці стартапів в сфері ШІ, прагне зберегти конкурентну перевагу французьких компаній і уникнути ризику потрапляння чутливої інформації в руки конкурентів. Хоча сторонам все ж вдалося досягти компромісу і Франція погодилася підтримати *Artificial Intelligence Act*, проте питання роботи французьких компаній-розробників ШІ в нових європейських регуляторних умовах все ще залишається значною мірою відкритим (Piquard, 2024).

Також не можна не відмітити активну роботу Франції щодо протидії дезінформації у медіапросторі. Організація «Репортери без кордонів» (*Reporters sans frontières*) та її партнери *Agence France Presse (AFP)*, Європейська мовна спілка (*l'Union européenne de radio-télévision*) та Глобальна мережа редакторів (*Global Editors Network*) запустили ініціативу саморегулювання ЗМІ, спрямовану на боротьбу з дезінформацією в Інтернеті під назвою «Ініціатива журналістської довіри» (*Journalism Trust Initiative*).

«Ініціативу журналістської довіри» було створено для сприяння журналістиці шляхом дотримання узгодженого набору стандартів довіри та

прозорості. Реалізація ініціативи відбувається за допомогою так званого Європейського центру стандартизації (*Comité européen de normalisation*), який створено у 2018 році для всіх стейкхолдерів, наприклад ЗМІ, професійних асоціацій і спілок, саморегулюючих організацій, таких як пресради та регуляторні органи, а також цифрові платформи, рекламодавці та представники інтересів споживачів. В інформаційному просторі, в якому неправдива інформація циркулює швидше, аніж достовірні новини, захист журналістики вимагає змінити цю тенденцію, надавши реальну перевагу всім тим, хто продукує правдиві новини та інформацію, незалежно від їх статусу («RSF et ses partenaires dévoilent la «Journalism Trust Initiative (JTI)», un dispositif innovant contre la désinformation», б. д.).

Окрім цього, французькі медіа активно працюють над власною «самофільтрацією». Тут показовим є кейс з 2023 року, коли журналісту французького каналу *BFM TV* були висунуті підозри у втручанні в новинний редакційний процес. Журналіст транслював короткі репортажі про спірні питання міжнародних відносин, які виходили в ефір приблизно о 2-й годині ночі та мали низькі рейтинги глядацької аудиторії. Новинні сюжети були спрямовані на сприяння інтересам Марокко та суданського лідера Хеметті, а також на приниження Катару. Ці відео були негайно вилучені, а також поширені в соціальних мережах, зокрема в *X*, з відповідним спростуванням («DISINFORMATION LANDSCAPE IN FRANCE», 2023).

У цьому конкретному випадку основним інструментом боротьби з дезінформацією та унеможливленням подібних випадків в майбутньому стала внутрішня робота *BMF TV* з розслідування інциденту та посилення редакційного контролю за публікацією інформації. Це важливий кейс, який демонструє, що ефективна боротьба з дезінформацією можлива не тільки за умови використання існуючих державних механізмів, але й з використанням внутрішніх ресурсів інформаційних компаній для фільтрації інформації (Ganguly & Conn, 2023).

Як ми бачимо, Франція за президентства Е. Макрона виступає одним з ініціаторів низки міжнародних проєктів, ціллю яких є посилення глобальної інформаційної та кібербезпеки, зокрема в частині протидії кібератакам та

дезінформації, а також щодо реагування на новітні технологічні виклики, такі як технологія «штучного інтелекту». Водночас ми можемо зробити висновок, що Франція не тільки ініціює зміни, але й висловлює готовність бути глобальним та європейським лідером у цій сфері. Підґрунтям для цього є як успіхи технологічних компаній Франції, так і візія Президента Франції зі збільшення геополітичної ваги Франції у світі та Європи загалом.

3.3. Перспективи імплементації Україною досвіду Франції у реалізації безпекової інформаційної політики

Політика інформаційної безпеки Франції базується на розвинутій системі нормативно-правових документів, які її регулюють, розгалуженої мережі державних інституцій, співпраці з приватним сектором та громадськістю. Приклади успішного реагування цієї системи на ризики, виклики та загрози інформаційній безпеці Франції свідчать про достатньо високу ефективність французької інформаційної моделі. Це актуалізує питання використання найкращих інструментів, методів та практик, які застосовує Париж у рамках власної політики інформаційної безпеки. Особливо це актуально для України, яка окрім воєнної протидії російській збройній агресії, щодня протистоїть інформаційним операціям, які проводить Кремль проти української держави та її громадян.

Статистичним свідченням важливості використання французького досвіду у протидії інформаційним загрозам та покращенні медіаграмотності є опитування, проведене *InMind* в 2023 році на замовлення Агентства *USAID*. Згідно з його результатами, майже половина українців інтуїтивно оцінює правдивість новин, тобто не перевіряє додатково отриману інформацію. Також 64% українців навіть не знають про існування фактчекінгових сервісів, що свідчить про критичну ситуацію з рівнем медіаграмотності українського суспільства. Водночас все ще 8%

українців користуються російськими медіа для отримання новинної інформації («Українські медіа, ставлення та довіра у 2023 р»., 2023).

Враховуючи попередній аналіз особливостей політики інформаційної безпеки Франції, ми виокремили кілька ключових сфер, де досвід Франції не тільки актуальний, але й справді може бути використаний Україною у практичній площині, а саме:

- інституційне посилення боротьби з кіберзагрозами та дезінформацією;
- залучення приватного сектору та громадськості до реалізації політики кіберзахисту держави;
- використання сучасних технологій, зокрема «штучного інтелекту», для боротьби з фейками;
- співпраця у протидії дезінформації з провідними транснаціональними інформаційно-технологічними компаніями, такими як *Google*, *Meta*, *X* тощо;
- встановлення внутрішнього дезінформаційного фільтра в українських медіа;
- боротьба з дезінформацією в стратегічних для інтересів держави регіонах.

Аналізуючи інституційне посилення боротьби з кіберзагрозами та дезінформацією як потенційну сферу запозичення Україною французького досвіду, важливо акцентувати увагу на оцінці роботи французького Агентства безпеки інформаційних систем (*ANSSI*). Саме ця французька інституція відповідає за розробку та впровадження політики кібербезпеки Франції, забезпечує координацію різних державних відомств у протидії кібервикликам, а також безпосередньо оцінює ризики та протидіє кіберзагрозам. Важливо підкреслити, що *ANSSI* концентрується не тільки на захисті державного сектору, але й відповідає за захист критичної приватної кіберінфраструктури. Окрім цього, агентство пропонує свою експертизу бізнесу та громадськості, та надає на регулярній основі, а не тільки у прив'язці до конкретного кіберінциденту, рішення для покращення власного захисту («What we do (ANSSI)», 2022). Це є однією з особливостей французького підходу до забезпечення власної кібербезпеки – сприйняття державної та приватної сфер як єдиної цифрової екосистеми, яка потребує комплексної стратегії захисту

від зовнішніх кіберзагроз. Саме ж агентство *ANSSI* визначено як центральне та ключове відомство, яке відповідає за кіберзахист такої екосистеми.

Це дещо контрастує з підходом України до розбудови системи кіберзахисту суспільства як спільноти держави, бізнесу та громадськості. Так, в Україні функціонують кілька спеціальних державних відомств, які відповідають за кібербезпеку, серед яких:

- Державна служба спеціального зв'язку та захисту інформації (Держспецзв'язку), яка відповідає за захист державних інформаційних систем шляхом визначення відповідності інформаційних та телекомунікаційних систем, які використовуються державними структурами в своїй роботі, вимогам до безпеки, встановлених державою («Державна служба спеціального зв'язку та захисту інформації України», б. д.). В структурі служби також працює Урядова команда реагування на комп'ютерні надзвичайні події України (*CERT-UA*), яка в оперативному режимі аналізує кіберінциденти та надає рекомендації щодо реагування на них («About CERT-UA», б. д.).

- Національний координаційний центр кібербезпеки (НКЦК) при Раді національної безпеки та оборони України. Цей орган відповідає за координацію різних державних безпекових органів, які дбають про кіберзахист держави (Про Національний координаційний центр кібербезпеки, 2016);

- Органи кібербезпеки сектору оборони. Йдеться про Кіберполіцію у складі Національної Поліції України, Департамент кібербезпеки Служби безпеки України, а також кібердепартаменти інших безпекових відомств.

Водночас, попри наявність НКЦК як головного координуючого органу в сфері кібербезпеки, інституційний рівень політики інформаційної безпеки України демонструє відсутність розгляду державою кібербезпеки України як комплексної системи, яка містить державний, приватний та громадський сектори. Це своєю чергою яскраво контрастує з підходом Франції, яка не тільки формує та розвиває систему кібербезпеки у всій різноманітності її акторів, але й створила єдиний центральний відповідальний орган – *ANSSI*. Тому, на нашу думку, для України потенційно перспективним є використання досвіду Франції саме з інституційної

централізації політики інформаційної безпеки, що могло б підвищити ефективність протидії кіберзагрозам.

Тим паче *ANSSI* має значний успішний досвід боротьби з кібервикликами та загрозами, особливо в умовах складних політичних процесів. Так, у травні 2017 року напередодні виборів Президента Франції, відбувся витік листування команди Е. Макрона, так званий кейс *Macron Leaks* (було викрадено й оприлюднено на форумі *4Chan* 9 гігабайтів файлів та 21 тис. електронних листів) (див. Додаток Д). Електронні листи швидко поширились за допомогою протрампівських та проросійських акаунтів у соціальних мережах, а також за підтримки *Wikileaks*. Особливістю цього вторгнення в кампанію стало введення декількох підроблених електронних листів зі скандальним змістом в загальну масу електронних листів, в яких містилися звичайні обміни повідомленнями («DISINFORMATION LANDSCAPE IN FRANCE», 2023).

Реагуючи на такий витік приватної інформації Е. Макрон доручив *ANSSI* розслідувати цей кіберінцидент. Зазначимо, що задіяння цієї організації можливе за умови, що кібератака була масованою і технічно складною. Окрім цього, виборча комісія Франції у координації з *ANSSI* закликала національні медіа та суспільство не довіряти інформації з неофіційних джерел з метою запобігання подальшого поширення неправдивої інформації та дестабілізації політичних процесів в країні. Виборча комісія Франції запровадила «блекаут» інформації передвиборчої гонки за день та частково у день виборів. Завдяки діям *ANSSI* та висновкам, які вказали на причетність Росії, Франції вдалось локалізувати загрозу витоку, унеможлививши його потенційний катастрофічний вплив на соціально-політичну ситуацію в державі (Sotto & Leicester, 2017).

Напередодні виборів Президента Франції у 2022 році *ANSSI* підключалось до перевірки походження фейків, зокрема акцентом в її роботі стала поширена інформація щодо планів використання владою Франції спеціального електронного устаткування для голосування *Dominion*, яке у 2020 році Д. Трамп назвав однією з основ «фальсифікації американських виборів». Це змусило *ANSSI* вкотре нагадати, що кожна електронна система, яка використовується державою під час виборів,

проходить тестування та сертифікацію *ANSSI,* а безпосередньо устаткування *Dominion* взагалі не планувалося для використання під час виборів 2022 року (Holroyd, 2022).

Все це вказує на те, що французькі вибори 2022 року були супроводжені активним контролем фактів, щоб забезпечити достовірність інформації в інформаційному просторі та запобігти поширенню дезінформації («DISINFORMATION LANDSCAPE IN FRANCE», 2023).

Також цікавим є кейс протидії Франції атаці проросійської хакерської групи на сайти Національної асамблеї та Сенату Франції у 2023 році. Завдяки ефективним діям *ANSSI* вдалось мінімізувати збої в роботі сайтів та не допустити витоку інформації. Відразу після цього Франція схвалила виділення протягом 2024-2030 років 4 млрд євро на посилення кіберзахисту Франції, а також розширила повноваження *ANSSI* щодо збору технічних даних трафіку та роботи серверів (див. Додаток Ґ) («Russian hackers strike French National Assembly website», 2023).

Важливим, на нашу думку, також є запозичення досвіду французького відомства з протидії іноземному втручанню *Viginum*. Ця структура, створена у 2021 році, тільки за останній рік виявила дві великі міжнародні дезінформаційні кампанії Росії проти Заходу, серед яких «*Portal Kombat*» та «*Doppelgänger*». Їх ціллю була дестабілізація ситуації в державах Заходу, зокрема Франції, з ціллю знизити рівень підтримки України у відбитті повномасштабної агресії РФ («France uncovers Russia's disinformation campaign justifying war in Ukraine», 2024).

Показовим є те, що *Viginum* працює не тільки над аналізом французького інфопростору, але й досліджує глобальне інфополе для виявлення інформаційних операцій, які потенційно загрожують інформаційній безпеці Франції.

Цей досвід може бути використаний Центром протидії дезінформації для покращення власної діяльності з виявлення дезінформаційних операцій на міжнародному рівні. Це дозволить державі краще розуміти міжнародне інформаційне середовище та відповідно розробити систему реагування на виклики.

Інституційне посилення політики кіберзахисту також актуалізує питання залучення бізнесу, громадськості, зокрема науковців, до розвитку системи

кібероборони держави. Попри наявну в Україні координацію держави та бізнесу у протидії кіберзагрозам, відсутній механізм об'єднаної роботи державного та приватного секторів з покращення кібербезпеки суспільства. На відміну від України, Франція приділяє значну увагу побудові таких механізмів. Так, у 2022 році Франція відкрила в Парижі кіберхаб «кіберкампаус», який об'єднує понад 1700 фахівців у сфері кібербезпеки з державного та приватного секторів, і основною ціллю роботи яких є розробка рішення для покращення кіберзахисту як державних систем, так і інформаційних систем бізнесу («France launches «cyber city» to pool resources for better digital security», 2022).

Відкриття «кіберкампусу» є частиною стратегії Е. Макрона з посилення кіберзахисту Франції, про яку було оголошено в 2021 році. Вона передбачає виділення понад 1 млрд євро на підтримку державних програм та приватних компаній, які спрямовані на кіберзахист Франції. Зокрема, завдяки цим інвестиціям Париж планує збільшити доходи компаній, які спеціалізуються на кібербезпеці, втричі – до 25 млрд євро в 2025 році з 7,9 млрд євро в 2019 році, та збільшити вдвічі кількість робочих місць в сфері кібербезпеки. Окрім цього, в рамках цієї стратегії Франція виділить 500 млн євро науковим установам та бізнесу на розробку нових рішень для покращення кібербезпеки («Macron announces €1bn security package after cyberattacks on French hospitals», 2021).

Одним із ключових у співпраці України та Франції в контексті протидії дезінформації має стати питання використання сучасних технологій для боротьби з фейками, особливо це стосується використання «штучного інтелекту». У цій сфері найцікавішим для України є розвиток Вищою інженерною школою Франції *EURECOM* та французьким Інститутом вивчення і координації музики та акустики (*IRCAM*) проєкту *DeTOX*. Суть проєкту полягає у створенні технічного інструменту на основі технології ШІ, який виявлятиме діпфейки, що особливо актуально в умовах постійного покращення можливостей «штучного інтелекту» творити дедалі більш достовірні діпфейки.

Цей проєкт концентруватиметься на спростуванні фейків щодо політичних лідерів та ключових військових осіб Франції. Зокрема, «штучний інтелект»

тренуватимуть з допомогою записів голосу лідерів Франції, щоб ШІ у майбутньому зміг використати цю базу для перевірки діпфейків. Ключова ціль проєкту – створити технічний інструмент, який в автоматичному режимі виявлятиме діпфейк без потреби глибокого аналізу контенту фактчекінговими платформами («DeTOX: A french-funded project on deepfake detection targeting important civilian and military personalities in France», 2023).

Такий досвід особливо актуальний для України, адже держава в умовах гібридної війни Росії на постійній основі стикається з використанням Кремлем діпфейків військово-політичного керівництва України для сіяння хаосу та дестабілізації ситуації в державі.

Найбільш показовим недавнім кейсом використання такого високотехнологічного інформаційного фейку стало поширення в інтернеті восени-взимку 2023 року серії відео- та аудіороликів, де на той час Головнокомандувач Збройних Сил України Валерій Залужний нібито закликає військових захопити владу в Україні, критикує Президента України Володимира Зеленського та розповідає про глибокий розкол у воєнно-політичному керівництві держави. Українська незалежна аналітична платформа «Вокс Чек» у рамках свого проєкту «Вокс Чек» та у співпраці з соцмережею *Facebook* перевірила відповідні матеріали та підтвердила, що це діпфейк, створений для дестабілізації ситуації в Україні («ВІДЕОФЕЙК: Валерій Залужний записав звернення, де наказує військовим покинути зону бойових дій та захоплювати владу», 2023; «ВІДЕОФЕЙК: Валерій Залужний створив петицію про мобілізацію депутатів Верховної Ради», 2023).

Аналогічний приклад використання ШІ для створення діпфейків проти лідерів України Росія продемонструвала на початку повномасштабного вторгнення. Так, в березні 2022 року російські ботоферми активно поширювали звернення Президента України Володимира Зеленського, де він нібито заявляє про «капітуляцію України» та закликає українську армію «скласти зброю». Для створення цього відео також була використана технологія діпфейку. Його творці сподівалися у такий спосіб дестабілізувати ситуацію в Україні, посіяти хаос і, як

наслідок, зламати обороноздатність держави («Deepfake video of Volodymyr Zelensky surrendering surfaces on social media", 2022).

Попри те, що робота фактчекінгової платформи дозволила нівелювати інформаційні загрози від таких вкидів, актуальним залишається виведення історій таких кейсів на міжнародний рівень, адже так ми покращимо обізнаність світової спільноти з фактами інформаційного терору Росії та посприяємо вдосконаленню фактчекінгових інструментів партнерів, які використовуються для боротьби з російською пропагандою. Саме тому важливим є поглиблення співпраці з Францією та європейськими проєктами в частині використання сучасних технологій для боротьби з дезінформацією як майданчику для взаємовигідного обміну досвіду.

Також цікавий є інший французький досвід з використання ШІ для протидії дезінформації. Так, агентство *AFP* та Вища нормальна школа (*Ecole Normale Supérieure Paris-Saclay*), один з найвідоміших математичних навчально-наукових закладів Франції, є партнерами європейського проєкту «*vera.ai*» (*VERification Assisted by Artificial Intelligence*). Заснований в 2022 році, проєкт передбачає створення на основі технології «штучного інтелекту» ефективних інструментів для боротьби з дезінформацією. Зокрема, з допомогою таких інструментів журналісти, дослідники, розслідувачі та громадськість зможуть перевіряти аудіо, відео та текстову інформацію на предмет наявності фейків або недостовірної інформації.

Проєкт все ще знаходиться на ранніх етапах розвитку, проте його технологічна прогресивність та потужна партнерська база (партнерами проєкту, окрім *AFP*, є такі потужні європейські інформаційні агентства, наукові установи, об'єднання як *EBU*, *Deutsche Welle*, *EU Disinfo Lab*) є перспективним майданчиком для українських медіа («vera.ai», б. д.). Особливо це актуалізується тим, що український інфопростір неодноразово атакується інформаційними вкидами та фейками, які потребують технологічної обробки для їх спростування.

Іншою важливою сферою для обміну досвідом в протидії дезінформації має стати співпраця з транснаціональними інформаційними корпораціями *Facebook*, *X*, *Google* та іншими, де Франція має чимало успішних кейсів кооперації задля

протидії фейкам. Одним із найкращих прикладів цього стала співпраця 8 головних французьких медіа (*France Télévisions*, *Le Monde*, *Agence France Presse*, *L'Express*, *France 24 The Observers*, *20 Minutes BFM-TV* та *Libération*) з *Facebook* та *Google* напередодні президентських виборів у Франції в 2017 році.

Зокрема, користувачам *Facebook* була надана можливість відмічати сумнівний контент, який стосується виборів. Після цього вищезазначені медіа перевіряли цей контент і якщо як мінімум 2 медіаресурси підтверджували його фейковість, *Facebook* відмічав цей контент як сумнівний.

Що ж до співпраці з *Google*, то департамент компанії, який відповідає за новини, *Google News Lab* та французькі медіа запустили проєкт *CrossCheck*. Його ціллю стала перевірка новин на наявність фейків, неправдивої інформації та пропаганди («Facebook, Google partner with French media to combat «fake news», 2017). Результатами роботи могли скористатися французькі ЗМІ під час підготовки власних новинних матеріалів. Окрім цього, результати кросчекінгу публікувались у блозі проєкту (Dieudonné, 2017).

Україна уже має успішний досвід з *Facebook* щодо викриття фейків, зокрема такою діяльністю у співпраці з соцмережею займається неприбуткова організація «Вокс Україна» (Ю. Даниленко, 2020). Проте, таке співробітництво, на відміну від досвіду Франції, не набуло системності, яка у протидії дезінформації є ключовою, адже саме інформаційні майданчики соцмереж є основним простором пропагандистських та дезінформаційних кампаній Росії.

Для прикладу, російські гравці комп'ютерної гри *Minecraft*, якою володіє глобальна інформаційно-технологічна компанія *Microsoft*, використали можливості гри для відтворення битви за Соледар, яка тривала з серпня 2022 року до січня 2023 року, створивши повноцінний пропагандистський контент, з яким могли ознайомитися гравці *Minecraft* зі всього світу (Myers & Browning, 2023). За умови налагодженої співпраці України та *Microsoft* в питанні протидії дезінформації такий контент міг би бути оперативно прибраний з гри, а гравці, які його створили, заблоковані.

Іншим показовим прикладом є використання соцмереж *Facebook* і *X* для поширення неправдивої інформації в рамках інформаційної кампанії Росії під назвою *«Doppelgänger»*. Жертвами цієї кампанії стали як Франція, так і Україна. Суть цієї масштабної інформаційної операції Росії полягає в дискредитації українського політичного керівництва та зниження рівня підтримки Заходом шляхом поширення фейкових новин, відео та аудіо («Doppelganger operation», 2023).

Також, на нашу думку, важливим є встановлення внутрішнього дезінформаційного фільтра в українських медіа, який би на редакційному рівні блокував превентивно публікацію дезінформації. Тут цікавим є досвід французького інформаційного агентства *AFP*, при якому функціонує спеціальна медіалабораторія *AFP Medialab*. Це невелика група дослідників, яка працює над розробкою інноваційних рішень з протидії дезінформації, якими могли б користуватися *AFP* та інші інформаційні агентства світу. Серед проєктів, які розвивала ця медіалабораторія слід відзначити проєкти *WeVerify*, *YouVerify!*, *YouCheck!*, *InVID*, *ASRAEL* та *AFP Transcriber*. Наразі лабораторія працює над реалізацією згаданого в цьому дослідженні проєкту *vera.ai*, який передбачає використання технології ШІ для спростування фейків («Medialab», б. д.).

Окрім цього, цікавою для України є робота Франції з боротьби з дезінформацією в стратегічних для інтересів держави регіонах. Так, Франція глибоко занепокоєна ростом обмежень основних свобод та посилення репресій у Білорусі. Ці заходи спрямовані на забезпечення контролю білоруського уряду над усім суспільством та пригнічення всіх, хто виступає проти агресивної війни Росії проти України. В Білорусі існує законодавчий арсенал, спрямований на стримування будь-якої форми опозиції, зокрема тих, хто виступає проти війни чи висловлює підтримку українському народу. Це створює чіткий зв'язок між російською агресією проти України та посиленням політики репресій в Білорусі.

Франція засуджує наявність у Булорусі великої кількості політичних в'язнів і систематичне застосування тортур та нелюдського поводження щодо політичних опозиціонерів. Зокрема, Париж неодноразово закликав Білорусь дотримуватися

своїх міжнародних зобов'язань, звільнити політичних ув'язнених з гуманітарних міркувань та надавати доступ до медичної допомоги. Франція вкотре засуджує серйозні порушення прав людини в Білорусі та висловлює неприйнятність участі режиму Лукашенка у незаконній військовій агресії Росії проти України.

Проте, ця робота обмежується не тільки заявами – Франція веде цілеспрямовану інформаційну роботу з розкриття на міжнародному рівні злочинів білоруського режиму та доведення до відома білоруського народу та світової громадськості загалом потреби у системних змінах у Білорусі («OSCE – Vive préoccupation vis-à-vis de la situation des droits de l'Homme en Biélorussie (11 mai 2023)», 2023).

Такий підхід є надзвичайно актуальним для України, адже білоруський напрямок зовнішньої політики є пріоритетним для забезпечення обороноздатності України. Тому будь-які дії, спрямовані на підрив білоруського режиму та розрив його союзницьких відносин з РФ, дозволить збільшити ймовірність перемоги України у війні з Росією.

Слід зазначити, що наразі вже створені механізми для обміну досвідом та поглиблення кіберспівпраці між Францією та Україною. У цьому контексті варто виокремити Угоду про співробітництво у сфері безпеки між Україною та Францією, яка була підписана В. Зеленським та Е. Макроном 16 лютого 2024 року. Вона, зокрема, виокремлює два треки співпраці у сфері інформаційної безпеки:

1) стратегічна комунікація та боротьба з іноземним втручанням, маніпулюванням інформацією;

2) кібербезпека.

У сфері боротьби з дезінформацією сторони будуть концентруватися на:

- покращенні спроможностей України протидіяти іноземному втручанню та інформаційним маніпуляціям;
- обміні досвідом;
- розробці спільних освітніх і навчальних програм для фахівців із цілісності інформації.

Зазначимо, що Франція також зобов’язалась допомогти Україні приєднатися до колективних інструментів боротьби з іноземним втручанням та маніпулюванням інформацією. Йдеться про загальноєвропейські механізми протидії дезінформації та пропаганді.

У сфері кібербезпеки Франція надаватиме підтримку, яка б дозволила покращити можливості України протидіяти ворожим кібероперація̈м, а також сприятиме поглибленню співпраці України з НАТО та ЄС у сфері кібербезпеки. Французька сторона допомагатиме, зокрема, шляхом посилення кіберстійкості та захисту критичної інфраструктури України. Угода не обмежується тільки стратегічною візією – держави також погодились налагодити оперативну співпрацю у боротьбі з кіберзлочинністю. Це вкрай важливо для України, адже динаміка кібератак Росії в умовах повномасштабної війни є надзвичайно високою, що потребує перманентної активної роботи з їх виявлення та нейтралізації («Угода про співробітництво у сфері безпеки між Україною та Францією», 2024).

Ця історична угода фактично задає рамку для співпраці України та Франції саме з врахуванням існуючих процесів у світовій політиці, серед яких ключове місце займають російська збройна агресія проти України та збільшення ролі інформаційної складової в світовій політиці. Окрім цього, цей документ є фактично першим підписаним Францією та Україною документом, де французька сторона надає гарантії безпеки Україні і конкретизує їх по різних сферах. Це контрастує з Будапештським меморандумом, підписантом якого була і Франція. Декларативний характер меморандуму, відсутність зобов’язуючих положень зумовили цілковиту неефективність документу для забезпечення безпеки України за умов нових геополітичних реалій (Sedliar, Sapsai & Tsyrfa, 2023, c. 153-160).

Окрім цього, в грудні 2022 року Міністр економіки, фінансів, промисловості та цифрового суверенітету Франції Бруно Ле Мер та Прем'єр-міністр України Денис Шмигаль узгодили та підписали спільну Дорожню карту для розвитку технологічного сектору. Відповідно до неї, Франція планує виділити 1 млн євро на підтримку українських технологічних стартапів, а також між сторонами буде

поглиблена співпраця в сфері захисту українських публічних даних («Франція виділить кошти на підтримку технологічних стартапів України», 2022).

Окрім простору для співпраці, запропонованого вищезазначеними угодами, майданчиком для обміну досвідом може стати міжнародний формат «Таллінський механізм». Цей інструмент співробітництва в сфері кібербезпеки був запущений в грудні 2023 року урядами України, Франції, Канади, Данії, Естонії, Німеччини, Нідерландів, Польщі, Швеції, Великої Британії та США («Талліннський механізм: Україна та міжнародні партнери започаткували новий інструмент співпраці у кіберпросторі», 2023).

Відповідно до досягнутих домовленостей, зазначені держави зобов'язуються надавати підтримку Україні в розбудові потужної системи кіберзахисту в коротко-, середньо- та довгостроковій перспективах. Також дозволяється участь приватного та громадського сектору держав-партнерів у проєктах розбудови такої системи в Україні. Сам же механізм виступить фактично координаційним майданчиком для узгодження партнерами допомоги Україні.

Окремо зазначимо, що «Талліннський механізм» формально закріплює принцип «нічого про Україну без України», що дозволить Україні отримувати ту підтримку, яка відповідає внутрішній оцінці українськими інституціями ключових потреб системи кіберзахисту. Окрім цього, учасники механізму зобов'язуються кооперуватися в питаннях посилення кіберспроможностей України з ЄС та НАТО («MISSION STATEMENT», 2023).

Також Україна та Франція мають можливість співпраці у сфері кібербезпеки, використовуючи механізм Кібердіалогу України та ЄС, який був започаткований в червні 2021 року. У рамках нього Україна, Євросоюз та держави-члени блоку мають можливість координувати політику в сфері кібербезпеки. Йдеться про узгодження законодавчих механізмів регулювання цієї сфери, обмін досвідом роботи профільних інституцій, а також координацію співпраці в рамках міжнародних організацій («Україна та ЄС започаткували Кібердіалог», 2021). З моменту започаткування механізму уже проведено 3 раунди Кібердіалогу.

Також цікавим форматом для обміну досвідом між Францією та Україною є створений у грудні 2015 року Європейським Союзом для боротьби з тероризмом Інтернет-форум ЄС (*EU Internet Forum – EUIF*). Його ключова ціль – посилення співпраці з цифровими платформами для протидії використанню Інтернету у терористичних цілях, а також висвітлення проблемних питань, що стосуються Інтернету та тероризму.

Основний фокус форуму зосереджений на проблемі зловживання Інтернетом у терористичних цілях шляхом двох основних напрямків:

1) зменшення доступності терористичного контенту в Інтернеті;
2) збільшення обсягу ефективних альтернативних наративів онлайн.

У 2019 році до сфери діяльності *EUIF* було додано посилення протидії сексуальному насильству над дітьми в мережі. У 2022 році *EUIF* ще більше розширив свій спектр, включно з боротьбою з торгівлею наркотиками та торгівлею людьми в Інтернеті («European Union Internet Forum (EUIF)», б. д.).

Наразі Україна та Франція шукають варіанти співпраці в сфері кібербезпеки на двосторонньому рівні, зокрема по лінії «держава-бізнес». Так, в лютому представники Ради національної безпеки і оборони України (РНБО), Національного координаційного центру кібербезпеки при РНБО України (НКЦК) зустрілись з представниками приватного сектору Франції, який займається питаннями кібербезпеки. Йдеться про такі організації як з *Cyber Task Force*, *Gatewatcher*, *Predicta Lab* та *Sekoia*. У фокусі зустрічей – налагодження співпраці з французьким бізнесом, опрацювання можливих варіантів державно-приватного партнерства, а також формати обміну досвідом («Фахівці НКЦК провели робочу зустріч з представниками французьких компаній у сфері кібербезпеки», 2023).

Співпраця не обмежується виключно формальними домовленостями і уже сьогодні відбувається низка практичних заходів з обміну досвідом в сфері кібербезпеки. Так, в грудні 2023 року французькі правоохоронці провели серію тренінгів для Національної поліції України щодо протидії кіберзлочинам. Зокрема, йдеться про використання сучасник методик збору, обробки, систематизації та аналізу інформації («Кібербезпека та кримінальний аналіз: французькі

правоохоронці провели тренінг для українських поліцейських», 2023). Зазначимо, що подібна співпраця повинна бути регулярною, адже Україна перебуває в режимі постійних кібератак та кіберпровокацій РФ з ціллю дестабілізації ситуації в країні та послаблення її обороноздатності.

Водночас слід наголосити, що попри потребу обміну досвідом між Україною та Францією як необхідну умову посилення кібероборони України, французька сторона уже відзначає значний прогрес, якого Україна досягла у покращенні політики інформаційної безпеки. Так, голова Командування кіберзахисту Франції (*COMCYBER*) Еймерік Боннемізон наголосив, що Україна здійснила «…справжню революцію, вийшовши на новий рівень у її комп'ютерній оборонній боротьбі». Він відзначив, що російські кібератаки були значно менш ефективними саме через покращення Україною власних можливостей протидії («Україна на тлі атак РФ здійснила «революцію кіберзахисту» - французький генерал», 2023).

Підсумовуючи зазначимо, що існує низка сфер, де французький досвід може бути використаний Україною для покращення власної протидії кіберзагрозам, дезінформації та пропаганді. Ключовим, що об'єднує ці сфери, є розгляд кібербезпеки держави як комплексної системи, яка містить в собі безпеку державних систем, бізнесу, громадського сектору та використання сучасних технологій для нівелювання загроз. Саме у цих аспектах Франція досягла значного прогресу, який важливо вмонтувати в українську систему захисту.

Висновки до Розділу 3

Франція продовжує відігравати ключову роль у формуванні глобальних стратегій протидії деструктивним впливам та успішної реалізації політики інформаційної безпеки. Однак, це лідерство не обмежується лише дипломатією та міжнародними відносинами. Країна активно приділяє увагу сфері кібербезпеки та інформаційної безпеки, де вона є важливим учасником глобальних ініціатив. Її діяльність охоплює взаємодію з іншими країнами загальноєвропейського та

євроатлантичного простору для розробки та впровадження заходів, спрямованих на забезпечення кіберзахисту та протидію дезінформації.

Ключовий аспект цього лідерства полягає у встановленні стандартів та принципів для захисту інформаційного простору. Франція виступає ініціатором формування єдиної стратегії протидії деструктивним впливам на міжнародному рівні. Її досвід і активна роль у цих питаннях надають країні вагомого впливу у кіберпросторі та сфері інформаційної безпеки.

Досвід Франції у сфері реалізації політики з інформаційної безпеки може бути надзвичайно корисним для України з кількох ключових причин:

1. Інституційна організація: Франція створила цілісну стратегію кібербезпеки з центральним органом, компетенції якого охоплюють як державну, так і приватну сфери. Україна може взяти на озброєння цей підхід для створення ефективної системи протидії кіберзагрозам, забезпечуючи взаємодію держави, бізнесу та громадськості.

2. Приватний сектор та громадськість: Франція успішно залучає приватний сектор та громадськість до реалізації політики кіберзахисту. Використання досвіду та практик приватного сектору може допомогти Україні вдосконалити загальнодержавну політику інформаційної безпеки.

3. Інноваційні технології: Франція активно використовує інноваційні технології, такі як «штучний інтелект», у боротьбі з дезінформацією. Україні варто розглянути можливості впровадження передових технологій для виявлення та протидії фейковим новинам.

4. Співпраця з транснаціональними компаніями: Франція успішно співпрацює з провідними транснаціональними компаніями у протидії дезінформації. Співпраця з такими компаніями, як *Google*, *Meta* тощо, може допомогти не лише боротися з фейками, але й унеможливити їх поширення.

5. Міждержавна співпраця: Україна та Франція вже мають існуючі міждержавні формати-майданчики, де можуть обмінюватися досвідом. Це полегшує взяття на озброєння найкращих практик політики інформаційної безпеки П’ятої Республіки для впровадження в Україні.

ВИСНОВКИ

1. У рамках дослідження актуального стану теоретичних та методологічних підходів до вивчення концептів інформаційне суспільство, інформаційна безпека, інформаційна операція з'ясовано, що дані концепції розглядаються в контексті ширших політологічних концепцій «м'якої сили», «гострої сили» та «розумної сили». Ці концепції передбачають, що інформація є фундаментальною складовою політики сучасних держав та міжнародних об'єднань, яку вони використовують для інформування громадськості, впливу на інших акторів міжнародних відносин та їх систему загалом.

Також акцентовано на критичній ролі інформаційної компоненти в концепції «гібридної війни» як актуального процесу розвитку міжнародних відносин. Так, держави, бізнес та громадськість активно використовують інформаційний інструментарій для отримання переваги над умовним противником для досягнення своїх цілей національної політики.

Окрім цього, цікавим є розгляд інформаційної безпеки в контексті концепції «глобального інформаційного суспільства», яка передбачає, що вплив інформації став настільки великим, а її всепроникність настільки потужною, що уже доречно говорити про сучасну інформаційну добу не як опис процесу, а як констатацію стану міжнародних відносин.

2. Французька внутрішньо- і зовнішньополітична стратегія в сфері інформаційної безпеки формується під впливом різних факторів, враховуючи складність сучасного інформаційного середовища та геополітичних реалій. До таких факторів належать:

а) виклики, ризики та загрози кібербезпеці

- технічні загрози: збільшення кількості і складності кібератак та технічних загроз, збільшення кількості суб'єктів, здатних проводити кібератаки, ставить Францію перед необхідністю активного захисту інформаційних систем;

- кібершпигунство та кіберсаботаж: дії іноземних держав, хакерських груп у сфері кібершпигунства і саботажу можуть впливати на формування стратегії відповіді.

б) геополітичні реалії

- зростання ролі наднаціональних організацій, зокрема таких як НАТО, ЄС, ООН та загалом міждержавних форматів співпраці під час формування національними державами власної політики інформаційної безпеки;

- геополітична нестабільність: гібридизація спецоперацій в системі міжнародних відносин, активніше використання інформаційних операцій під час проведення військових дій та дестабілізуючих політичний простір операцій, зростання ролі медіа та соціальних мереж як майданчиків для проведення інформаційних операцій.

в) технологічний прогрес

- стрімкий розвиток технологій та їх проникнення у практично всі сфери міжнародних відносин, зокрема інформаційну;

- збільшення уваги держав до покращення своєї кіберінфраструктурної мережі;

- розвиток державами власного «кібеарсеналу» для проведення зовнішніх кіберагресій та захисту від них.

г) соціокультурні та політичні чинники

- використання інформаційного середовища в контексті геополітичного протистояння демократії та автократії;

- збільшення ролі бізнесу та громадськості в сучасних демократіях в забезпеченні інформаційної безпеки;

- радикалізація інформаційного простору, викликана соціально-політичними, демографічними, економічними та культурними процесами трансформацій у французькому суспільстві.

д) міжнародні зобов'язання

- кібербезпека в рамках Європейського Союзу: дотримання стандартів та виконання рекомендацій ЄС з кібербезпеки та інформаційної безпеки.

е) економічні інтереси

- захист економічних інтересів: захист критично важливих інфраструктур та технологічних розробок;

- збільшення частки ринку ІКТ у економіці Франції.

Розуміння цих чинників та реалізація практичних кроків за цими напрямами допомагає П’ятій Республіці адаптувати свою стратегію в інформаційній безпеці, щоб відповідати умовам і викликам сучасного геополітичного середовища.

3. Аналіз загальноєвропейської та євроатлантичної політики ЄС та НАТО продемонстрував, що їх базовою особливістю є оборонний характер розвитку. Так, Євросоюз та Північноатлантичний альянс значну увагу приділяють захисту власної інформаційної інфраструктури, протидії дезінформації та підтримці зовнішніх партнерів, зокрема України, у їх протидії інформаційним загрозам. Для цього вони покращують власну нормативно-правову базу, розробляють стратегії розвитку та забезпечення інформаційної безпеки, формують ефективну інституційну інфраструктуру, яка спроможна реалізувати та впровадити стратегії інформаційної безпеки.

Важливою особливістю сучасної політики інформаційної безпеки ЄС та НАТО є акцентування на шляхах протидії ворожому, агресивному та такому, що суперечить міжнародному праву, впливу стратегії гібридної війни Росії. Її ціллю є підрив демократії та просування своїх національних інтересів на Заході.

Так як Франція є членом ЄС та НАТО, активно інтегрована у їх структури, вона поділяє ключові цілі й принципи політики інформаційної безпеки, вдосконалюючи своє законодавство, ініціюючи удосконалення європейського та реалізуючи загальноєвропейську та євроатлантичну стратегії в інфопросторі у партнерстві з іншими державами-членами.

4. Аналіз безпекової політики Французької Республіки уможливив висновок, що П’ята Республіка є значущою складовою загальноєвропейської політики, яка визначається низкою ключових напрямків.

Франція бере активну участь у спільних ініціативах з іншими країнами Європейського Союзу та НАТО з метою зміцнення обороноздатності та

забезпечення безпеки у регіоні. Однією з пріоритетних сфер є кібербезпека та інформаційна безпека, що відображається в розробці стратегій протидії кіберзагрозам та дезінформаційним кампаніям, регуляторних актів, які регулюють цю сферу, та які за змістом, цілями та принципами відповідають стратегіям ЄС та НАТО. Франція також бере активну участь у розробці та впровадженні стратегічних документів з кібербезпеки на рівні ЄС та Північноатлантичного альянсу. Вона сприяє формулюванню спільних підходів та стратегій для забезпечення інформаційної безпеки у європейському контексті. Окрім цього, Париж ініціює на регулярній основі вдосконалення загальноєвропейської та євроатлантичної політик з акцентом на збільшенні уваги до кібербезпеки, захисту приватності в інформаційну добу та протидії дезінформаційним кампаніям.

Франція активно співпрацює з іншими країнами ЄС, структурами самого Євросоюзу, зокрема Єврокомісією, Європейським агентством з мережевої та інформаційної безпеки (*ENISA*) в сферах обміну інформацією, розробки стандартів та спільних заходів щодо кібербезпеки.

Країна виступає важливим гравцем у міжнародних дипломатичних відносинах, впливаючи на світові події та сприяючи утриманню міжнародного порядку. Так, Франція співпрацює з іншими європейськими країнами для вирішення глобальних проблем, що свідчить про тісний зв’язок її безпекової політики з загальноєвропейськими стратегіями.

Франція сформувала потужну інституційну структуру для реалізації політики інформаційної безпеки, яка глибоко інтегрована в європейську та євроатлантичну, водночас зберігаючи автономність та концентруючись на викликах, які стоять перед Францією. Окрім цього, Франція наполягає на своїй лідерській ролі в ЄС, зокрема у питаннях кібербезпеки та інформаційної безпеки загалом, та виступає за більшу суб’єктність та незалежність Євросоюзу як геополітичного гравця.

5. На сьогодні Франція зберігає свою важливу роль у формуванні підходів, принципів та розробці інструментів для підтримки міжнародних структур, спрямованих на протидію зовнішнім деструктивним впливам. В дисертаційному дослідженні було окреслено два виміри розвитку безпекової політики Франції у

інформаційній сфері – стратегічний та тактичний, які містять широкий спектр заходів, спрямованих на покращення та вдосконалення складових національної інформаційної безпеки, що своєю чергою підтримують її лідерську позицію.

До стратегічного виміру належать такі заходи:

а) дипломатія та міжнародні відносини: Франція активно взаємодіє з іншими державами у розробці спільних дипломатичних стратегій та підходів до протидії деструктивним впливам, включно з інформаційними аспектами;

б) кібербезпека та інформаційна безпека: Франція приділяє велику увагу кібербезпеці та інформаційній безпеці, і вона є активним учасником глобальних ініціатив у цих галузях. Країна взаємодіє з іншими державами для розробки і впровадження заходів, спрямованих на забезпечення кіберзахисту та протидію дезінформації;

в) лідерство у розробці стандартів: Франція відіграє ключову роль у встановленні стандартів та принципів для захисту інформаційного простору, сприяючи формуванню єдиної стратегії протидії деструктивним впливам.

До тактичного виміру, на нашу думку, належать такі заходи:

а) моніторинг та виявлення потенційних загроз в інформаційному середовищі: Франція постійно вдосконалює національні системи моніторингу для виявлення аномалій та потенційних інформаційних та кіберзагроз, з огляду на власний досвід та світові тенденції – розробляє та впроваджує системи оперативного реагування на інциденти в інформаційному середовищі;

б) інформаційний та кібербезпековий аудит: Франція проводить регулярний аудит системи інформаційної безпеки для ідентифікації слабких місць та вразливостей у системах;

в) освіта та навчання: Франція безперервно підвищує рівень обізнаності працівників та суспільства щодо інформаційної та кібербезпеки;

г) реагування на кіберінциденти: Франція визначає процедури та розробляє план дій для негайного реагування на кіберінциденти та дезінформаційні кампанії; вибудувала таку систему реалізації політики інформаційної безпеки, де державні та недержавні установи активно взаємодіють одна з одною для проведення

розслідувань в інформаційному середовищі та притягнення злочинців до відповідальності.

Ці стратегічні та тактичні заходи спрямовані на забезпечення інформаційної безпеки Франції за умов постійно зростаючих загроз та викликів в інформаційному просторі. Отже, можна визнати, що Франція продовжує виступати як один з лідерів у формуванні міжнародних підходів та інструментів для боротьби з зовнішніми загрозами у сфері інформаційної безпеки.

6. Дослідження політики інформаційної безпеки Франції вказує на кілька ключових аспектів, які можуть слугувати орієнтиром для вдосконалення політики України в цій сфері та застосування комунікативних та інноваційних інструментів. Ось деякі висновки та рекомендації:

а) інституційне посилення політики інформаційної безпеки України: Франція приділяє велику увагу створенню і впровадженню цілісної стратегії кібербезпеки, в центрі якої функціонування єдиного центрального органу з безпеки інформаційних систем, чия компетенція проникає в державну та приватну сфери. Україна може взяти на озброєння цей підхід Франції, щоб вибудувати ефективну системи протидії кіберзагрозам, яка б базувалась на спільній роботі держави, бізнесу та громадськості;

б) залучення приватного сектору та громадськості до реалізації політики кіберзахисту держави дозволить використати досвід та практики приватного сектору для вдосконалення загальнодержавної політики інформаційної безпеки. Французьким шаблоном для таких дій може слугувати створення кіберхабів, де фахівці з державного, приватного та громадського секторів зможуть разом працювати над розробкою рішень з посилення кібербезпеки;

в) використання інноваційних технологій та інструментів: Франція використовує інноваційні технології, такі як «штучний інтелект», для боротьби з дезінформацією. Україні слід розглядати можливості використання передових технологій для ефективного виявлення та протидії фейковим новинам;

г) співпраця у протидії дезінформації з провідними транснаціональними компаніями, зокрема *Google*, *Meta*, *X* тощо. Успішний досвід Франції кооперації з

цими компанії у протидії фейкам, особливо під час політичного процесу, свідчить про важливість налагодження стратегічних відносин з такими компаніями, аби не тільки боротися з фейками, але й унеможливлювати їх поширення;

Україна та Франція уже мають існуючі міждержавні та міжнародні формати-майданчики, на яких можуть обмінюватися досвідом, що тільки спрощує взяття Україною на озброєння найкращих практик політики інформаційної безпеки П’ятої Республіки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Акт про цифрові послуги (DSA) та Акт про цифрові ринки (DMA): нові підходи ЄС до регулювання Інтернет-посередників. (2022). Взято з https://dslua.org/publications/akt-pro-tsyfrovi-posluhy-dsa-ta-akt-pro-tsyfrovi-rynky-dma-novi-pidkhody-yes-do-rehuliuvannia-internet-poserednykiv/

2. Бебик, В. [Валерій]. (2011). Глобальне інформаційне суспільство: поняття, структура, комунікації. Інформація і право, (1), 41–49

3. Бебик, В. [Валерій]. (2005). Інформаційно-комунікаційний менеджмент у глобальному суспільстві: психологія, технології, техніка паблік рілейшнз. Київ: МАУП.

4. Бебик, В., Шергін, С., & Дегтерьова, Л. (2006). Сучасна глобалістика: провідні концепції і модерна практика. Київ: Університет «Україна».

5. Бєлоусова, Н. (б. д.). Особливості реалізації стратегії інформаційного суспільства в Європейському Союзі. Проблеми міжнародних відносин: зб. наук. праць, (6), 45–54.

6. Біленчук, П. (2018). Правові засади інформаційної безпеки України. Харків.

7. Білоусов, О. (2013). Розвиток концепцій інформаційного суспільства: від формування теорії постіндустріалізму до сучасності. Актуальні проблеми політики, (49), 60–68

8. Бондар, І. (2014). Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки, (1), 68–75.

9. ВІДЕОФЕЙК: Валерій Залужний записав звернення, де наказує військовим покинути зону бойових дій та захоплювати владу. (2023). Взято з https://voxukraine.org/videofejk-valerij-zaluzhnyj-zapysav-zvernennya-de-nakazuye-vijskovym-pokynuty-zonu-bojovyh-dij-ta-zahoplyuvaty-vladu

10. ВІДЕОФЕЙК: Валерій Залужний створив петицію про мобілізацію депутатів Верховної Ради. (2023). Взято з https://voxukraine.org/videofejk-valerij-zaluzhnyj-stvoryv-petytsiyu-pro-mobilizatsiyu-deputativ-verhovnoyi-rady

11. Войціховський, А. (2020). Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). Вісник Харківського національного університету імені В. Н. Каразіна, (29), 281–288.

12. Горбулін, В. (2014). «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. Стратегічні пріоритети, (4), 5–12

13. Гуржій, Т. (2018). Інформаційне право: виклики гібридної війни. Зовнішня торгівля: економіка, фінанси, право, (4), 16–26

14. Гурковський, В. (2004). Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки (автореф. дис. канд. наук з держ. упр.). Національна академія державного управління при Президентові України

15. Даниленко, С. [С.], Авер'янова, Н., Воропаєва, Т., & Дроботенко, М. (2022). Стратегія «розумної сили» як ключова передумова перемоги України в росіфсько-українській неоімперській війні. Українознавчий альманах, (30), 43–53

16. Даниленко, С. [Сергій]. (2020). Інституціональність дезінформації та симетрична протидії її деструктивному впливу. Biuletyn Monitoring propagandy i dezinformacji, (2), 17–19

17. Даниленко, С. (2013). Інформаційне суспільство в контексті цивілізаційного вибору України. Проблеми міжнародних відносин, (7), 64–76

18. Даниленко, С. [Сергій]. (2021). Перевтілення демократії в інформаційну добу: роль нових медіа та громадянського комунікування. Політичні дослідження, (1), 90–105

19. Даниленко, С. [С.], & Прокопенко, Я. (2011). Інтернет технології як інструмент досягнення зовнішньополітичних цілей. Актуальні проблеми міжнародних відносин, (102), 96–102

20. Даниленко, С. [Сергій]. (2014). Соціальні медіа як інструмент суспільних трансформацій у країнах нестабільних демократій: український досвід. Актуальні проблеми міжнародних відносин, (121), 49–61

21. Даниленко, С., Нестеряк, Ю., & Грінчук, М. (2018). Современные тенденции в сфере коммуникационной безопасности. Wschód Europy, (4), 171–187

22. Даниленко, С. [С.], & Фурсай, О. (2020). Деструктивний інформаційний вплив на соціально-політичні процеси (на прикладі Франції). Вісник Київського національного університету імені Тараса Шевченка: Міжнародні відносини, 1(51), 25–30.

23. Даниленко, Ю. (2020). Фактчек vs. Fakenews: чи допомагає перевірка фактів у Facebook проти поширення дезінформації? Взято з https://voxukraine.org/faktchek-vs-fakenews-chi-dopomagaye-perevirka-faktiv-u-facebook-proti-poshirennya-dezinformatsiyi

24. Державна служба спеціального зв'язку та захисту інформації України. (б. д.). Взято з https://cip.gov.ua/ua

25. Довгань, О. (2017). Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. Київ: Видавничий дім «Артек»

26. Довгань, О. (2014). Національний інформаційний суверенітет – об'єкт інформаційної безпеки. Інформація і право, (3), 102–112

27. Дубов, Д. (2014). Кіберпростір як новий вимір геополітичного суперництва. Київ: НІСД

28. Дубов, Д. (2019). «Роль медіаграмотності у протидії дезінформації, ворожим наративам та операціям впливу». Взято з https://niss.gov.ua/sites/default/files/2019-12/tezy-dubov.pdf

29. Дубов, Д., & Ожеван, М. (2012). Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців: аналітична доповідь. Київ: НІСД.

30. Ісмайлов, К. (2016). Поняття «кібербезпека» та «інформаційна безпека». Типологія безпеки. У Міжнародна науково-практична конференція «Актуальні проблеми автоматизації та управління» (с. 32–33)

31. Зіставлення з реальними фактами: Спростування російської дезінформації щодо НАТО. (2024). Взято з https://www.nato.int/cps/uk/natohq/115204.htm

32. Карпчук, Н., & Юськів, Б. (2022). Інформаційні приводи й інформаційний супровід гібридної війни Російської Федерації проти України. Історико-політичні проблеми сучасного світу: Збірник наукових статей, (45), 71–85

33. Кисельов, С., & Кордун, О. (2019). Реакція на події у світовій політиці та економіці за 1-14.01.2019. протести «жовтих жилетів» у Франції». Взято з https://niss.gov.ua/sites/default/files/2019-02/111AnZap-Protesty-France-1-14.01.2019-e61a4.pdf

34. Кібербезпека та кримінальний аналіз: французькі правоохоронці провели тренінг для українських поліцейських. (2023). Взято з https://www.npu.gov.ua/news/kiberbezpeka-ta-kryminalnyi-analiz-frantsuzki-pravookhorontsi-provely-treninh-dlia-ukrainskykh-politseiskykh?fbclid=IwAR3vdnDkXCkgUB-ldbYeUcK0Wh1slMwZM-PVisVLoOj-zsbfQAaY0U5h3tw

35. Кононенко, В., Здоровко, С., & Корольова, А. (2023). Інформаційна безпека як стан. Науковий вісник Ужгородського Національного Університету, (76), 244–250.

36. Кононенко, В., Новікова, Л., & Копицька, П. (2021). Політика міжнародних організацій з питань інформаційної безпеки. Науковий вісник Ужгородського національного університету. Серія Право, (65), 353–358

37. Копійка, М. (2020). Модернізація політики міжнародних організацій у сфері інформаційної безпеки. Політичне життя, (1), 102–109

38. Коппель, О., & Пархомчук, О. (2022). Мегатренди глобального розвитку. Вісник Національного університету імені Тараса Шевченка, (2), 10–15.

39. Курбан, О. (2016). Сучасні інформаційні війни в мережевому онлайн просторі. Київ: ВІКНУ

40. Литвиненко, О. (2003). Інформаційні впливи та операції. Теоретико-аналітичні нариси: Монографія. Київ: НІСД

41. Лук'янова, В., & Лаутар, А. (2013). Інформаційна безпека в умовах розвитку інформаційної системи. Вісник Хмельницького національного університету, (2), 97–101

42. Ожеван, М. (2016). Глобальна війна стратегічних наративів: виклики та ризики для України. Стратегічні пріоритети, (4), 30–40

43. Ожеван, М. (2010). Інформаційна стратегія нового президента США Барака Обами. Актуальні проблеми міжнародних відносин, (93), 20–25

44. Парахонський, В. (2015). Зовнішня політика України в умовах кризи міжнародного безпекового середовища: аналітична доповідь. Київ: НІСД.

45. Полевий, В. (2018). Визначення поняття інформаційної складової державного суверенітету. Інформаційна безпека людини, суспільства, держави, (1), 136–144.

46. Померанцев, П. (2020). Це не пропанагда. Подорож на війну проти реальності. Київ: Yakaboo Publishing

47. Почепцов, Г. (2019). Дезинформация. Київ

48. Про Національний координаційний центр кібербезпеки, УКАЗ Президента України (2016) (Україна). Взято з https://ips.ligazakon.net/document/U242_16?an=3

49. Про основні засади забезпечення кібербезпеки України, Закон України (2017) (Україна). Взято з https://zakon.rada.gov.ua/laws/show/2163-19#Text

50. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України», Указ Президента України (2020) (Україна). Взято з https://www.president.gov.ua/documents/3922020-35037

51. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», Указ Президента України (2017) (Україна). Взято з https://zakon.rada.gov.ua/laws/show/47/2017#Text

52. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки», Указ Президента України (2021) (Україна). Взято з https://zakon.rada.gov.ua/laws/show/685/2021#Text

53. Солодка, О. (2020). Забезпечення інформаційного суверенітету держави: правовий дискурс. Інформація і право, (1), 80–87

54. Талліннський механізм: Україна та міжнародні партнери започаткували новий інструмент співпраці у кіберпросторі. (2023). Взято з https://www.kmu.gov.ua/news/tallinnskyi-mekhanizm-ukraina-ta-mizhnarodni-partnery-zapochatkuvaly-novyi-instrument-spivpratsi-u-kiberprostori

55. Тоффлер, Е. (2007). Нова парадигма влади. Знання, багатство й сила. Харків: Акта.

56. Угода про співробітництво у сфері безпеки між Україною та Францією. (2024). Взято з https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-89005

57. Угода про співробітництво у сфері безпеки між Україною та Сполученим Королівством Великої Британії і Північної Ірландії. (2024). Взято з https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-88277?fbclid=IwAR1VZ8On-4z3geM2FDeHYVQU7xJRut5fMVBFalER-cUfuRR548xw3pIUeao

58. У Франції вивчають причетність РФ до руху «Жовті жилети». (2018). Взято з https://www.pravda.com.ua/news/2018/12/10/7200753/

59. У Франції наберуть додатково 1500 "кіберпатрульних". (2022). Взято з https://www.epravda.com.ua/news/2022/01/10/681291/

60. Україна на тлі атак РФ здійснила "революцію кіберзахисту" - французький генерал. (2023). Взято з https://www.eurointegration.com.ua/news/2023/01/13/7154086/

61. Україна офіційно приєдналася до Центру кіберзахисту НАТО. (2023). Взято з https://www.ukrinform.ua/rubric-technology/3710022-ukraina-oficijno-priednalasa-do-centru-kiberzahistu-nato.html

62. Україна та ЄС започаткували Кібердіалог. (2021). Взято з https://mfa.gov.ua/news/ukrayina-ta-yes-zapochatkuvali-kiberdialog

63. Українські медіа, ставлення та довіра у 2023 р. (2023). Взято з https://internews.in.ua/wp-content/uploads/2023/10/Ukrainski-media-stavlennia-ta-dovira-2023r.pdf

64. Фахівці НКЦК провели робочу зустріч з представниками французьких компаній у сфері кібербезпеки. (2023). Взято з https://www.rnbo.gov.ua/ua/Diialnist/6079.html

65. Франція виділить кошти на підтримку технологічних стартапів України. (2022). Взято з https://zn.ua/ukr/UKRAINE/frantsija-vidilit-koshti-na-pidtrimku-tekhnolohichnikh-startapiv-ukrajini.html

66. Фролова, О. [О.]. (2019). Міжнародне співробітництво в галузі забезпечення інформаційної безпеки. Вісник Львівського університету. Серія "Міжнародні відносини", (46), 123–136

67. Фролова, О. (2018). Роль ООН в системі міжнародної інформаційної безпеки. Електронне видання Інституту міжнародних відносин. Взято з http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3468/3140

68. About CeMAS. (б. д.). Взято з https://cemas.io/about-cemas/

69. About CERT-UA. (б. д.). Взято з https://cert.gov.ua/about-us

70. About ENISA - The European Union Agency for Cybersecurity. (б. д.). Взято з https://www.enisa.europa.eu/about-enisa

71. About NewsGuard. (б. д.). Взято з https://www.newsguardtech.com/about-newsguard/

72. About the NCSC. (б. д.). Взято з https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

73. Action plan on strategic communications. (2015). Взято з https://www.eeas.europa.eu/sites/default/files/action_plan_on_strategic_communication.docx_eeas_web.pdf

74. Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act). (2017). Взято з https://perma.cc/7UCW-AA3A

75. AFP Factuel. (2024). Взято з https://factuel.afp.com

76. AFP Faktencheck. (б. д.). Взято з https://faktencheck.afp.com/list

77. Agence nationale de la sécurité des systèmes d'information. (2024). Взято з https://cyber.gouv.fr

78. A Global Strategy for the European Union’s Foreign And Security Policy. (2016). Brussels: European Union.

79. Alaphilippe, A., Machado, G., Raquel, M., & Poldi, F. (2022). Doppelganger: Media clones serving Russian propaganda.

80. Anderlini, J., & Caulcutt, C. (2023). Europe must resist pressure to become ‘America’s followers,’ says Macron. Взято з https://www.politico.eu/article/emmanuel-macron-china-america-pressure-interview/

81. Annual patent applications related to artificial intelligence. (б. д.). Взято з https://ourworldindata.org/grapher/artificial-intelligence-patents-submitted?tab=table

82. Antoniuk, D. (2023). Massive ransomware attack hinders services in 70 German municipalities. Взято з https://therecord.media/massive-cyberattack-hinders-services-in-germany

83. Apostle, J., & Kawkabani, R. (2023). France Cybersecurity Update: Cyber-Attacks Must Be Reported to Authorities Within 72-Hours to Benefit from Insurance Coverage. Взято з https://www.orrick.com/en/Insights/2023/02/France-Cybersecurity-Update-Cyber-Attacks-Must-Be-Reported-to-Authorities-Within-72-Hours

84. ARCOM. (2024). Взято з https://www.arcom.fr

85. ARD-FAKTENFINDER. (б. д.). Взято з https://www.tagesschau.de/faktenfinder

86. Arquilla, J., & Ronfeldt, D. (1997). Cyberwar is Coming! Athena’s Camp: Preparing for Conflict in the Information Age, 24–60

87. ASSOCIATION D’ÉDUCATION AUX MÉDIAS ET À L’INFORMATION. (2024). Взято з https://entreleslignes.media

88. Bangemann, M. (1995). Europe and the Global Information Society Recommendations to the European Council. Взято з https://op.europa.eu/en/publication-detail/-/publication/44dad16a-937d-4cb3-be07-0022197d9459/language-en

89. Barnes, J., & Cooper, H. (2019). Trump Discussed Pulling U.S. From NATO, Aides Say Amid New Concerns Over Russia. Взято з https://www.nytimes.com/2019/01/14/us/politics/nato-president-trump.html

90. Bell, D. (1976). The Coming of Post-Industrial Society: A Venture in Social Forecasting. New York: Basic Books.

91. Berzina, K., Kovalčíková, N., & Salvo, D. (2019). European Policy Blueprint for Countering Authoritarian Interference in Democracies. Взято з https://www.gmfus.org/news/european-policy-blueprint-countering-authoritarian-interference-democracies

92. Bilal, A. (2021). Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. NATO Review. Взято з https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

93. Biselli, A. (2023). Bundesrat blockiert Hinweisgeberschutzgesetz. Взято з https://netzpolitik.org/2023/whistleblower-bundesrat-blockiert-hinweisgeberschutzgesetz/

94. Brattberg, E., & Maurer, T. (2018). Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks. Взято з https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

95. Britain, France lead 35 nation agreement on controlling spyware, mercenary hackers. (2024). Взято з https://www.reuters.com/technology/cybersecurity/britain-france-lead-35-nation-agreement-controlling-spyware-mercenary-hackers-2024-02-06/

96. Brooke, H. (2016). Inside the Digital Revolution. Journal of International Affairs, (1), 29–53

97. Bruggemann, M. (2010). Information policy and the public sphere: EU communications and the promises of dialogue and transparency. Javnost – The Public, Journal of the European Institute for Communication and Culture, 17(1), 5–22

98. Brussels Summit Communiqué. (2021). Взято з https://www.nato.int/cps/en/natohq/news_185000.htm

99. Cahyadi, A., & Magda, R. (2021). Digital Leadership in the Economies of the G20 Countries: A Secondary Research. Economies 2021, (9)

100. Campus Cyber. (б. д.). Взято з https://campuscyber.fr

101. Castells, M. (2010). End of Millennium. The Information Age: Economy, Society and Culture. Oxford: Wiley-Blackwell

102. Caulcutt, C. (2023). France condemns Russian disinformation campaign linked to Stars of David graffiti. Взято з https://www.politico.eu/article/france-condemns-russia-involvement-stars-of-david-graffiti/

103. CESG. (б. д.). Взято з https://www.gov.uk/government/organisations/cesg

104. Chan, S. (2017). Fearful of Hacking, Dutch Will Count Ballots by Hand. Взято з https://www.nytimes.com/2017/02/01/world/europe/netherlands-hacking-concerns-hand-count-ballots.html

105. CHAPTER 3 HEARTS AND MINDS: Enhancing societal resilience against disinformation. (2019). Взято з https://www.jstor.org/stable/resrep21143.7

106. Chin, K. (2024). Biggest Data Breaches in the UK. Взято з https://www.upguard.com/blog/biggest-data-breaches-uk

107. Chin, K. (2023). Cybersecurity Laws and Regulations in Germany. Взято з https://www.upguard.com/blog/cybersecurity-laws-and-regulations-germany

108. Chin, K. (2024b). List of Biggest Data Breaches in France. Взято з https://www.upguard.com/blog/biggest-data-breaches-france

109. Chłoń, T. (2022). NATO and Countering Disinformation: The Need for a More Proactive Approach from the Member States

110. Chong, A. (2015). Smart Power and Military Force: An Introduction. Journal of Strategic Studies, (38), 233–244

111. Collective defence and Article 5. (2023). Взято з https://www.nato.int/cps/en/natohq/topics_110496.htm

112. Commit to transparency — sign up for the International Fact-Checking Network's code of principles. (2024). Взято з https://www.ifcncodeofprinciples.poynter.org

113. Compendium on Cyber Security of Election Technology. (2018).

114. Commission opens formal proceedings against X under the Digital Services Act. (2023). Взято з https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6709

115. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Tackling online disinformation: a European Approach. (2018). Взято з https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

116. Communiqué des ministres des affaires étrangères du G7 sur leurs convergences de vue en matière de politique étrangère, le 6 avril 2019. (2019). Взято з https://www.vie-publique.fr/discours/268996-ministere-de-leurope-et-des-affaires-etrangeres-06042019-g7

117. Conolly, K. (2024). Germany unearths pro-Russia disinformation campaign on X. Взято з https://www.theguardian.com/world/2024/jan/26/germany-unearths-pro-russia-disinformation-campaign-on-x.

118. CONSEIL DE DÉONTOLOGIE JOURNALISTIQUE ET DE MÉDIATION. (2024). Взято з https://cdjm.org

119. CONSTANTINESCU, V. (2023). Russian Cybercrime Group Attacks Germany for Helping Ukraine. Взято з https://www.bitdefender.com/blog/hotforsecurity/russian-cybercrime-group-attacks-germany-for-helping-ukraine/

120. Convention on cybercrime. (2022)

121. CORRECTIV - Über uns. (б. д.). Взято з https://correctiv.org/ueber-uns/

122. Countering Influence Operations. (б. д.). Взято з https://carnegieendowment.org/specialprojects/counteringinfluenceoperations

123. Covid-19 : le vaccin, un nouvel enjeu de pouvoir à l'échelle mondiale. (2021). Взято з https://www.francetvinfo.fr/sante/maladie/coronavirus/vaccin/covid-19-le-vaccin-un-nouvel-enjeu-de-pouvoir-a-l-echelle-mondiale_4348763.html

124. Cyber defence. (2023). Взято з https://www.nato.int/cps/en/natohq/topics_78170.htm

125. Cyber Defence Pledge. (2016). Взято з https://www.nato.int/cps/en/natohq/official_texts_133177.htm

126. Cyber Norm Initiative: Synthesis of Lessons Learned and Best Practices. (2019). Взято з https://www.diplomatie.gouv.fr/IMG/pdf/_eng_synthesis_cyber_norm_initiative_cle44136e.pdf

127. Cybersécurité : Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans le cyberespace. (2018). Взято з https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/les-domaines-d-action-de-la-diplomatie-numerique-francaise/garantir-la-securite-internationale-du-cyberespace-a-travers-le-renforcement-de/article/cybersecurite-appel-de-paris-du-12-novembre-2018-pour-la-confiance-et-la

128. Cybersecurity and New Technologies. (2023)

129. Cyber security breaches survey 2023. (2023). Взято з https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023#chapter-4-prevalence-and-impact-of-breaches-or-attacks

130. Cyber Security Strategy. (2011). Взято з https://www.gov.uk/government/publications/cyber-security-strategy

131. Danylenko, S., & Shustenko, S. (2020). Activities of the Council of Europe in ensuring the human right to information: issues of compliance with the modern challenges of democracy. Central European Political Studies, (3), 133–146

132. Danylenko, S., & Fursai, O. (2022). «Vaccinodemic» as a component of the global hybrid conflict between democracy and autocracy: the case of Ukraine. «Rocznik Instytutu Europy Środkowo-Wschodniej», (20), 19–45.

133. Déclaration conjointe du président de la République française Emmanuel Macron et de la Première ministre de Nouvelle-Zélande Jacinda Ardern à l'occasion du Sommet de l'Appel de Christchurch 2022. (2022). Взято з https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-

numerique/actualites-et-evenements/article/declaration-conjointe-du-president-de-la-republique-francaise-emmanuel-macron

134. Deepfake video of German chancellor sparks angry reaction. (2023). Взято з https://www.aa.com.tr/en/europe/deepfake-video-of-german-chancellor-sparks-angry-reaction/3066455

135. Deepfake video of Volodymyr Zelensky surrendering surfaces on social media. (2022). Взято з https://www.youtube.com/watch?v=X17yrEV5sl4

136. DeTOX: A french-funded project on deepfake detection targeting important civilian and military personalities in France. (2023). Взято з https://eurecom-blog.medium.com/detox-a-french-funded-project-on-deepfake-detection-targeting-important-civilian-and-military-23c30262ee3d

137. Dieudonné, D. (2017). Fact-checking the French election: lessons from CrossCheck, a collaborative effort to combat misinformation. Взято з https://blog.google/outreach-initiatives/google-news-initiative/fact-checking-french-election-lessons-crosscheck-collaborative-effort-combat-misinformation/

138. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive (1995) (EU). Взято з https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046

139. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Directive № 2016/1148 (2016) (EU).

140. DISINFORMATION LANDSCAPE IN FRANCE. (2023). Взято з https://www.disinfo.eu/wp-content/uploads/2023/03/20230224_FR_DisinfoFS.pdf

141. Doffman, Z. (2019). Cyber Warfare: Army Deploys «Social Media Warfare» Division To Fight Russia. Взято з https://www.forbes.com/sites/zakdoffman/2019/08/01/social-media-warfare-new-military-cyber-unit-will-fight-russias-dark-

arts/?ss=cybersecurity&fbclid=IwAR2j_7UEPuBQH_8rbKWn61MFJDpOMNliFZRn2xKbL38oxDVVGHfNhIznUtM&sh=7dd38e694f6e

142. Dönmez, Ü. (2023). France accuses Russia of being behind major disinformation campaign. Взято з https://www.aa.com.tr/en/europe/france-accuses-russia-of-being-behind-major-disinformation-campaign/2921578

143. Doppelganger operation. (2023). Взято з https://www.disinfo.eu/doppelganger-operation

144. Drucker, P. (2001). Management Challenges for the 21st Century

145. Duboust, O. (2024). Data of half the population of France stolen in its largest ever cyberattack. This is what we know. Взято з https://www.euronews.com/next/2024/02/08/data-of-33-million-people-in-france-stolen-in-its-largest-ever-cyberattack-this-is-what-we

146. Duff, A. (1998). Daniel Bell's theory of the information society. Journal of Information Science, (24), 373–455

147. Dzitac, D. (2023). Home Data Science in Applications Chapter The Soft Power of Understanding Social Media Dynamics: A Data-Driven Approach. Data Science in Applications. Studies in Computational Intelligence, (1084)

148. Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States. (2023). Взято з https://www.osce.org/files/f/documents/2/7/539108_0.pdf

149. ENISA meets cyber-experts to plan Cyber Europe 2018. (2017). Взято з https://www.enisa.europa.eu/news/enisa-news/enisa-meets-cyber-experts-to-plan-cyber-europe-2018

150. EU cybersecurity initiatives: working towards a more secure online environment. (2017). Взято з https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

151. European Council meeting (19 and 20 March 2015) – Conclusions. (2015). Взято з https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf

152. European Cybersecurity Journal: strategic perspectives on cybersecurity management and public policies (3-тє вид.). (2017). The Kosciuszko Institute

153. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties. (2016). Взято з https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.html

154. European Union Internet Forum (EUIF). (б. д.). Взято з https://home-affairs.ec.europa.eu/networks/european-union-internet-forum-euif_en

155. EUvsDisinfo. (б. д.). Взято з https://euvsdisinfo.eu

156. EUvsDisinfo: how to debunk over 6,500 disinformation cases in four years? (2019). Взято з https://www.eeas.europa.eu/eeas/euvsdisinfo-how-debunk-over-6500-disinformation-cases-four-years_en

157. Evaluation of the EU decentralised agencies in 2009 (Звіт Європейської комісії). (2009). Brussels

158. Exercises & Training. (б. д.). Взято з https://shape.nato.int/exercises

159. Facebook, Google partner with French media to combat ‘fake news’. (2017). Взято з https://www.france24.com/en/20170206-facebook-google-partner-with-french-media-combat-fake-news

160. Factsheet: Rapid Alert System. (2019). Взято з https://www.eeas.europa.eu/node/59644_en

161. Faktencheck bei dpa. (б. д.). Взято з https://www.dpa.com/de/faktencheck#faktencheck-bei-dpa

162. #FAKTENFUCHS. (б. д.). Взято з https://www.br.de/nachrichten/faktenfuchs-faktencheck,QzSIzl3

163. Federal Office for Information Security. (б. д.). Взято з https://www.bsi.bund.de/DE/Home/home_node.html

164. Filippone, D. (2019). Le ministère des Armées signe une convention cyberdéfense avec 8 industriels. Взято з https://www.lemondeinformatique.fr/actualites/lire-le-ministere-des-armees-signe-une-convention-cyberdefense-avec-8-industriels-77100.html

165. Fondation Descartes. (2024). Взято з https://www.fondationdescartes.org

166. France launches «cyber city» to pool resources for better digital security. (2022). Взято з https://www.rfi.fr/en/france/20220216-france-launches-cyber-city-to-pool-resources-for-better-digital-security

167. France Slams Russia's Sputnik Vaccine as 'Propaganda' Tool. (2021). Взято з https://www.themoscowtimes.com/2021/03/26/france-slams-russias-sputnik-vaccine-as-propaganda-tool-a73377

168. France's response to Resolution 73/27 and Resolution 73/266. (2019). Взято з https://www.diplomatie.gouv.fr/IMG/pdf/190514-_french_reponse_un_resolutions_73-27_-_73-266_ang_cle4f5b5a-1.pdf

169. France uncovers a vast Russian disinformation campaign in Europe. (2024). Взято з https://www.economist.com/europe/2024/02/12/france-uncovers-a-vast-russian-disinformation-campaign-in-europe

170. France uncovers Russia's disinformation campaign justifying war in Ukraine. (2024). Взято з https://www.pravda.com.ua/eng/news/2024/02/12/7441555/

171. Freedman, R. (2023). Sweeping EU digital misinformation law takes effect. Взято з https://www.legaldive.com/news/digital-services-act-dsa-eu-misinformation-law-propaganda-compliance-facebook-gdpr/691657/

172. French National Digital Security Strategy. (2015).

173. French report flags Azeri-linked disinformation campaign targeting 2024 Olympics. (2023). Взято з https://www.aol.com/french-report-flags-azeri-linked-180606549.html

174. Friedman, O. (2019). Hybrid Conflicts and Information Warfare: New Labels, Old Politics. Boulder: Lynne Rienner

175. Friedman, T. (1999). The Lexus and the Olive Tree. New York: Farrar Straus & Giroux

176. Friedman, T. (2007). The world is flat: a brief history of the twenty-first century. New York: Farrar, Straus and Giroux

177. Funding NATO. (2024). Взято з https://www.nato.int/cps/en/natohq/topics_67655.htm

178. Gallarotti, G. (2010). Cosmopolitan Power in International Relations: A Synthesis of Realism, Neoliberalism, and Constructivism. Cambridge: Cambridge University Press

179. Gallarotti, G. (2015). Smart Power: Definitions, Importance, and Effectiveness. Journal of Strategic Studies, (38), 245–281

180. Ganguly, M., & Conn, D. (2023). French broadcaster BFMTV suspends presenter amid disinformation scandal. Взято з https://www.theguardian.com/world/2023/feb/15/french-broadcaster-bfmtv-suspends-presenter-disinformation-scandal-rachid-mbarki

181. General Data Protection Regulation. (б. д.). Взято з https://gdpr-info.eu

182. General Report. (2008). Взято з https://www.enisa.europa.eu/publications/corporate/enisa_gr_2008.pdf

183. Germany (DE). (2021). Взято з https://www.cyberwiser.eu/germany-de

184. Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy. (2021). Взято з https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

185. Global Power Index 2023 Report. (2024)

186. Gooding, M. (2023). UK government's NCF hackers have launched cyberattacks on enemies – GCHQ. Взято з https://techmonitor.ai/technology/cybersecurity/gchq-cyber-attacks-uk-hackers-russia

187. Háberová, B. (2019). Social media as new source of soft power. Взято з https://www.iir.cz/social-media-as-new-source-of-soft-power

188. Hague, W. (2011). Security and freedom in the cyber age - seeking the rules of the road. Взято з https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road

189. Hartmann, T. (2023). «Sécurisation et régulation de l'espace numérique»: ce que contient le projet de loi. Взято з https://www.euractiv.fr/section/plateformes/news/la-france-propose-un-texte-de-

combat-numerique/?_ga=2.134329523.39570210.1703355257-1872606923.1703355255

190. Hentzen, P.-Y. (2021). National Strategy for Cybersecurity: the French response to the threat. Взято з https://www.stormshield.com/news/national-strategy-for-cybersecurity-the-french-response-to-the-threat/

191. Holroyd, M. (2022). French election 2022: Misinformation spreads online ahead of the first round vote. Взято з https://www.euronews.com/my-europe/2022/04/08/french-election-2022-misinformation-spreads-online-ahead-of-the-first-round-vote

192. Horbulin, V. (2017). The World Hybrid War: Ukrainian Forefront. Kharkiv: Folio.

193. Information security. (б. д.). Взято з https://csrc.nist.gov/glossary/term/information_security

194. Information Security Policy Directive for the United Nations Secretariat (б. д.). Взято з https://iseek-external.un.org/system/files/iseek/LibraryDocuments/1630-20130314106273998754.pdf

195. INFOSEC. (б. д.). Взято з https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing/isacs-toolkit/glossary/infosec

196. Interstate Media Treaty (Medienstaatsvertrag). (2020). Взято з https://www.die-medienanstalten.de/fileadmin/user_upload/Rechtsgrundlagen/Gesetze_Staatsvertraege/Interstate_Media_Treaty_en.pdf

197. ISD Geschichte. (б. д.). Взято з https://isdgermany.org/#geschichte

198. Janczewski, L., & Colarik. A. (2008). Cyber Warfare and Cyber Terrorism. Hershey: Information Science Reference

199. Jankowicz, N., & Pierson, S. (2020). Freedom and Fakes: A Comparative Exploration of Countering Disinformation and Protecting Free Expression.

200. Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity strategy of the European Union: an Open, Safe and Secure Cyberspace Cybersecurity

Strategy of the European Union: An Open, Safe and Secure Cyberspace. (2013). Взято з https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001

201. Joint communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response. (2016). Взято з https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018

202. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Report on the implementation of the Action Plan Against Disinformation. (2019). Взято з https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=comnat:JOIN_2019_0012_FIN

203. Joint press conference by NATO Secretary General Jens Stoltenberg, President of the European Council Charles Michel and President of the European Commission, Ursula von der Leyen. (2023). Взято з https://www.nato.int/cps/en/natohq/opinions_210551.htm

204. Karlsen, G. H. (2019). Divide and rule: ten lessons about Russian political influence activities in Europe. Nature. Взято з https://www.nature.com/articles/s41599-019-0227-8

205. Kavanagh, C. (2017). The United Nations, Cyberspace and International Peace and Security.

206. Kayali, L., & Calcutt, C. (2023). France exposes mega Russian disinformation campaign. Взято з https://www.politico.eu/article/france-accuses-russia-of-wide-ranging-disinformation-campaign/

207. Kharpal, A. (2023). France makes high-profile push to be the A.I. hub of Europe setting up challenge to U.S., China. Взято з https://www.cnbc.com/2023/06/19/france-makes-push-to-be-europes-ai-hub-setting-up-us-challenge-.html

208. Kofman, M., & Rojansky, M. (2015). Closer Look at Russia's «Hybrid War». Взято з https://www.wilsoncenter.org/sites/default/files/media/documents/publication/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf

209. Kong, W. (2005). Information Sovereignty Reviewed. Intercultural Communication Studies, (14), 119–135

210. Kong, W. [W.], & Marler, T. (2022). Ukraine's Lessons for the Future of Hybrid Warfare. Взято з https://nationalinterest.org/feature/ukraine's-lessons-future-hybrid-warfare-205922

211. Le commandement de la cyberdéfense (COMCYBER). (б. д.). Взято з https://www.defense.gouv.fr/comcyber/nous-connaitre

212. La France et la cybersécurité. (2022). Взято з https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/lutter-contre-la-criminalite-organisee/la-france-et-la-cybersecurite/

213. Landi, M. (2023). 'Robust mechanisms' will fight AI deepfakes before election, minister says. Взято з https://www.independent.co.uk/news/uk/politics/government-mps-rishi-sunak-national-cyber-security-centre-mayor-b2463309.html

214. Larsen, J. (2014). The Wales Summit and NATO's Deterrence Capabilities: An Assesment. Взято з https://www.files.ethz.ch/isn/186010/11Nov14_Rep_Assess_Wales_Summit_NATOs_Det_Cap.pdf

215. LA STRATÉGIE NATIONALE POUR L\'INTELLIGENCE ARTIFICIELLE. (2018). Взято з https://www.entreprises.gouv.fr/fr/numerique/enjeux/la-strategie-nationale-pour-l-ia

216. Laudrain, A. (2021). France Doubles Down on Countering Foreign Interference Ahead of Key Elections. Взято з https://www.lawfaremedia.org/article/france-doubles-down-countering-foreign-interference-ahead-key-elections-0

217. Le Règlement européen sur les services numériques (DSA) : protéger les droits des citoyens sur internet. (2023). Взято з https://www.arcom.fr/actualites/le-reglement-europeen-sur-les-services-numeriques-dsa-proteger-les-droits-des-citoyens-sur-internet

218. Libicki, M. (1995). What is Information Warfare. Washington: National Defense University Strategic Forum

219. Lisbon Summit Declaration. (2010). Взято з https://www.nato.int/cps/en/natohq/official_texts_68828.htm

220. Loi du 29 juillet 1881 sur la liberté de la presse. (б. д.). Взято з https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006070722

221. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l\'économie numérique (1). (2004). Взято з https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164

222. Loi n° 2010-1 du 4 janvier 2010 relative à la protection du secret des sources des journalistes (1). (2010). Взято з https://www.legifrance.gouv.fr/loda/id/JORFTEXT000021601325

223. Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information [Електронний ресурс] // Legifrance. – 2018. – Режим доступу до ресурсу: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559/

224. Loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte. (2022). Взято з https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045388745

225. Macron announces €1bn security package after cyberattacks on French hospitals. (2021). Взято з https://www.thelocal.fr/20210219/macron-announces-1bn-security-package-after-cyberattacks-on-french-hospitals

226. MANIFESTE POUR UNE ÉTHIQUE DU NUMÉRIQUE. (2021). Взято з https://www.ccne-ethique.fr/cnpen

227. Marzouki, Y., & Oullier, O. (2012). Revolutionizing Revolutions: Virtual Collective Consciousness and the Arab Spring. Взято з https://www.huffpost.com/entry/revolutionizing-revolutio_b_1679181

228. Masuda, Y. (1985). Hypothesis on the genesis of homo intelligens. Futures. Guilford, (17), 479–494

229. Medialab. (б. д.). Взято з https://www.afp.com/en/agency/medialab

230. Media & News Survey 2022. (2022). Взято з https://europa.eu/eurobarometer/surveys/detail/2832

231. Military Spending by Country. (2024). Взято з https://wisevoter.com/country-rankings/military-spending-by-country/

232. Minister launches new strategy to fight online disinformation. (2021). Взято з https://www.gov.uk/government/news/minister-launches-new-strategy-to-fight-online-disinformation

233. MISSION STATEMENT. (2023). Взято з https://mfa.gov.ua/storage/app/sites/1/tm-mission-statement.pdf

234. Morgenthau, H. (1948). Politics among nations: the struggle for peace and power

235. Moulson, G., & Gera, V. (2024). Germany, France and Poland vow to procure more weapons for Ukraine in a show of unity. Взято з https://apnews.com/article/germany-france-poland-ukraine-military-support-2b6615f15e05f166910c3141d3baac0f

236. Myers, S., & Browning, K. (2023). Russia Takes Its Ukraine Information War Into Video Games. Взято з https://www.nytimes.com/2023/07/30/technology/russia-propaganda-video-games.html

237. National Cyber Security Strategy 2016 to 2021. (2016). Взято з https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

238. National Cyber Strategy 2022. (2022). Взято з https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

239. National Cyber Strategy 2022: Policy Paper. (2022). Взято з https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

240. National Protective Security Authority. (б. д.). Взято з https://www.npsa.gov.uk

241. NATO Agency, Oracle sign cyber information sharing agreement. (2019). Взято з https://www.ncia.nato.int/about-us/newsroom/nato-agency--oracle-sign-cyber-information-sharing-agreement-.html

242. NATO and European Union leadership sign third joint declaration. (2023). Взято з https://www.nato.int/cps/en/natohq/news_210523.htm

243. NATO 2030 and the new Strategic Concept. (2022). Взято з https://natolibguides.info/nato2030/2022strategicconcept

244. NATO launches Industry Cyber Partnership. (2014). Взято з https://www.ncia.nato.int/about-us/newsroom/nato-launches-industry-cyber-partnership.html

245. NATO's approach to countering disinformation [Прес-реліз]. (2023). NATO. Взято з https://www.nato.int/cps/ru/natohq/topics_219728.htm?selectedLocale=en

246. NATO 2022: Strategic Concept. (2022). Взято з https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

247. New leader for NATO's Cyber Security Centre. (2023). Взято з https://www.ncia.nato.int/about-us/newsroom/new-leader-for-natos-cyber-security-centre.html

248. NIS Cooperation Group. (2023). Взято з https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

249. Nissen, T. (2016). Social Media's Role in «Hybrid Strategies». Взято з https://stratcomcoe.org/cuploads/pfiles/tomas_nissen_article_12-09-2016.pdf

250. Nussbaum, A. (2021). Macron Rushes to Shore Up French Cyber Defenses After Attacks. Взято з https://www.bloomberg.com/news/articles/2021-02-17/france-s-macron-boosts-cyber-security-spending-after-attacks

251. Nye, J., & Armitage, R. (2007). Afterword: Election '08, Smart Power '09 in Global 177 Forecast: The Top Security Challenges of 2008. Взято з https://www.csis.org/analysis/afterword-election-08-smart-power-09-global-forecast-topsecurity-challenges-2008

252. Nye, J. (1991). Bound to Lead: The Changing Nature of American Power.

253. Nye, J., Cohen, C., & Armitage, R. (2007). A smarter, more secure America. Report of the CSIS Commission on Smart Power. Взято з http://csis.org/publication/smarter-more-secure-america

254. Nye, J. (2004). Soft Power. the Means to Success in World Politics. New York: Public Affairs

255. O'Carroll, L. (2023). X to be investigated for allegedly breaking EU laws on hate speech and fake news. Взято з https://www.theguardian.com/technology/2023/dec/18/x-to-be-investigated-for-allegedly-breaking-eu-laws-on-hate-speech-and-fake-news

256. Odebade, A., & Benkhelifa, E. (б. д.). Evaluating the impact of government Cyber Security initiatives in the UK. Взято з https://arxiv.org/ftp/arxiv/papers/2303/2303.13943.pdf

257. OSCE – Vive préoccupation vis-à-vis de la situation des droits de l'Homme en Biélorussie (11 mai 2023). (2023). Взято з https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/la-france-et-l-europe/evenements-et-actualites-lies-a-la-politique-europeenne-de-la-france/actualites-europeennes/article/osce-vive-preoccupation-vis-a-vis-de-la-situation-des-droits-de-l-homme-en

258. 82% of French people say they are worried about the global risks of cyber-attacks. (2022). Взято з https://www.ipsos.com/en/82-french-people-say-they-are-worried-about-global-risks-cyber-attacks

259. Okinawa Charter on Global Information Society (б. д.). Взято з https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html#:~:text=We%20will%20exercise%20our%20leadership,undermine%20the%20integrity%20of%20the

260. Palma, B. (2024). AI is transforming cybersecurity: How can security experts respond? Взято з https://www.weforum.org/agenda/2024/01/arms-race-cybersecurity-ai/

261. Pamment, J. (2020). EU Code of Practice on Disinformation: Briefing Note for the New European Commission. Взято з https://carnegieendowment.org/2020/03/03/eu-code-of-practice-on-disinformation-briefing-note-for-new-european-commission-pub-81187

262. Papakonstantinou, V. (2022). Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity? Computer Law & Security Review, (44)

263. Pareto Economics: About us. (2024). Взято з https://pareto-economics.com/about-us/

264. Paris Call. (2024). Взято з https://pariscall.international/en/

265. Paul, C., & Matthews, M. (2016). The Russian "Firehose of Falsehood" Propaganda Model. Взято з https://www.rand.org/pubs/perspectives/PE198.html

266. Pipchenko, N. (2020). Digital diplomacy: how international actors transform their foreign policy activity. Ukraine Analytica, (2), 19–26

267. Piquard, A. (2024). France agrees to ratify the EU Artificial Intelligence Act after seven months of resistance. Взято з https://www.lemonde.fr/en/economy/article/2024/02/03/france-agrees-to-ratify-the-eu-artificial-intelligence-act-after-seven-months-of-opposition_6489701_19.html

268. POUR UNE COORDINATION DE LA CYBERDÉFENSE PLUS OFFENSIVE DANS LA LOI DE PROGRAMMATION MILITAIRE 2024-2030. (б. д.). Взято з https://www.senat.fr/rap/r22-638/r22-638-syn.pdf

269. Prague Summit Declaration. (2002). Взято з https://www.nato.int/docu/pr/2002/p02-127e.htm

270. Protect The Future. (2024). Взято з https://www.nato.int/protect-the-future/

271. Rahman-Jones, I., & Vallance, C. (2023). Online Safety Bill: divisive internet rules become law. Взято з https://www.bbc.com/news/technology-67221691

272. Rawlinson, K. (2015). "Islamist cyber attacks" hit France. Взято з https://sd-magazine.com/?p=1638

273. Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information

Security (ENISA) and repealing Regulation (EC) No 460/2004 Text with EEA relevance, Regulation № 526/2013 (2013) (EU)

274. Revue stratégique de cyberdéfense. (2018). Взято з https://www.sgdsn.gouv.fr/publications/revue-strategique-de-cyberdefense

275. Riga Summit Declaration. (2006). Взято з https://www.nato.int/cps/en/natohq/official_texts_37920.htm

276. Rinke, A. (2023). Exclusive: Germany, France and Italy reach agreement on future AI regulation. Взято з https://www.reuters.com/technology/germany-france-italy-reach-agreement-future-ai-regulation-2023-11-18/

277. Robin, M. (2023). Les politiques européennes de lutte contre la propagande. Взято з https://www.robert-schuman.eu/questions-d-europe/0665-les-politiques-europeennes-de-lutte-contre-la-propagande

278. Rolland, S. (2019). French Tech : Macron annonce 5 milliards d\'euros pour les startups en hyper-croissance. Взято з https://www.latribune.fr/technos-medias/innovation-et-start-up/french-tech-macron-annonce-5-milliards-d-euros-pour-les-startups-en-hyper-croissance-828279.html

279. RRN. A complex and persistent information manipulation campaign [Прес-реліз]. (2023). Paris: Ministry for Europe and Foreign Affairs of France.

280. RSF et ses partenaires dévoilent la “Journalism Trust Initiative (JTI)”, un dispositif innovant contre la désinformation. (б. д.). Взято з https://rsf.org/fr/rsf-et-ses-partenaires-dévoilent-la-journalism-trust-initiative-jti-un-dispositif-innovant-contre

281. Russian hackers strike French National Assembly website. (2023). Взято з https://www.politico.eu/article/french-national-assembly-website-russian-cyberattack-hack-kremlin-emmanuel-macron

282. Schifrin, N. (2017). Social media giants are vulnerable to foreign propaganda. What can they do to change? Взято з https://www.pbs.org/newshour/show/social-media-giants-are-vulnerable-to-foreign-propaganda-what-can-they-do-to-change

283. Sciutto, J. (2024). Trump will pull US out of NATO if he wins election, ex-adviser warns. Взято з https://edition.cnn.com/2024/02/12/politics/us-out-nato-second-trump-term-former-senior-adviser/index.html

284. Second act on increasing the security of IT systems (German IT Security Act 2.0). (2021). Взято з https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/IT-SiG/2-0/it_sig_2-0

285. Securing free and fair European elections: Council adopts conclusions. (2019). Взято з https://www.consilium.europa.eu/en/press/press-releases/2019/02/19/securing-free-and-fair-european-elections-council-adopts-conclusions/

286. Sedliar, Y., Sapsai, A., & Tsyrfa, Y. (2023). Political and legal assessment of the Budapest Memorandum: From Ukraine's renunciation of nuclear weapons to the annexation of the Crimean Peninsula. Social & Legal Studios, (3), 153–160

287. Service de vigilance et protection contre les ingérences numériques étrangères. (2022). Взято з https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques

288. Silomon, J. (2020). The Düsseldorf Cyber Incident. Взято з https://ifsh.de/en/news-detail/the-duesseldorf-cyber-incident

289. SOMA - About us. (2024). Взято з https://www.disinfobservatory.org/about-us/

290. Sotto, P., & Leicester, J. (2017). French cybersecurity agency to probe Macron hacking attack. Взято з https://www.cbc.ca/news/world/france-election-hack-lead-emmanuel-macron-marie-lepen-1.4103148

291. Statistics. (б. д.). Взято з https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

292. Stein, G. (1995). Information Warfare. Airpower Journal

293. Stolton, S. (2020). EU Rapid Alert System used amid coronavirus disinformation campaign. Взято з https://www.euractiv.com/section/media/news/eu-alert-triggered-after-coronavirus-disinformation-campaign/

294. Strafgesetzbuch. (б. д.). Взято з https://dejure.org/gesetze/StGB/130.html

295. Strategic communications. (б. д.). Взято з https://www.eeas.europa.eu/taxonomy/term/400164_en

296. Strategic Concept 2010. (2010). Взято з https://www.nato.int/cps/en/natohq/topics_82705.htm

297. Stratégie internationale de la France pour le numérique. (2015). Взято з https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf

298. Study: Over 80% of people in the UK regularly come across fake news. (2022). Взято з https://newsworks.org.uk/news-and-opinion/study-over-80-of-people-in-the-uk-regularly-come-across-fake-news/

299. Sur internet. (б. д.). Взято з https://www.interieur.gouv.fr/Archives/Archives-des-sous-rubriques/Conseils-pratiques/Sur-internet

300. Survey finds more than 50% of German companies victim of cyberattacks. (2023). Взято з https://www.thestar.com.my/tech/tech-news/2023/10/10/survey-finds-more-than-50-of-german-companies-victim-of-cyberattacks

301. Szafranski, R. (1995). Theory of Information Warfare. Airpower Journal.

302. The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. (2023). Взято з https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

303. The 2022 Code of Practice on Disinformation. (2022). Взято з https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

304. The Christchurch Call. (2024). Взято з https://www.christchurchcall.com

305. The Digital Services Act (DSA). (б. д.). Взято з https://www.eu-digital-services-act.com

306. The EU Cybersecurity Act. (2019). Взято з https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

307. The EU's Cybersecurity Strategy for the Digital Decade. (2020). European Commission. Взято з https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

308. The Global Forum on Digital Security for Prosperity. (б. д.). Взято з https://www.oecd.org/digital/global-forum-digital-security/

309. The Global Risks. Report 2024. (19-те вид.). (2024). World Economic Forum.

310. The Kremlin's Efforts to Covertly Spread Disinformation in Latin America [Прес-реліз]. (2023). U.S. Department of State. Взято з https://www.state.gov/the-kremlins-efforts-to-covertly-spread-disinformation-in-latin-america

311. The National Cyber Response Centre. (б. д.). Взято з https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/Nationales-Cyber-Abwehrzentrum/nationales-cyber-abwehrzentrum.html

312. The near-term impact of AI on the cyber threat. (2024). Взято з https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

313. The State of IT Security in Germany. (2023). Взято з https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

314. The State of IT Security in Germany in 2023 at a Glance. (2023). Взято з https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/Lagebericht2023-Doppelseite_e.pdf?__blob=publicationFile&v=5

315. Timeline. (2022). Взято з https://www.bsi.bund.de/EN/Das-BSI/Zeitstrahl/BSI-Zeitstrahl_node.html

316. Toffler, A. (б. д.). The Third Wave. Взято з https://calculemus.org/lect/07pol-gosp/arch/dekalog-dawne/materialy/waves.htm

317. Touraine, A. (1971). The Post-Industrial Society. Tomorrow's Social History: Classes, Conflicts and Culture in the Programmed Society. New York: Random House

318. UK exposes attempted Russian cyber interference in politics and democratic processes. (2023). Взято з https://www.gov.uk/government/news/uk-exposes-attempted-russian-cyber-interference-in-politics-and-democratic-processes

319. UK launches first national CERT. (2014). Взято з https://www.gov.uk/government/news/uk-launches-first-national-cert

320. vera.ai. (б. д.). Взято з https://www.veraai.eu/home

321. Video game clips misleadingly shared amid Israel-Hamas war. (2023). Взято з https://factcheck.afp.com/doc.afp.com.33XX8DR

322. Vilnius Summit Communiqué. (2023). Взято з https://www.nato.int/cps/en/natohq/official_texts_217320.htm

323. Voo, J., Hemani, I., & Cassidy, D. (2022). National Cyber Power Index 2022. Взято з https://www.belfercenter.org/publication/national-cyber-power-index-2022

324. Walker, C., Kalathil, S., & Ludwig, J. (2018). Soft power is out; sharp power is in. Here's how to win the new influence wars. Взято з https://foreignpolicy.com/2018/09/14/forget-hearts-and-minds-sharp-power

325. Webster, F. (2013). Theories of the Information Society

326. What Is Information Security? (б. д.). Взято з https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

327. What is information security (InfoSec)? (б. д.). Взято з https://www.microsoft.com/en-au/security/business/security-101/what-is-information-security-infosec

328. What we do (ANSSI). (2022). Взято з https://cyber.gouv.fr/en/what-we-do

329. WHISTLEBLOWING: THE GERMAN PARLIAMENT PASSES THE WHISTLEBLOWER PROTECTION ACT. (2022). Взято з https://www.herbertsmithfreehills.com/insights/2022-12/whistleblowing-the-german-parliament-passes-the-whistleblower-protection-act#:~:text=This%20is%20the%20aim%20of,implements%20EU%20requirements%20(delayed)

330. Willsher, K. (2022). Europe must be more independent and shore up its defence, says Macron. Взято з https://www.theguardian.com/world/2022/mar/03/europe-must-become-more-independent-shore-up-defence-emmanuel-macron

331. Witner, J. (2020). Defining Hybrid Warfare. per Concordiam: Journal of European Security and Defense Issues, (10), 7–15

332. Wren, A., & Allison, N. (2024). Trump has an early lead on Biden. But problems are piling up around him. Взято з https://www.politico.com/news/2024/03/21/trump-biden-polling-lead-problems-00148131

333. Yuskiv, B., Karpchuk, N., & Khomych, S. (2021). Media reports as a tool of hybrid and information warfare (the case of RT – Russia Today). Codrul Cosminului, XXVII, (1), 235–258

ДОДАТКИ

ДОДАТОК А

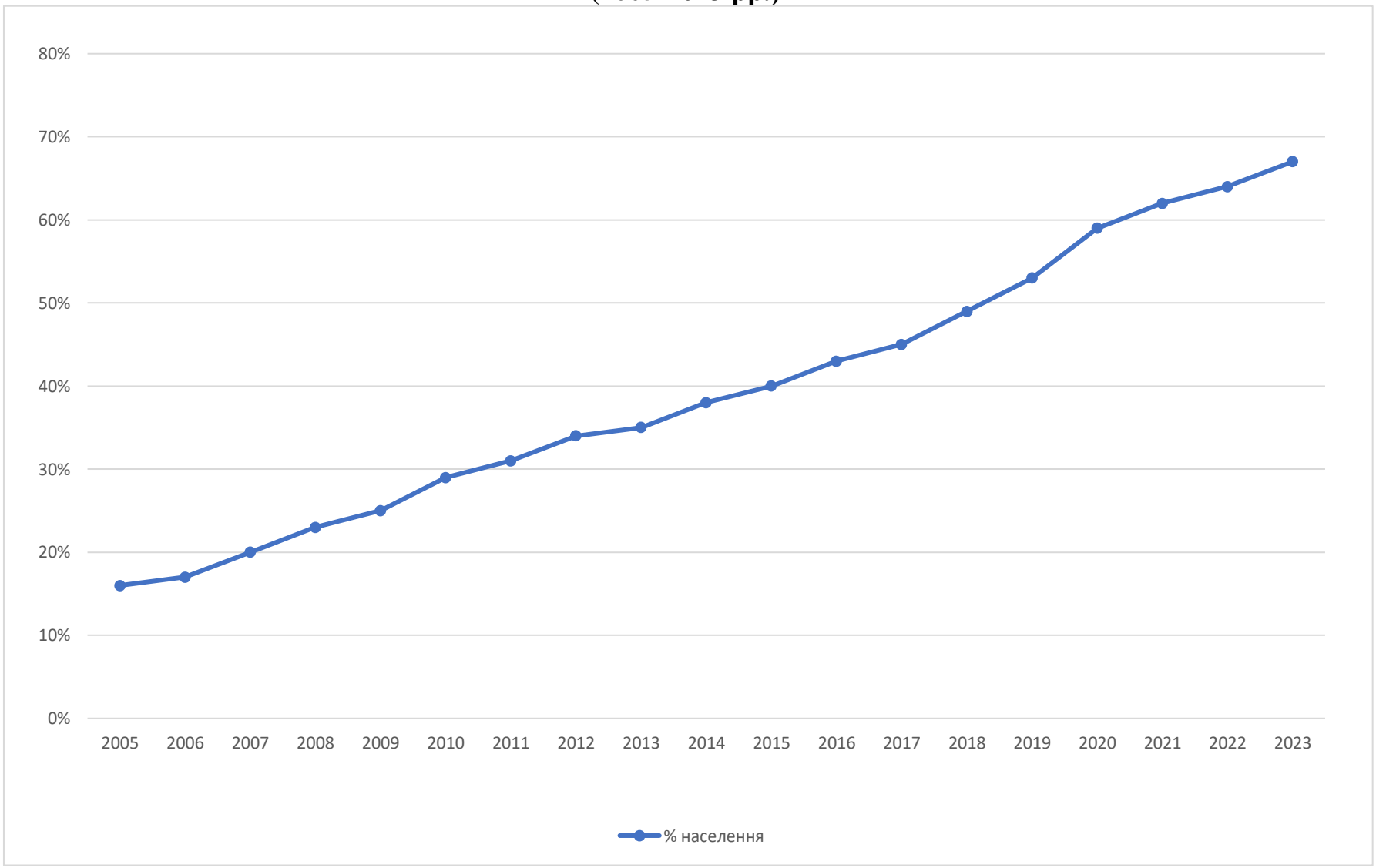
Найбільші глобальні ризики за ступенем складності та небезпеки для світу

У короткостроковій перспективі (2 роки)	
1.	**НЕПРАВДИВА ІНФОРМАЦІЯ ТА ДЕЗІНФОРМАЦІЯ**
2.	Погодні катаклізми
3.	Поляризація суспільства
4.	**НЕЗАХИЩЕНІСТЬ В КІБЕРПРОСТОРІ**
5.	Міждержавні збройні конфлікти
6.	Нестача економічних можливостей для населення
7.	Інфляція
8.	Вимушена міграція
9.	Економічний спад
10.	Забруднення навколишнього середовища

У довгостроковій перспективі (10 років)	
1.	Погодні катаклізми
2.	Критичні зміни в процесах функціонування Землі як планети
3.	Втрата біорізноманіття та колапс екосистем
4.	Дефіцит природніх ресурсів
5.	**НЕПРАВДИВА ІНФОРМАЦІЯ ТА ДЕЗІНФОРМАЦІЯ**
6.	Негативні наслідки розвитку технології штучного інтелекту
7.	Вимушена міграція
8.	**НЕЗАХИЩЕНІСТЬ В КІБЕРПРОСТОРІ**
9.	Поляризація суспільства
10.	Забруднення навколишнього середовища

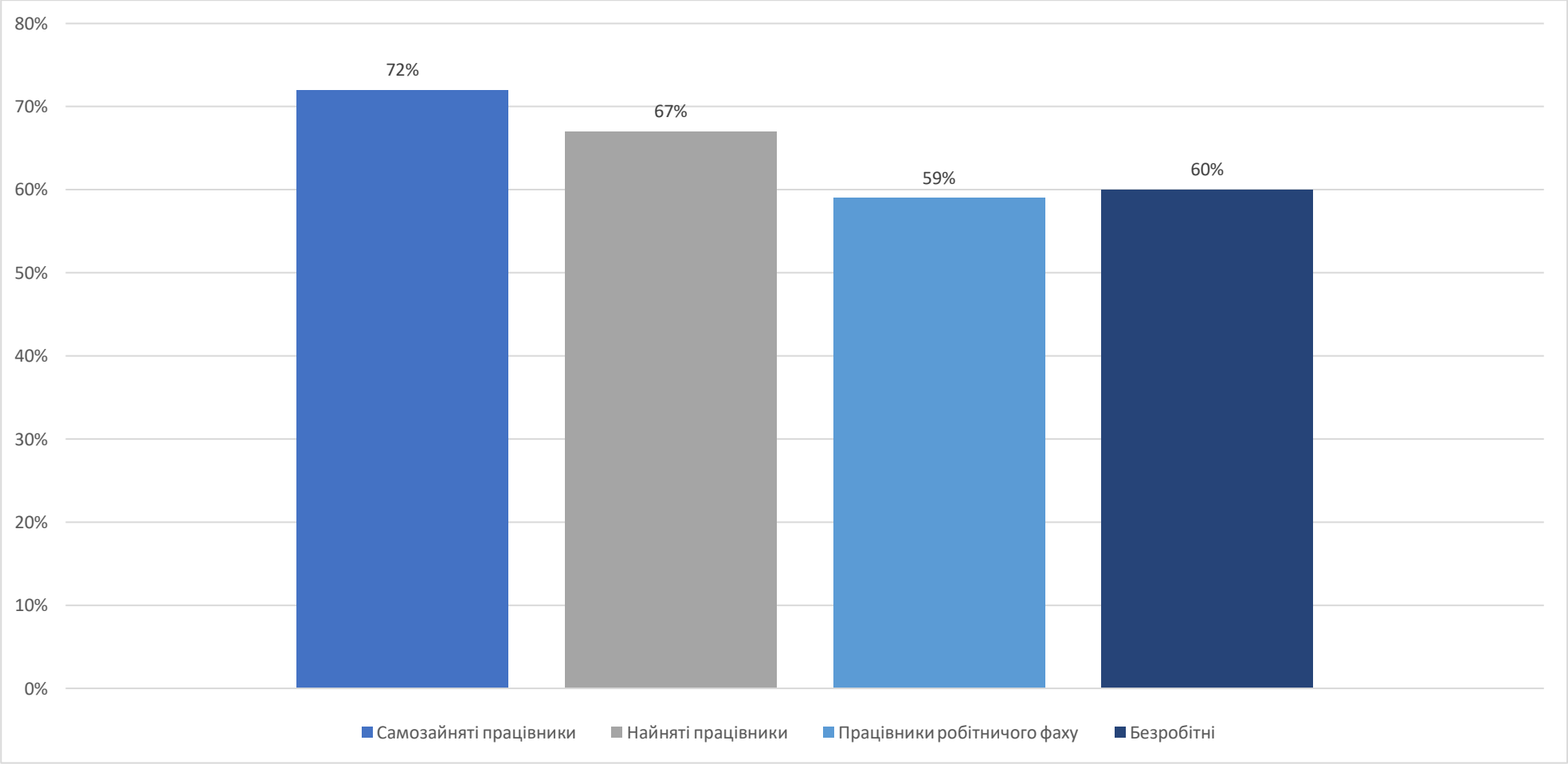
ДОДАТОК Б

Динаміка частки населення світу, яке користується Інтернетом (2005-2023 рр.)



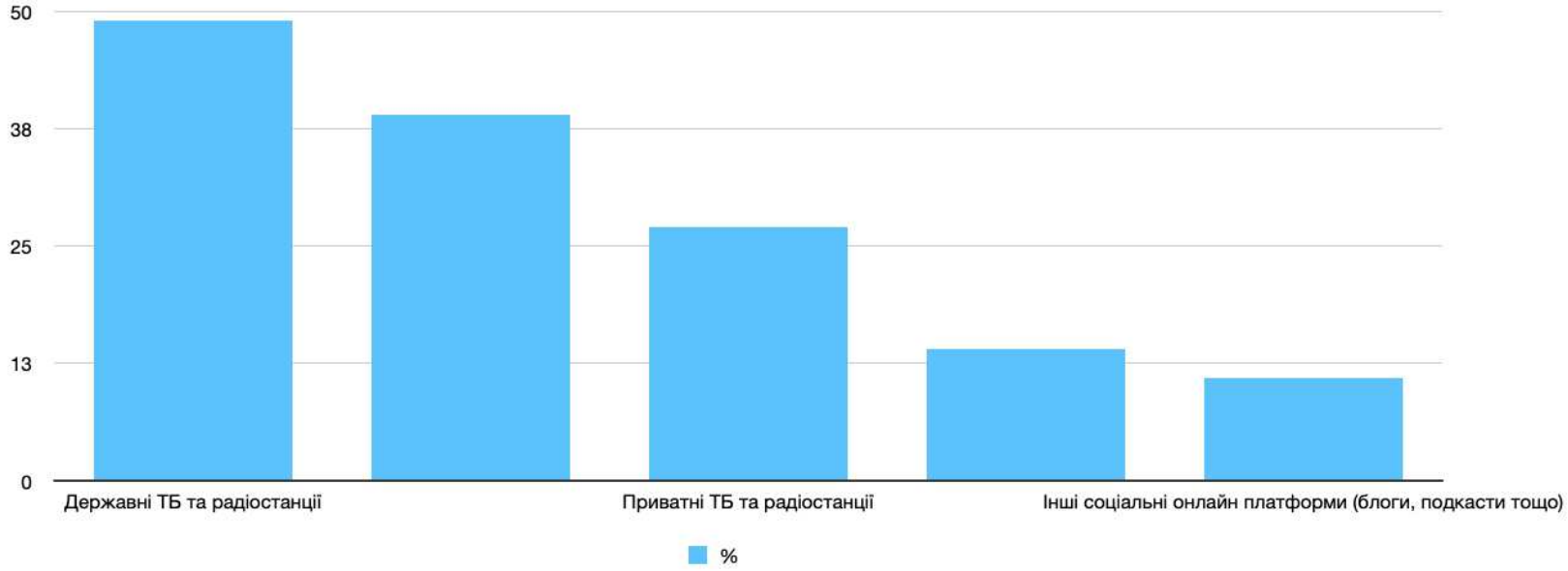
ДОДАТОК В

Дезінформація та населення ЄС (дослідження 2022 року). Оцінка впевненості різних груп населення



ДОДАТОК Г

Джерела інформації, які користуються найбільшою довірою серед європейців



Джерела інформації	%
Державні ТБ та радіостанції	49
Друкована преса (включно з її онлайн форматами)	39
Приватні ТБ та радіостанції	27
Люди, групи, друзі, які я відстежую в соцмережах	14
Інші соціальні онлайн платформи (блоги, подкасти тощо)	11

ДОДАТОК Ґ

Порівняльна таблиця кібератак Росії на критичну інфраструктуру Франції, України, Німеччини та Великої Британії

Країна	Франція	Україна	Німеччина	Велика Британія
Кіберінцидент	Атака на веб-ресурси Національної асамблеї та Сенату Франції	Атака на оператора мобільного зв'язку «Київстар»	Атака на критичну інфраструктуру *(урядові сайти, сайти банків та аеропортів)*	Серія кібератак на політиків, державні та приватні інституції
Дата	03-05.2023 р.	12.12.2023 р.	01.2023 р.	2015- (офіційно викрита мережа в 2023 році)
Сторона, відповідальна за кібератаку	**NoName057(16)** *(хакерська група, афілійована з російськими спецслужбами)*	**«Солнцепёк»** *(хакерський підрозділ Генштабу армії РФ)*	**Killnet** *(хакерська група, афілійована з російськими спецслужбами)*	**«Центр 18» ФСБ Росії** *(інша назва: Star Blizzard)*
Ціль	Перешкоджання роботи парламенту з підтримки України Загострення внутрішньої соціально-політичної ситуації у Франції	Позбавлення українців зв'язку Дестабілізація соціальної ситуації	Атака-відповідь на рішення ФРН передати Україні танки Leopard, ухвалене на початку 2023 року	Проникнення в політичну систему Британії та отримання контролю над громадським сектором
Специфіка кібератаки	Використання **DDoS-атаки** для перешкоджання роботи сайтів парламенту	Комплексна атака на критичну віртуальну інфраструктуру компанії Використання скомпрометованих даних співробітників компанії	Використання **DDoS-атаки** для перешкоджання роботи сайтів	Фішинг, злам сайтів, викрадення та злив конфіденційної інформації

Результат	Тимчасова *(декілька годин)* недоступність ресурсів парламенту для користувачів	Частково зруйнована віртуальна інфраструктура компанії Збитки понад 100 млн доларів Постраждали 24,1 млн абонентів оператора	Тимчасова *(декілька годин)* недоступність ресурсів для користувачів	Доступ до чутливої інформації, зокрема злив торгівельних документів США і Британії напередодні виборів 2019 р. Використання інформації для втручання у внутрішні політичні процеси
Ступінь успішності	**Низький**	**Високий**	**Низький**	**Високий**
Реакція держави	Схвалення парламентом в липні 2023 виділення протягом 2024-2030 рік 4 млрд євро на посилення кіберзахисту Франції Розширення повноважень Агентства ANSSI, зокрема щодо збору технічних даних трафіку та роботи серверів	Публікація рекомендацій для органів влади та компанії щодо посилення кібербезпеки Відсутні системні державні рішення для унеможливлення таких атак	Надання BSI рекомендацій урядовим і приватним установам щодо посилення кібербезпеки Відсутні системні державні рішення для унеможливлення таких атак	Публікація Британією, США, Канадою, Австралією та Новою Зеландію детальних рекомендацій щодо убезпечення від зловмисників

ДОДАТОК Д

Порівняльна таблиця дезінформаційних кампаній Росії проти Франції, України, Німеччини та Великої Британії

Країна	Франція	Україна	Німеччина	Велика Британія
Кампанія	Дезінформаційна кампанія напередодні президентських виборів 2017 року	Дезінформаційна кампанія «Майдан-3»	Дезінформаційна кампанія в Х зі зриву постачань зброї Україні	Дезінформаційна кампанія під час Brexit
Період	2017 рік	2023-2024 рр.	12.2023–01.2024 рр.	2015-2016 рр. (напередодні референдуму щодо виходу з ЄС)
Ціль	Підтримка проросійських кандидатів (Марін Ле Пен, Франсуа Фійон, Жан-Люк Меланшон)	Дестабілізація соціально-політичної ситуації в країні Послаблення обороноздатності України	Зрив підтримки Німеччиною України, зокрема військової	Вплив на суспільну думку, зокрема переконання британців в необхідності Brexit
Специфіка кампанії	Використання кібератак для отримання і зливу чутливої інформації (MacronLeaks) Використання фейкових аккаунтів, зокрема у Facebook, для компрометації кампанії Е. Макрона	Використання фейкових аккаунтів в соцмережах Використання наративів про «примусову мобілізацію», «корупцію» та «брехню щодо війни»	Використання понад 50 тис. фейкових аккаунтів в соцмережі Х Поширення ними фейків з критикою підтримки урядом ФРН України Використання популярних хештегів #Oktoberfest #Bundesliga для більшого охоплення публікацій	Використання інформаційних ресурсів Russia Today та Sputnik для поширення фейків на користь виходу Британії з ЄС Проплачені компанії у соцмережах Facebook, Twitter Використання мережі ботоферм для сіяння інформаційного хаосу
Результат	Тимчасова дестабілізація політичної ситуації в державі	Запуск процесів «бродіння» в українському сегменті соцмереж	Росії вдається робити питання підтримки України суперечливим в німецькому суспільстві	Більшістю голосів британці підтримали вихід держави з ЄС, який був офіційно завершений 31 січня 2020 року

	Водночас, кампанії не вдалось підірвати авторитет Е. Макрона серед його виборців	Виокремлення маргіналізованих груп, які сприяють дестабілізації ситуації в Україні	Водночас, це не зупиняє надання військової підтримки України	Росія уникнула відповідальності за своє інформаційне втручання
Ступінь успішності	**Низький** (переміг Е. Макрон, який був основною ціллю кампанії)	**Низький** (консолідація українського суспільства залишається достатньо потужною)	**Середній** (дискусія щодо підтримки України триває, проте наразі ключової цілі (відмови від підтримки) РФ досягти не вдалося)	**Високий** (досягнено поставленої цілі)
Реакція держави	Проведення ANSSI семінарів для політичних партій Франції з протидії дезінформації та кібератакам Блокування у кооперації з Facebook понад 70 тис. фейкових аккаунтів	Наразі відсутня системна робота держави з протидії кампанії в соцмережах Відповідь держави є реакційною і спрямована виключно на реагування на меседжі	Контакт з Х щодо цієї ситуації, внаслідок чого було заблоковано низку аккаунтів **Значна частина профілів досі активна**	**Відсутня** Перемога «брекзитерів» унеможливила запуск формальних розслідувань причетності РФ до втручання у виборчий процес

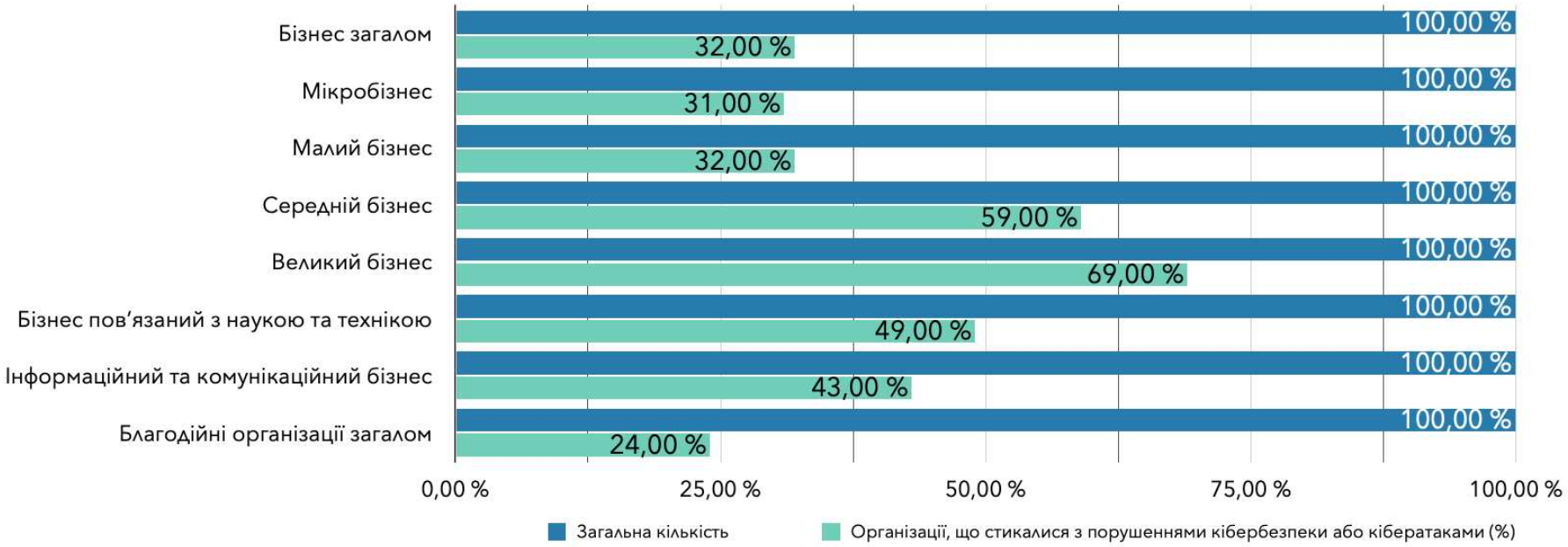
ДОДАТОК Е

Сприйняття дезінформації та фейків британським суспільством (2022 рік)

ДОДАТОК Є

Ситуація з кібербезпекою у Великій Британії (2023 рік)

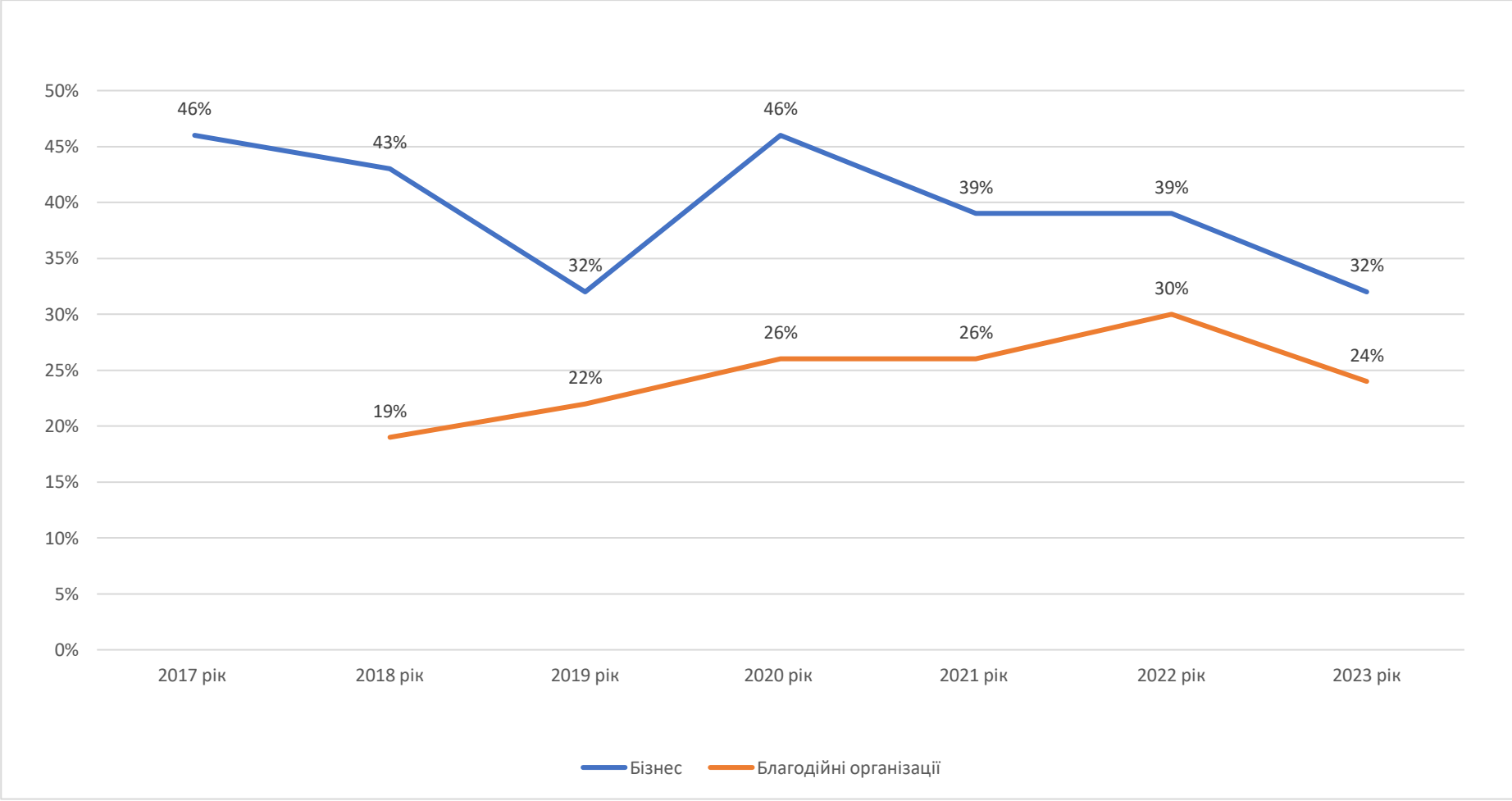
Відсоток організацій, які стикались з порушеннями кібербезпеки або кібератаками в останні 12 місяців



В опитуванні взяли участь 2263 британських підприємства та 1174 благодійних організацій

ДОДАТОК Ж

Відсоток організацій, які фіксували будь-які кіберпорушення чи кібератаки



ДОДАТОК З

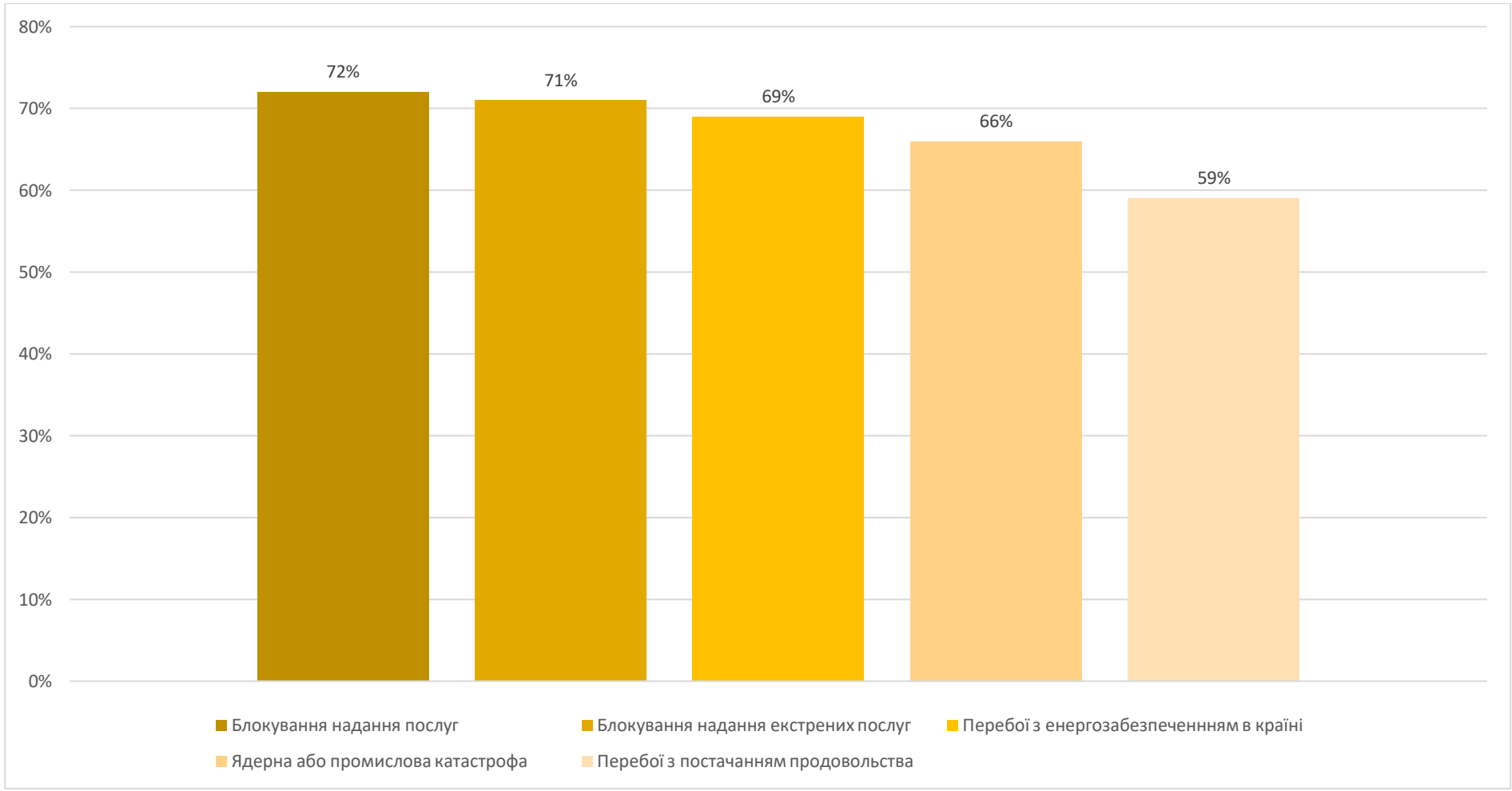
Ініціативи Великої Британії у сфері кібербезпеки

Назва ініціативи	Рік старту	Цільова група	Характеристика
Інструкція з 10-ти кроків *(10 steps guidance)*	2012	Бізнес	Консультативна підтримка бізнесу із захисту себе в кіберпросторі
CISP	2013	Бізнес	Створення безпечного кіберсередовища для обміну інформацією про загрози та покращення ситуаційної освідомленості
Cyber Essentials	2014	Бізнес	Надання бізнесу додаткових інструментів для покращення кібербезпеки та просування іміджу компанії
Cyber Aware	2014	Громадяни та бізнес	Надання порад громадянам та бізнесу як захистити себе онлайн та уникнути найпоширеніших загроз в кіберпросторі
Take-five-to-stopfraud	2016	Громадяни та бізнес	Кампанія консультативної підтримки громадян та бізнесу щодо того, як уникнути фінансових махінацій онлайн
Industry 100	2016	Державний та приватний сектори	Просування співпраці державного та приватного секторів щодо реагування на кібервиклики та їх запобігання
Small Business Guide	2017	Малий бізнес	Надання порад малому бізнесу щодо покращення свого кіберзахисту
CyBok	2017	Наукова спільнота	Майданчик для отримання освіти в сфері кібербезпеки, тренування та фахової практики
Small Charity Guide	2018	Благодійні організації	Надання інформації благодійним організаціям щодо того, як вони можуть себе захистити в кіберпросторі
Exercise in Box	2019	Бізнес	Онлайн інструмент, який допомагає організаціям оцінити свій рівень готовності до кібератак, а також надає безпечне середовища для тестування реакції на таку атаку

ДОДАТОК И

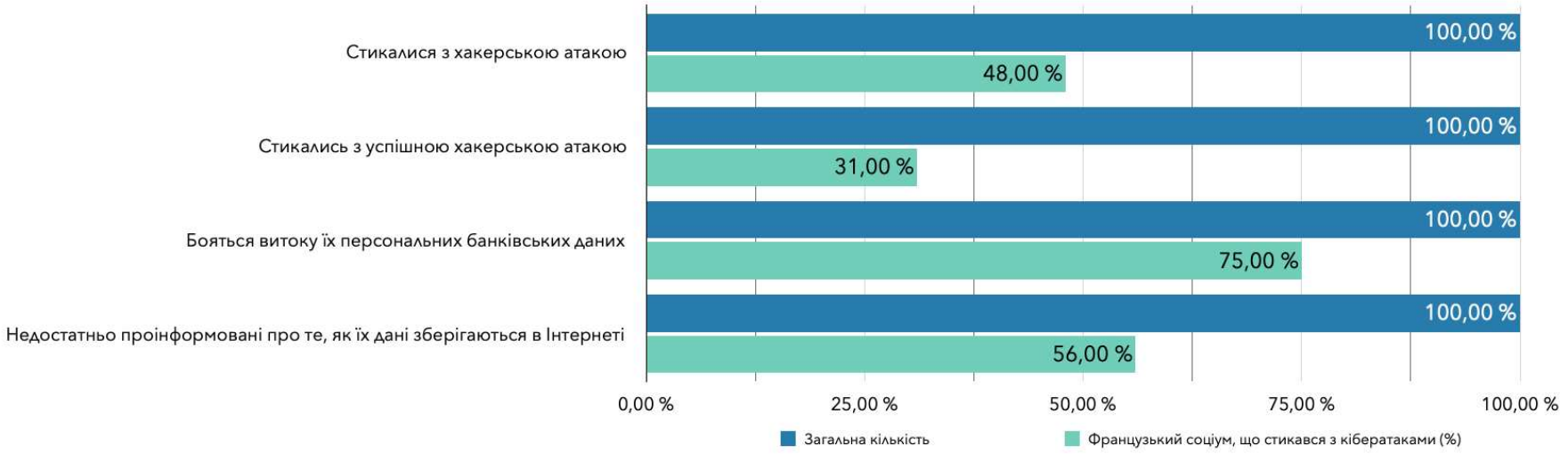
Громадська думка Франції щодо безпеки в кіберпросторі

Наслідки кібератак, яких найбільше бояться французи



ДОДАТОК І

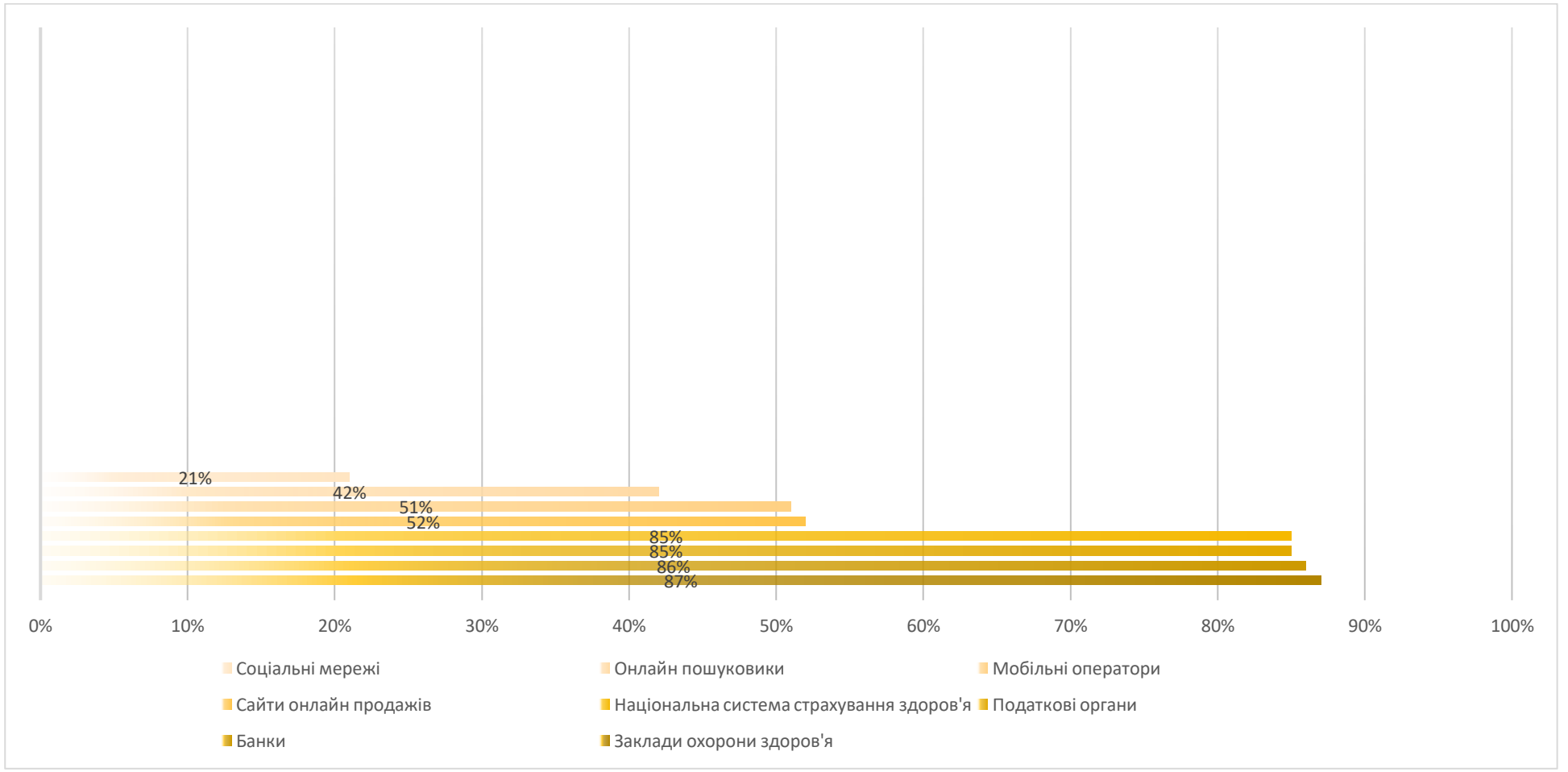
Кібератаки і французький соціум



Дослідження проведене компаніями Ipsos та Sopra Steria в березні 2022 року. В опитуванні взяли участь майже 1000 респондентів віком 18 років та більше

ДОДАТОК Ї

Рівень довіри французького суспільства до організацій-утримувачів персональних даних



Досліджене проведене компаніями Ipsos та Sopra Steria в березні 2022 року. В опитуванні взяли участь майже 1000 респондентів віком 18 років та більш

ДОДАТОК Й

Кількість щорічних подач заявок на отримання патенту на технології, пов'язані зі штучним інтелектом (2020 рік)

ДОДАТОК К

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації

Статті у наукових фахових виданнях України,
включених до міжнародних наукометричних баз даних:

1. Фурсай О. В. Система забезпечення інформаційної безпеки Франції / Олександра Володимирівна Фурсай. // Вісник Львівського університету. Серія Філосовсько-політологічні студії – 2021. – №34. – С. 222–227, DOI https://doi.org/10.30970/PPS.2021.34.29

2. Фурсай О. В. Політика інформаційної безпеки Європейського Союзу / Олександра Володимирівна Фурсай. // Літопис Волині. – 2023. – №29. – С. 165–170, DOI https://doi.org/10.32782/2305-9389/2023.29.27

3. Фурсай О. В. Російська дезінформаційна кампанія «Doppelgänger» як новітній виклик інформаційній безпеці держав заходу / Олександра Володимирівна Фурсай. // Філософія та політологія в контексті сучасної культури. –2024. – Том 16 № Спецвипуск. – С. 84-92, DOI https://doi.org/10.15421/352411

4. Фурсай О. В. «Штучний інтелект» як виклик міжнародній інформаційній безпеці / Олександра Володимирівна Фурсай. // Регіональні студії. – 2023. – № 35. – С. 167, DOI https://doi.org/10.32782/2663-6170/2023.35.28

Статті в наукових періодичних виданнях інших держав,
включених до міжнародних наукометричних баз даних:

5. Fursai O. “Vaccinodemic” as a component of the global hybrid conflict between democracy and autocracy: the case of Ukraine / S. Danylenko, O. Fursai. // Rocznik Instytutu Europy Środkowo-Wschodniej. – 2022. – Vol. 20, Iss. 2 – p. 19–45, DOI https://doi.org/10.36874/RIESW.2022.2.2

Опубліковані праці апробаційного характеру:

6. Фурсай О. В. Інфодемія в епоху Covid-19 / Олександра Володимирівна Фурсай. // ІМВ. Міжнародна науково-практична конференція студентів, аспірантів і молодих вчених «Актуальні проблеми міжнародних відносин». – 2021. – С. 120–123.

7. Фурсай О. В. Медіа-агент як базова ланка пропагандистської діяльності терористичних угрупувань / Олександра Володимирівна Фурсай. // ІМВ. Міжнародна науково-практична конференція студентів, аспірантів та молодих вчених «Шевченківська весна». – 2021. – С. 147–149.

8. Фурсай О. В. «Вакцинодемія» як елемент світового гібридного протистояння демократії та автократії / Олександра Володимирівна Фурсай. // ГО «Грузинсько-українськиӣ експертниӣ центр». Міжнародна науково-практична інтернет-конференція «Сучасні загрози глобальниӣ та регіональниӣ безпеці». – 2023. – С. 115–120.

9. Фурсай О. В. Інформаційна безпека як аспект національної безпеки / Олександра Володимирівна Фурсай. // ІМВ. Міжнародна науково-практична конференція студентів, аспірантів і молодих вчених «Актуальні проблеми міжнародних відносин». – 2023. – С. 143–146.

10. Фурсай О. В. Глобальне інформаційне суспільство: теоретико-методологічні засади концепції / Олександра Володимирівна Фурсай. // The 6th International scientific and practical conference “Current challenges of science and education” MDPC Publishing, Berlin, Germany. – 2024. – С. 339–345.

11. Фурсай О. В. «Doppelgänger»: нова зброя Росії на інформаційному фронті війни проти заходу / Олександра Володимирівна Фурсай. // The 3rd International scientific and practical conference “Science and society: modern trends in a changing world” MDPC Publishing, Vienna, Austria.. – 2024. – С. 252–258.

ДОДАТОК Л

ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

1. Фурсай О. В. Міжнародна науково-практична конференція студентів, аспірантів і молодих вчених «Актуальні проблеми міжнародних відносин» (28 жовтня 2021 р., м. Київ, тема виступу «Інфодемія в епоху Covid-19», тези опубліковані);

2. Фурсай О. В. Міжнародна науково-практична конференція студентів, аспірантів та молодих вчених «Шевченківська весна» (29 березня 2021 р., м. Київ, Україна, тема виступу «Медіа-агент як базова ланка пропагандистської діяльності терористичних угрупувань», тези опубліковані);

3. Фурсай О. В. Міжнародна науково-практична інтернет-конференція «Сучасні загрози глобальній та регіональній безпеці», (29 жовтня 2023 р., м. Одеса, Україна, тема виступу «Вакцинодемія» як елемент світового гібридного протистояння демократії та автократії», тези опубліковані);

4. Фурсай О. В. Міжнародна науково-практична конференція студентів, аспірантів і молодих вчених «Актуальні проблеми міжнародних відносин», (1 грудня 2023 р., м. Київ, Україна, тема виступу «Інформаційна безпека як аспект національної безпеки», тези опубліковані);

5. Фурсай О. В. The 6th International scientific and practical conference “Current challenges of science and education” (12-14 лютого 2024 р., м. Берлін, Німеччина, тема виступу «Глобальне інформаційне суспільство: теоретико-методологічні засади концепції», тези опубліковані);

6. Фурсай О. В. The 3rd International scientific and practical conference “Science and society: modern trends in a changing world”, (19-21 лютого 2024 р., м. Відень, Австрія, тема виступу «Doppelgänger»: нова зброя Росії на інформаційному фронті війни проти заходу», тези опубліковані).