МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ І.І. МЕЧНИКОВА

Кваліфікаційна наукова

праця на правах рукопису

Сокоринський Володимир Олегович

УДК : 321.64:004 (342.7) (043.5)

ДИСЕРТАЦІЯ

ФЕНОМЕН ЦИФРОВОГО ТОТАЛІТАРИЗМУ: КОНЦЕПТУАЛІЗАЦІЯ ЗАГРОЗ ДЕМОКРАТІЇ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

05 – соціальні та поведінкові науки, 052 – Політологія.
Подається на здобуття наукового ступеня доктора філософії

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

Науковий керівник :

доктор політичних наук, професор

Мілова Марія Іллівна

Одеса – 2025

АНОТАЦІЯ

Сокоринський В.О. Феномен цифрового тоталітаризму: концептуалізація загроз демократії в інформаційному суспільстві. **–** Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 052 «Політологія» – Одеський національний університет імені І. І. Мечникова, Одеса, 2025.

Дисертація присвячена дослідженню феномену цифрового тоталітаризму та концептуалізації його загроз в інформаційному суспільстві, що виникають на початку XXI століття у результаті стрімкого розвитку цифровізації як глобального процесу впровадження інформаційно-комунікаційних технологій в різних сферах життєдіяльності суспільства, які кардинально змінюють і політичний ландшафт, впливають на трансформацію влади в авторитарних та демократичних державах, про що свідчать різні прояви кризи демократії, поширення її неліберальних практик та нові виклики і загрози.

В дисертації доводиться, що цифровий тоталітаризм проявляється у використанні інформаційно-комунікаційних технологій з метою здійснення масового спостереження, контролю, маніпуляцій, цензури та інших форм втручання у приватне життя громадян, що створює загрози порушення основоположних прав і свобод людини. В умовах глобальної цифровізації, з одного боку, зростає ступінь цифрового демократичного розвитку, електроні форми участі громаданян, електронне врядування, а з іншого — виникають нові форми цифрової нерівності, соціального контролю, політичних маніпуляцій та домінування урядових структур над особистістю. Саме в такому складному контексті виникла нагальна потреба у глибокому та грунтовному аналізі сутності феномену цифрового тоталітаризму, його основних цифрових інструментів та суб'єктів впливу, функціонуванні сучасних систем та механізмів захисту прав людини, їх

адаптації до новітніх загроз цифрового середовища, а також виробленні ефективних механізмів та інструментів протидії цифровому тоталітаризму.

Актуальність вибору теми дослідження обумовлена активними процесами цифрової трансформації інформаційного суспільства, а також помітним зростанням наявних практик обмеження свободи слова, права на приватність особистого життя, права на доступ до інформації в цифровому середовищі. Особливу актуальність у контексті дослідження становило вивчення взаємодії держави, інформаційного суспільства та приватних технологічних корпорацій у питаннях забезпечення цифрової безпеки та правового захисту людини. У фокусі дослідження є пошук оптимального балансу між потребами національної безпеки та захистом основоположних прав людини в умовах сучасної цифрової епохи, коли держави дедалі активніше вдаються до використовування технологій цифрового моніторингу, регулювання дії у мережі Інтернет та усебічному контролю за власним суспільством.

В межах дисертаційного дослідження автором уперше було проведено комплесне міждисциплінарне дослідження феномену цифрового тоталітаризму на стику політичної філософії, концепцій інформаційного суспільства, прав людини та інновацій у сфері технологій. Проаналізовано та представлено типологію загроз цифрового тоталітаризму, що виникають внаслідок монополізації цифрових платформ та централізації даних з боку технологічних корпорацій. Також актуалізовано класифікацію форм цифрового контролю, яка охоплює як державні, так і корпоративні інструменти впливу на інформаційне середовище та соціальну поведінку. Доведено, що цифровий тоталітаризм виникає не виключно в умовах авторитаризму, а також у демократичних державах як наслідок передачі регуляторних функцій великим технологічним корпораціям. Був удосконалений концептуальний підхід до оцінки ефективності правозахисних інституцій в умовах цифрової трансформації шляхом порівняльного аналізу моделей регулювання у різних політичних системах.

Сформульовано теоретико-методологічну основу для дослідження цифрового тоталітаризму як комплексного явища, що виникає в результаті інтеграції цифрових інструментів, систем інформаційного контролю та політичної влади.

В дисертаційному дослідженні з'ясовано, що класичні підходи до вивчення феномену цифрового тоталіатризму та загроз демократії в інформаційних суспільствах потребують суттєвої, ретельної модернізації, а також адаптації. Було встановлено, що державні політичні рішення, значно відстають від темпів неконтрольованих цифрових трансформацій, внаслідок чого виникає дефіцит відповідних правових гарантій у сфері захисту приватності, прав збереження та непередачі персональних даних, свободи вираження поглядів у цифровому середовищі. Особливо проблемним аспектом є недостатньо чітке та адекватне регулювання діяльності великих технологічних IT-корпорацій, від яких безпосередньо залежить доступ громадян до цифрових платформ, інформаційних ресурсів та можливостей соціальної комунікації у мережі Інтернет та цифровому просторі.

Значну увагу приділено аналізу механізмів захисту прав людини в контексті розвитку цифрових технологій. Зокрема, детально проаналізована динаміка підходів до захисту прав людини в умовах цифрових трансформацій, роль та рішення Європейського суду з прав людини, Європейської комісії, Ради ООН з прав людини у формуванні нових правових стандартів захисту цифрових прав людини. Окрема увага була зосереджена також на порівняльному аналіз практик цифрового регулювання в демократичних та авторитарних державах у сфері кібербезпеки, цифрового суверенітету, а також інституційна спроможність міжнародних та національних систем забезпечення прав людини в умовах інформаційного суспільства.

В дисертації висвітлено проблеми впливу інструментів та загроз цифрового тоталітаризму на діяльність та функціонування демократичних інституцій. Особливу увагу приділено технології масового спостереження,

як інструменту політичного управління. Визначені особливості алгоритмічної цензури, маніпуляції інформацією та процесів контролю політичного дискурсу, які характерезується маніпулятивними практиками контролю громадської думки, й контрольованості політичних та соціальних дій людини з боку держав. Розкрито методи та сучасні практики цифрового стеження, маніпулювання інформаційним простором за допомогою бот-мереж, впровадження та використання алгоритмічного контролю ШІ (штучного інтелекту), а також втілення елементів соціального рейтингування, яке застосовується у деяких державах Азійського регіону.

Проаналізувавши різні підходи та концептуальні доробки дослідників, було визначено та систематизовано ключові загрози цифрового тоталітаризму, серед яких *нормалізація цифрового нагляду* - поширення практик масового спостереження, що стають звичними та прийнятними у суспільстві, призводить до зниження чутливості громадян до порушень їхніх прав на приватність. *Стирання меж між приватним і публічним* - зростаюча інтеграція цифрових технологій у повсякденне життя ускладнює розмежування особистого простору та публічної сфери, що може призвести до зловживань з боку держави та корпорацій. *Комодифікація даних та приватності* - перетворення особистих даних на товар, що продається та купується, підриває фундаментальні права людини та сприяє експлуатації індивідуальної інформації без належного контролю. *Технократична централізація управління* - зосередження влади в руках вузького кола технічних спеціалістів, які володіють унікальними навичками у сфері цифрових технологій, призводить до того, що процес прийняття ключових політичних та соціальних рішень дедалі більше залежить від алгоритмів, штучного інтелекту та технічних стандартів. Це, в свою чергу, може суттєво знижувати роль демократичних інституцій і громадянського суспільства, перетворюючи політику на сферу технічного управління, де пріоритет віддається ефективності й раціональності на шкоду участі громадян та прозорості ухвалення рішень. Така модель управління також

несе загрозу встановлення авторитарних режимів, у яких технічні рішення використовуються як інструмент соціального контролю та маніпулювання поведінкою населення. Одночасно, технократична централізація становить ризик для демократичного устрою суспільства і потребує вироблення нових механізмів демократичного контролю, підзвітності технократичних структур та прозорості алгоритмічних рішень. Подальші перспективи дослідження сучасних систем захисту прав людини в умовах цифрового тоталітаризму полягають у кількох важливих напрямах. Насамперед, актуальним залишається більш грунтовний аналіз та оцінювання ефективності міжнародних та національних правових механізмів, спрямованих на протидію цифровим загрозам. Особливої уваги заслуговує дослідження процесу імплементації міжнародних стандартів у національні правові системи, а також виявлення перешкод, які виникають на цьому шляху. Це дозволить краще зрозуміти які саме елементи правових моделей забезпечують оптимальний рівень захисту цифрових прав людини та яким чином їх можна застосовувати на законодавчих, виконавичах рівнях влади та соціально-культурних і економічних аспектах державного урядування.

Досліджено взаємодії державних органів, громадянського суспільства та приватних технологічних корпорацій у питанні забезпечення цифрових прав. Зокрема, важливим завданням подальших досліджень є пошук ефективних механізмів регулювання діяльності великих цифрових платформ, від яких значною мірою залежить інформаційна та комунікативна інфраструктура сучасного суспільства. Враховуючи посилення впливу таких корпорацій, необхідно розробити нові концепції їх політичної відповідальності за порушення прав людини у цифровому просторі.

Визначена проблематика розробки подальших нових підходів до забезпечення приватності та захисту персональних даних в умовах поширення технологій штучного інтелекту, алгоритмічного контролю та автоматизованого прийняття рішень. Перспективним у цьому контексті є

дослідження етичних та правових аспектів застосування штучного інтелекту, зокрема з огляду на загрози дискримінації, соціальної стигматизації та втручання у приватне життя громадян.

Представлене дослідження актуалізує проблему впливу нової тоталітарності на розвиток демократичних держав в інформаційну добу. Важливо детальніше дослідити механізми формування цифрових інформаційних бульбашок, політичної поляризації та радикалізації суспільних настроїв, що часто супроводжують використання сучасних інформаційних технологій. Вивчення цих аспектів дозволить запропонувати конкретні стратегії запобігання негативним явищам, які ставлять під загрозу функціонування демократичних інститутів та громадянських свобод.

Досліджено регіональні та національни практики у сфері цифрової безпеки та цифрового суверенітету. Особливу увагу приділино країнам, які перебувають на різних рівнях цифрового розвитку, з метою визначення кращих практик та вироблення універсальних рекомендацій щодо захисту цифрових прав, які можна було б ефективно застосовувати у різних юрисдикціях. Поглиблене вивчення цього напрямку дослідження сприяє формуванню комплексної правової та політичної відповіді на виклики цифрового тоталітаризму і забезпечить надійнішу реалізацію фундаментальних прав і свобод людини в сучасних умовах цифровізації суспільства.

Отже, проведене дослідження підтверджує критичну важливість протидії проявам цифрового тоталітаризму для забезпечення фундаментальних прав людини в епоху інформаційного суспільства. У результаті комплексного аналізу законодавства України у сфері цифрових прав та його порівняння з моделями США, ЄС і КНР з’ясовано ключові тенденції й виявлено як кращі практики, так і недоліки існуючих правових механізмів. Значення отриманих результатів полягає у формуванні цілісного уявлення про ефективність нормативно-правових підходів до

захисту цифрових прав та розробці рекомендацій для вдосконалення національного законодавства з урахуванням міжнародного досвіду.

Наукова новизна роботи визначається тим, що вперше у вітчизняній політичні науці комплексно досліджено феномен «цифрового тоталітаризму» та його загрози демократії в інформаційних суспільствах, запропоновано авторське визначення цього явища й класифіковані політичні та соціально-культурні заходи протидії. Крім того, проведений порівняльно аналіз дозволив ідентифікувати унікальні риси та спільні тенденції регулювання загроз на національному та міжнародному рівнях. Отримані результати становлять значну теоретичну основу та мають практичну цінність для проведення подальших досліджень у сфері цифрових прав і вдосконалення національної правової політики у цій сфері. Перспективи подальших досліджень вбачаються у поглибленні аналізу динаміки розвитку цифрового законодавства, оцінці ефективності впровадження запропонованих заходів протидії цифровому тоталітаризму та розширенні порівняльного правового аналізу шляхом залучення досвіду інших держав і регіонів. Таким чином, результати роботи є вагомим внеском у розвиток теорії та практики феномену цифрового тоталітаризму та захисту прав людини в цифровому суспільстві й формують підґрунтя для майбутніх наукових пошуків як у цій галузі, так і в політичній науці в цілому.

***Ключові слова**: цифровий тоталітаризм, інформаційне суспільство, тоталітаризм*, *демократія, загрози демократії, цифровізація, штучний інтелект, системи спостереження, цифрові права, захист прав людини, цифрові технології, інформаційна безпека, , маніпулятивний вплив*, *дезінформація, Китай.*

ABSTRACT

Sokorynskyi V.O. The Phenomenon of Digital Totalitarianism: Conceptualizing Threats to Democracy in the Information Society. – Qualification scientific work in the form of a manuscript. Dissertation for the

Doctor of Philosophy degree in the specialty 052 Political Science". – Odesa National University I. I. Mechnikov, Odesa, 2025.

The dissertation is devoted to the study of the phenomenon of digital totalitarianism and the conceptualization of its threats in the information society, which arise at the beginning of the 21st century as a result of the rapid development of digitalization as a global process of implementing information and communication technologies in various spheres of society, which radically change the political landscape and influence the transformation of power in authoritarian and democratic states, as evidenced by various manifestations of the crisis of democracy, the spread of its illiberal practices, and new challenges and threats.

The dissertation argues that digital totalitarianism manifests itself in the use of information and communication technologies for the purpose of mass surveillance, control, manipulation, censorship and other forms of interference in the private lives of citizens, which creates threats of violation of fundamental human rights and freedoms. In the context of global digitalization, on the one hand, the degree of digital democratic development, electronic forms of citizen participation, electronic governance are increasing, and on the other hand, new forms of digital inequality, social control, political manipulation and dominance of government structures over the individual are emerging. It is in such a complex context that there is an urgent need for a deep and thorough analysis of the essence of the phenomenon of digital totalitarianism, its main digital tools and subjects of influence, the functioning of modern systems and mechanisms for protecting human rights, their adaptation to the latest threats of the digital environment, as well as the development of effective mechanisms and tools to counter digital totalitarianism.

The relevance of the choice of the research topic is due to the active processes of digital transformation of the information society, as well as the noticeable growth of existing practices of restricting freedom of speech, the right to privacy of personal life, the right to access information in the digital

environment. Of particular relevance in the context of the study was the study of the interaction of the state, the information society and private technological corporations in matters of ensuring digital security and legal protection of the person. The focus of the study is the search for the optimal balance between the needs of national security and the protection of fundamental human rights in the conditions of the modern digital era, when states are increasingly resorting to the use of digital monitoring technologies, regulation of actions on the Internet and comprehensive control over their own society.

Within the framework of the dissertation research, the author conducted for the first time a comprehensive interdisciplinary study of the phenomenon of digital totalitarianism at the junction of political philosophy, concepts of the information society, human rights and innovations in the field of technology. The typology of threats to digital totalitarianism arising from the monopolization of digital platforms and data centralization by technological corporations was analyzed and presented. The classification of forms of digital control, which includes both state and corporate instruments of influence on the information environment and social behavior, was also updated. It was proved that digital totalitarianism arises not only in conditions of authoritarianism, but also in democratic states as a result of the transfer of regulatory functions to large technological corporations. The conceptual approach to assessing the effectiveness of human rights institutions in conditions of digital transformation was improved through a comparative analysis of regulatory models in different political systems. A theoretical and methodological basis for the study of digital totalitarianism as a complex phenomenon arising from the integration of digital tools, information control systems, and political power has been formulated.

The dissertation research revealed that classical approaches to studying the phenomenon of digital totalitarianism and threats to democracy in information societies require significant, thorough modernization, as well as adaptation. It was found that state political decisions significantly lag behind the pace of uncontrolled digital transformations, resulting in a shortage of appropriate legal

guarantees in the field of privacy protection, the rights to preserve and not transfer personal data, and freedom of expression in the digital environment. A particularly problematic aspect is the insufficiently clear and adequate regulation of the activities of large technological IT corporations, on which citizens' access to digital platforms, information resources, and opportunities for social communication on the Internet and digital space directly depend.

Considerable attention was paid to the analysis of mechanisms for protecting human rights in the context of the development of digital technologies. In particular, the dynamics of approaches to protecting human rights in the context of digital transformations, the role and decisions of the European Court of Human Rights, the European Commission, and the UN Human Rights Council in the formation of new legal standards for the protection of digital human rights were analyzed in detail. Special attention was also focused on a comparative analysis of digital regulation practices in democratic and authoritarian states in the field of cybersecurity, digital sovereignty, as well as the institutional capacity of international and national systems for ensuring human rights in the context of the information society.

The dissertation highlights the problems of the influence of tools and threats of digital totalitarianism on the activities and functioning of democratic institutions. Special attention is paid to the technology of mass surveillance as a tool of political governance. The features of algorithmic censorship, information manipulation and processes of control of political discourse, which are characterized by manipulative practices of controlling public opinion, and the controllability of political and social actions of a person by states, are determined. The methods and modern practices of digital surveillance, manipulation of information space using botnets, the introduction and use of algorithmic control of AI (artificial intelligence), as well as the implementation of elements of social rating, which is used in some countries of the Asian region, are revealed.

Having analyzed various approaches and conceptual developments of researchers, the key threats of digital totalitarianism were identified and

systematized, including the normalization of digital surveillance - the spread of mass surveillance practices that become commonplace and acceptable in society, leading to a decrease in citizens' sensitivity to violations of their rights to privacy. Blurring the boundaries between private and public - the growing integration of digital technologies into everyday life makes it difficult to distinguish between personal space and the public sphere, which can lead to abuse by the state and corporations. Commodification of data and privacy - the transformation of personal data into a commodity that is sold and bought, undermines fundamental human rights and promotes the exploitation of individual information without proper control. Technocratic centralization of governance - the concentration of power in the hands of a narrow circle of technical specialists with unique skills in the field of digital technologies, leads to the fact that the process of making key political and social decisions increasingly depends on algorithms, artificial intelligence and technical standards. This, in turn, can significantly reduce the role of democratic institutions and civil society, turning politics into a sphere of technical governance, where priority is given to efficiency and rationality to the detriment of citizen participation and transparency of decision-making. Such a governance model also carries the threat of establishing authoritarian regimes in which technical solutions are used as a tool of social control and manipulation of the behavior of the population. At the same time, technocratic centralization poses a risk to the democratic structure of society and requires the development of new mechanisms of democratic control, accountability of technocratic structures and transparency of algorithmic decisions. Further prospects for research into modern systems for the protection of human rights in conditions of digital totalitarianism lie in several important directions. First of all, a more thorough analysis and assessment of the effectiveness of international and national legal mechanisms aimed at countering digital threats remains relevant. Of particular interest is the study of the process of implementing international standards into national legal systems, as well as the identification of obstacles that arise along the way. This will allow us to better understand which elements of legal models provide the

optimal level of protection of digital human rights and how they can be applied at the legislative, executive levels of government, and socio-cultural and economic aspects of public governance.

The interaction of state bodies, civil society and private technology corporations in the issue of ensuring digital rights is studied. In particular, an important task of further research is the search for effective mechanisms for regulating the activities of large digital platforms, on which the information and communication infrastructure of modern society largely depends. Given the increasing influence of such corporations, it is necessary to develop new concepts of their political responsibility for human rights violations in the digital space.

The issue of developing further new approaches to ensuring privacy and protecting personal data in the context of the spread of artificial intelligence technologies, algorithmic control and automated decision-making is identified. In this context, the study of the ethical and legal aspects of the use of artificial intelligence is promising, in particular in view of the threats of discrimination, social stigmatization and interference in the private lives of citizens.

The presented study actualizes the problem of the influence of new totalitarianism on the development of democratic states in the information age. It is important to study in more detail the mechanisms of the formation of digital information bubbles, political polarization and radicalization of public sentiment that often accompany the use of modern information technologies. Studying these aspects will allow us to propose specific strategies for preventing negative phenomena that threaten the functioning of democratic institutions and civil liberties. Regional and national practices in the field of digital security and digital sovereignty were studied. Particular attention was paid to countries at different levels of digital development, in order to identify best practices and develop universal recommendations for the protection of digital rights, which could be effectively applied in different jurisdictions. In-depth study of this area of research contributes to the formation of a comprehensive legal and political response to the challenges of digital totalitarianism and will ensure a more reliable

implementation of fundamental human rights and freedoms in modern conditions of digitalization of society.

Thus, the conducted study confirms the critical importance of countering the manifestations of digital totalitarianism for ensuring fundamental human rights in the era of the information society. As a result of a comprehensive analysis of the legislation of Ukraine in the field of digital rights and its comparison with the models of the USA, the EU and the PRC, key trends were identified and both best practices and shortcomings of existing legal mechanisms were identified. The significance of the results obtained lies in forming a holistic view of the effectiveness of regulatory approaches to the protection of digital rights and developing recommendations for improving national legislation, taking into account international experience.

The scientific novelty of the work is determined by the fact that for the first time in domestic political science, the phenomenon of "digital totalitarianism" and its threats to democracy in information societies have been comprehensively investigated, the author's definition of this phenomenon has been proposed, and political and socio-cultural countermeasures have been classified. In addition, the comparative analysis has allowed us to identify unique features and common trends in the regulation of threats at the national and international levels. The results obtained constitute a significant theoretical basis and have practical value for conducting further research in the field of digital rights and improving national legal policy in this area. Prospects for further research are seen in deepening the analysis of the dynamics of the development of digital legislation, assessing the effectiveness of the implementation of the proposed measures to counter digital totalitarianism, and expanding comparative legal analysis by drawing on the experience of other states and regions. Thus, the results of the work are a significant contribution to the development of the theory and practice of the phenomenon of digital totalitarianism and the protection of human rights in the digital society and form the basis for future scientific research both in this field and in political science as a whole.

Keywords: *digital totalitarianism, information society, totalitarianism, democracy, threats to democracy, digitalization, artificial intelligence, surveillance systems, digital rights, protection of human rights, digital technologies, information security, manipulative influence, disinformation, China..*

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті в наукових фахових виданнях України

1. Сокоринський В. О Сучасні інструменти захисту прав, свободи та безпеки особистості в епоху «Цифрового тоталітаризму». *Регіональні студії*. 2022. Вип. 28. С.35-39. URL: http://www.regionalstudies.uzhnu.uz.ua/archive/28/6.pdf

2. Сокоринський В. О. Сучасні системи захисту прав людини в КНР в контексті загрози «цифрового тоталітаризму» *Регіональні студії*. Вип. 33. С.39-44. URL: http://regionalstudies.uzhnu.uz.ua/archive/33/7.pdf

3. Сокоринський В. О «Цифровий Паноптикум» як метод розповсюдження цифрового тоталітаризму та загроза сучасним міжнародним відносинам. *Politicus*. 2024. № 2. С.118-122. URL: http://politicus.od.ua/2_2024/2_2024.pdf

Тези доповідей на наукових конференціях

1. Сокоринський В.О. Цифровий тоталітаризм як виклик інтеграційним процесам у світі. У *Соціально-економічний та політичний розвиток країн в умовах глобальної нестабільності* [Електронний ресурс] : матеріали Міжнародної науково-практичної конференції (м. Одеса, 27 травня 2022 р.). Одеса: Одес. нац. ун-т ім. І. І. Мечникова, 2022. 5с.

2. Сокоринський В.О. Цифровий тоталітаризм як загроза сучасній цифровій дипломаті. У *Сучасні загрози глобальній та регіональній безпеці* : матер.Міжнар. наук.-практ. інтерн.-конф. (м. Одеса, 29 жовтня 2023 р.) уклад. А. Полухіна; ГО «ГУЕЦ». Одеса: Фенікс, 2023. 389 с.

3. Сокоринський В.О. Цифровий Паноптикум як метод розповсюдження Цифрового тоталітаризму. Сучасні системи спостереження та контролю за суспільствами. У *Трансформація українського суспільства в цифрову еру* : матеріали III Всеукраїнської науково-практичної конференції, 22 березня 2024 р. Львів – Торунь : Liha-Pres, 2024. 108 с.

URL:https://dspace.onua.edu.ua/server/api/core/bitstreams/e21276ef-218d-4e4d-905f-7c7d428df5ad/content

4. Сокоринський В.О. Сучасний стан загроз цифрового тоталітаризму у світі. VI Міжнародна науково-практична конференція У *Політичні процеси сучасності : глобальний та регіональний виміри*. 8-9 травня 2025 р. м.Івано-Франківськ. URL: https://kpn.pnu.edu.ua/2025/05/06/prohrama-konferentsii/

5. Сокоринський В.О., Мілова М.І. Цифровий тоталітаризм: трансформація влади в епоху тотального нагляду. У *Сталий розвиток регіонів, міст та спільнот в умовах глобальних перетворень: виклики, можливості, сценарії майбутнього.* Міжнародна наукова конференція. 16 травня 2025 р. м. Одеса. URL: https://onu.edu.ua/uk/fakultety/fakultet-mizhnarodnykh-vidnosyn-politolohii-ta-sotsiolohii/mizhnarodna-konferentsiia-do-iuvileiu-onu-ta-fmvps-stalyi-rozvytok-v-umovakh-hlobalnykh-zmin

ЗМІСТ

ВСТУП

Актуальність дослідження. У XXI столітті людство вступило в нову фазу цивілізаційного розвитку – фазу інформаційного суспільства, що визначається тотальним проникненням цифрових технологій у всі сфери життя. Інтернет, алгоритмічне управління, великі дані, соціальні мережі, штучний інтелект і системи масового спостереження не лише створили безпрецедентні можливості для комунікації, знань і розвитку, але й породили нові форми соціального контролю, маніпуляції свідомістю та обмеження свободи. У цьому контексті актуалізується поняття цифрового тоталітаризму – феномену, що характеризується використанням інформаційно-комунікаційних технологій для тотального нагляду, централізованого управління поведінкою громадян і знищення приватності.

Цифровий тоталітаризм не обмежується класичними уявленнями про авторитарні чи диктаторські режими. Його риси сьогодні простежуються як у відкрито недемократичних державах, так і в демократичних суспільствах, де заради «національної безпеки», «боротьби з дезінформацією» чи «цифрової ефективності» ухвалюються закони, які обмежують свободи громадян і посилюють владу технократичних еліт та технологічних корпорацій. Постає необхідність критично осмислити, яким чином цифрові технології впливають на природу влади, права людини та демократичні інститути.

Роль цифровізації у трансформації політичних, правових та соціокультурних процесів особливо загострилася в умовах глобальних викликів останніх років – таких як пандемія COVID-19, інформаційні війни, гібридні конфлікти, зростання політичної поляризації та ескалація цифрової залежності. Запровадження карантинних обмежень, перехід до дистанційної форми роботи та навчання, а також активне використання систем контролю мобільності населення продемонстрували, наскільки швидко технологічні рішення можуть інтегруватися в інфраструктуру управління суспільством.

За даними звіту Freedom House за 2021 рік, саме в цей період було зафіксовано зростання використання цифрових технологій для посилення державного спостереження, обмеження прав громадян та політичних свобод – навіть у країнах із усталеними демократичними традиціями.

Експансія інформаційно-комунікаційних технологій не лише трансформує економічні та освітні процеси, а й докорінно змінює природу політичної влади, легітимність інституцій, характер громадянської участі та межі приватності. У цьому контексті постає проблема аналізу *цифрового тоталітаризму* як особого типу владного режиму, що ґрунтується на алгоритмічному управлінні, моніторингу поведінки, обмеженні альтернативного мислення та делегуванні політичних функцій приватним технологічним структурам.

Незважаючи на те, що дослідження цифрової трансформації суспільства активно ведеться в межах соціології, політичної науки, права, економіки та культурології, низка критично важливих аспектів досі залишаються недостатньо вивченими. Зокрема, відсутня загально прийнята концептуалізація цифрового тоталітаризму як міждисциплінарного феномену; недостатньо розроблені теоретико-методологічні підходи до аналізу впливу цифрових технологій на демократичні практики; бракує системного аналізу трансформації механізмів захисту прав людини в умовах цифрової гібридності політичного контролю. Також не набули належного обґрунтування транснаціональні загрози, пов’язані з концентрацією владних повноважень в руках технологічних корпорацій, здатних фактично формувати інформаційний порядок денний у масштабах планети.

Зв'язок із науковими програмами, планами, темами. Дисертація виконана в межах науково-дослідної теми кафедри політології Одеського національного університету імені І.І. Мечникова «Динаміка локальних політичних процесів в умовах глобальної світ-системної трансформації» (державна реєстрація № 0123U102703 від 28.05.23), одним з виконавців якої є дисерант.

Мета і завдання дослідження.

Мета дослідження полягає у виявленні сутності феномену цифрового тоталітаризму як загрози демократичного розвитку в умовах інформаційного суспільства, аналіз його основних механізмів впливу на права, свободи людини та обґрунтування напрямів удосконалення системи їхнього захисту в інформаційному суспільстві.

Досягнення означеної мети зумовило необхідність вирішення наступних **завдань:**

1. Проаналізувати еволюцію концепції тоталітаризму та її трансформацію в контексті цифрового розвитку;

2. Охарактеризувати ключові ознаки інформаційного суспільства як передумови формування нових форм політичного контролю;

3. Розглянути методологічні підходи до вивчення цифровізації влади, контролю та управління;

4. Виявити основні технологічні інструменти, що використовуються для цифрового моніторингу, цензури та інформаційного впливу;

5. Простежити приклади алгоритмічної цензури, процеси маніпуляції інформацією та контролю політичного дискурсу;

6. Визначити роль технологічних корпорацій як суб’єктів політичного впливу, досліджуючи їхнє відношення до трансформації режимів інформаційного управління в умовах цифрових технологій;

7. Дослідити механізми захисту прав людини в умовах цифрових трансформацій та порівняти ефективність регуляторних практик у демократичних і авторитарних державах;

8. Оцінити використання цифрових технологій у політичних практиках, спрямованих на протидію загрозам цифрового тоталітаризму, зокрема, на формування нових механізмів державного і громадянського контролю;

9. З’ясувати політико-правову базу захисту прав людини, що функціонують в умовах цифровізації, та виявити перспективи їх

удосконалення для ефективнішого забезпечення прав людини в цифрову епоху.

Об’єктом дослідженням є цифровий тоталітаризм як явище та наслідки процесу ціфровізації, який кардинально змінює політичну, соціальну, економічну, правову та інші сфери розвитку інформаційного суспільства.

Предметом дослідження є загрози цифрового тоталітаризму демократичному розвитку, форми його прояву та вплив на права людини та політичні свободи.

Методологічна основа дослідження обумовлена предметом, метою та завданнями дисертації. Базується на фундаментальних засадах політичної науки, соціології, міжнародних відносн, державного управління, правознавства, прогнозування, а також на наукових дослідженнях у сфері цифрового тоталіатризму, цифровізації інформаційних суспільств. Вирішення поставлених завдань було зроблено використовуючи комплекс загальнонаукових та спеціальних методів наукового дослідження. Серед загальних методів наукового пізнання, використані такі, як *аналіз* та *синтез*, *узагальнення*, *індукції, дедукції, термінологічний* та *історичний* метод, за допомогою якого визначалося виникнення та розвиток процесу цифровізації.

Запровадження *системного методу* дозволило проаналізувати основні показники цифровізації як об'єктивного процесу, типологізувати прояви сутності цифрового тоталітаризму та розкрити їх в контексті загроз демократії. Він сприяв виявленню переваг та недоліків процесу «оцифровування» суспільства, його сильних та слабких сторін, аналізу цифрових інструментів як елементів системи та звязків між ними, що сприяє прогнозуванню майбутніх наслідків.

Завдяки *аналітичному методу* дослідження були проаналізовані наукові праці та роботи дослідників минулих років щодо контексту наукової

проблематики, узагальнення інформації з різних джерел для вивчення показників цифровізації.

У ході написання роботи було використано також *компаративний метод*, який дозволив встановити спільні та відмінні риси цифровізації у процесах міжнародної взаємодії, порівняти політичні практики прояву цифрового тоталітаризму у авторитарних та демократичних державах.

Були використані спеціальні методи політологічної науки, такі, як *контент-аналіз* завдяки якому були досліджені офіційні нормативно-правові акти, заяви, статті тощо. *Завдяки івент-аналізу* були проаналізовані заяви, відношення, ставлення науковців, політиків, урядів до трансформаційних та цифровізаційних процесів в контексті розвитку інформаційного суспільства.

Наукова новизна одержанних результатів полягає в тому, що вперше у вітчизняній політичні науці здійснено та обгрунтовано комплексний аналіз феномену цифрового тоталітаризму та його загрози демократії в інформаційних суспільствах. Запропоновано авторське визначення цього явища й систематизовано політичні, правові та соціально-культурні заходи протидії.

У процесі дослідження були отримані результати, новизна яких конкретизується в наступному:

Уперше :

- системно проаналізовано та сформульовано теоретико-методологічну основу аналізу цифрового тоталітаризму як системного явища, що виникає в цифрову епоху на основі синтезу цифрових технологій, інформаційного контролю та структур політичної влади;

- запропоновано оновлену типологію форм цифрового контролю, яка враховує як державні, так і корпоративні механізми впливу на інформаційний простір і поведінку громадян;

- досліджено сучасний світовий досвід та сформульоване авторське розуміння «цифрового тоталітаризму» як системи цифрових інструментів та

технологій управління суспільством, що значно посилює характер загроз демократії;

- проаналізовано ключові механізми цифрового контролю, включаючи масове спостереження, алгоритмічне управління та система соціального рейтингу**;**

- доведено, що цифровий тоталітаризм формується не лише в авторитарних державах, але й у демократичних суспільствах унаслідок делегування владних повноважень технологічним корпораціям;

- удосконалено підхід до аналізу інституційної спроможності правозахисних механізмів у контексті цифрових трансформацій через порівняльне дослідження практик регулювання в різних політичних режимах;

- представлено авторське тлумачення феномену «цифрового тоталітаризму», який перестає бути лише домінуванням однієї партії чи концентрацією влади – він трансформується у розгалужену систему соціотехнічного впливу, де контроль реалізується через алгоритмічне управління поведінкою громадян, збір та аналіз персональних даних, моделювання публічного дискурсу, а також нормативне та технічне обмеження доступу до інформації.

Уточнено та доповнено:

- понятійно-категоріальний апарат дослідження цифрового тоталітаризму, з урахуванням міждисциплінарного підходу (соціологія, філософія, політологія, право);

- сучасні наукові підходи до аналізу цифрового тоталітаризму, зокрема його типологія та відмінність від класичних підходів тлумачення;

- системне осмислення викликів та загроз процесів цифровізації для сучасного етапу розвитку демократії;

Набули подальшого розвитку:

- удосконалено розуміння та тлумачення феномену цифрового тоталітаризму в контексті трансформацій демократичних інституцій в інформаційному суспільстві;

- систематизовано загрози демократичним правам і свободам, що виникають внаслідок монополізації цифрових платформ та централізації даних з боку технологічних корпорацій;

- аргументовано вплив цифрових технологій на звуження громадянської участі та перетворення політичного суб'єкта на об'єкт маніпуляції;

- досліджено роль великих технологічних корпорацій у формуванні цифрової архітектури влади та їх вплив на політичні процеси;

Авторським дослідницьким здобутком є збір та аналіз значного масиву фактологічних даних та систематизація існуючих наукових підходів до вивчення феномену цифрового тоталітаризму та його загроз основним стандартам демократії у інформаційному суспільстві.

Практичне значення одержаних результатів. Основні теоретичні положення роботи та запропоновані висновки можуть бути використані у практичній діяльності для врахування переваг та недоліків, а також вироблення ефективного законодавства про закріплення прав та свобод людини та громадянина в умовах цифрового тоталітаризму.

Отримані результати можуть використовуватися у науково-дослідницькій роботі для подальшого дослідження теоретичних питань політології, історії, теорії прав людини; під час навчального процесу при викладанні дисциплін: «Політологія», «Вступ до фаху», «Загальна теорія політики», «Порівняльний аналіз політичних систем», «Сучасна зарубіжна політологія», «Політична культура та ідеологія», «Політичні комунікації», «Політична конфліктологія», «Політичне прогнозування», «Політика і права людини», при написанні курсових, бакалаврських та магістерських робіт, при підготовці методичних рекомендацій з відповідних дисциплін, а також в написанні навчальних посібників. Теоретико-прикладні результати

дослідження використані в роботі Департаменту цифрового розвитку та туризму Одеської обласної адміністрації за напрямом «інформаційна політика», «комунікації з громадськістю», цифрова освіта, в освітянських проектах з медіаграмотності «Фільтр» та платформа онлайн-освіти Prometheus, які мають на меті вчитися визначати маніпулятивний медіаконтент, розрізняти дезінформацію, шкідливі пропагандистські наративи тощо.

Апробація результатів досліджень. Результати, ідеї та висновки теоретико-методологічної складової дисертації обговорювались на наукових конференціях: Міжнародній науково-практичній конференції «Соціально-економічний та політичний розвиток країн в умовах глобальної нестабільності» (м. Одеса, 27 травня 2022 р.); Міжнародній науково-практичній інтернет-конференції. «Сучасні загрози глобальній та регіональній безпеці» (м. Одеса, 29 жовтня 2023 р.); III Всеукраїнській науково-практичній конференції «Трансформація українського суспільства в цифрову еру» (м. Львів — Торунь, 22 березня 2024 р.); VI Міжнародній науково-практичній конференції «Політичні процеси сучасності: глобальний та регіональний виміри». (м. Івано-Франківськ. 8–9 травня 2025 р.); Міжнародній науковій конференції «Сталий розвиток регіонів, міст та спільнот в умовах глобальних перетворень: виклики, можливості, сценарії майбутнього» (16 травня 2025 р. м. Одеса). Також обговорення результатів дисертації відбувалось на методологічних семінарах та щорічних наукових конференціях кафедри політології Одеського національного університету імені І. І. Мечникова (2022–2025 рр.).

Публікації. Основні ідеї, напрацювання, положення та висновки дисертації подані автором у 8 публікаціях: з них 3 статті, розміщені у виданнях, які визнані МОН України фаховими, та 5 тезів виступів на Міжнародних та Всеукраїнських наукових та науково-практичних конференціях**.**

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів з підрозділами та висновками до них, загальних висновків, списку використаних джерел – 286 наймінувань та додатків . Загальний обсяг роботи викладено на 240 сторінках, з них основний текст займає 206 сторінок.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ЦИФРОВОГО ТОТАЛІТАРИЗМУ

1.1. Формування дискурсу тоталітаризму: від класичних до цифрових форм

Феномен тоталітаризму є одним із ключових і водночас найбільш суперечливих у політичній теорії XX століття. Його концептуалізація відображає не лише еволюцію форм політичної влади, але й зміни у характері політичного контролю, що переходить від відкрито репресивних режимів до складних гібридних систем, які базуються на поєднанні насильства, ідеології та сучасних цифрових технологій. У цьому контексті тоталітаризм постає як історично зумовлена політична модель, що зазнає трансформації відповідно до умов розвитку суспільства, технологій та комунікаційних середовищ.

Тоталітаризм (від латин. totalis – цільний, повний) – політичний режим, за яким держава намагається здійснювати повний контроль за всіма сторонами суспільного життя та за принципом: «все у державі, нічого поза державою, нічого проти держави» [87, с.29]. Вивчення класичних моделей тоталітаризму, таких як нацизм у Німеччині, сталінізм у Радянському Союзі, італійській фашизм часів правління Б.Муссоліні чи маоїзм у Китаї, створює теоретичне підґрунтя для подальшого аналізу новітніх форм авторитарного та тоталітарного контролю в епоху цифровізації. Саме через ретроспективний погляд на історичні форми владарювання стає можливим ідентифікувати сталі ознаки тоталітарного режиму, зокрема: монополію на ідеологію, тотальний контроль над особистим і публічним життям, централізовану систему управління, політичні репресії, контроль інформаційного простору та інституційне зрощення партійної влади з державною бюрократією.

Важливим аспектом є теоретичне розмежування понять «тоталітаризм», «авторитаризм» та «диктатура», оскільки «тоталіатризм» має історичну специфіку, концептуальне навантаження та межі застосування в політичному аналізі. Розуміння цих відмінностей дозволяє точніше окреслити характеристики сучасних політичних режимів, особливо у контексті цифрового спостереження, інформаційної маніпуляції та новітніх форм обмеження прав людини. Під авторитаризмом прийнято вважати «недемократичний політичний режим, який передбачає концентрацію влади в руках окремої особи або групи осіб, котрі не прагнуть досягнення суспільної згоди стосовно легітимності їх влади. При цьому відбувається зменшення ролі представницьких інститутів влади і громадян в цілому, вони усуваються від процесу прийняття політичних рішень» [161, с.84].

Поняття «диктатури» розуміється, як «нічим не обмежена політична, економічна та ідеологічна влада у державі або певному регіоні однієї чи кількох осіб, класу, соціальних груп, які у своїх діях спираються на безпосереднє застосування апарату насильства (армії, поліції, карних установ), а також відповідний політичний режим» За словами українського дослідника В. Горбатенко, сутність «диктатури полягає : «в узурпації…політичної влади з наступним поширенням панування на всі сфери життєдіяльності суспільства» [24].

Поняття «тоталітаризм» було вперше розвинуте в ХХ-му столітті і відоме через твори таких авторів, як Ганс Кельзен, який у відомій роботі «Абсолютизм та релятивізм у філософії та політиці», розглядає тоталітаризм, як прояв політичного абсолютизму [228], а також Г. Арендт у «Витоки тоталітаризму» [1]. У цьому творі, авторка, детально аналізує природу тоталітаризму, підкреслюючи його унікальність серед інших форм політичного панування. Також було зазначено, що тоталітаризм не лише прагне до повного контролю над усіма аспектами життя суспільства, але й активно замінює компетентних та талановитих осіб на менш здібних, але

лояльних. Тоталітарні режими характеризуються уніфікованим ідеологічним контролем та масштабним репресивним апаратом, спрямованим на політичних опонентів та інші форми непокори.

Так почався класичний дискурс вивчення поняття «тоталітаризм» в політичній науці. До Ганни Арендт також долучився Карл Йоахім Фрідріх та Збігнев Бжезинський, які у 1956 році випустили спільну роботу «Тоталітарна диктатура і авторкія». Вони першими виділили шість рис тоталітарного режиму, зокрема «основні риси або характеристики, які ми пропонуємо як загальновизнані для тоталітарних диктатур, налічують шість пунктів. Цей «синдром» або сукупність рис включає: розгорнуту ідеологію; єдину масову партію, як правило, очолювану однією особою; систему терористичного поліцейського контролю; монополію на засоби масової комунікації; монополію на озброєння; та централізовано керовану економіку» [219].

Майкл Кертіс у власній роботі «Тоталітаризм», продовжуючи дослідження класичної концепції цього феномену, поєднавши соціологічний, політологічний та філософський підхід, систематизувавши доробки минулих науковців дійшов до узагальнюючих характеристик режиму:

1) Офіційна і єдина існуюча ідеологія чи сукупність поглядів, які суспільство зобов'язується сповідувати і які стають фундаментом створення нового типу політичного і соціального ладу та нової людини.

2) Монополія на контроль не лише над політичним, економічним, соціальним та культурним життям суспільства, але й приватним життям людей, так само і над їх мисленням з метою підкорення всього суспільства.

3) Використання терору, концентраційних таборів і політичної поліції для створення атмосфери повної покори і постійно існуючої загрози для кожної особи.

4) Ієрархічно побудована однопартійна система або режим, створений на основі якого-небудь руху, в якому повністю відсутнє поняття плюралізму в тому сенсі, який у нього вкладають демократи Заходу.

5) Підкорення всіх особистих, суспільних і колективних інтересів, які можуть сприяти розвитку справжньої природи окремої особистості.

6) Як наслідок вищезгаданого, наголос на централізацію влади, єдність і інтеграцію, за яких опозиція і навіть інакодумство розглядаються як злочин.

7) Скасування будь-яких законних обмежень на дії тих, в чиїх руках зосереджена влада.

8) Монополія на контроль над засобами масової інформації, над системами освіти і культури з метою мобілізації суспільства.

9) Відсутність усвідомлених вільних виборів.

10) Монополія на контроль над зброєю і збройними силами.

11) Заперечення права громадян на виїзд за кордон, а в окремих випадках і на пересування всередині країни.

12) Централізоване планування економіки, в якій на процес виробництва здійснюють вплив зовнішні фактори, а споживання контролюється з метою накопичення інвестиційного капіталу.

13) Виключність правителя-диктатора, чия особистість може стати вирішальним фактором, що визначатиме природу даного політичного режиму [257, с.18-19].

Ця класифікація стала однією з універсальною та загальновживаною серед науковців, котрі продовжили поглбилювати дослідження проблематики із урахуванням трансформації тогочасних суспільств.

Ще у 1969 р. К. Фрідріх зробив додаткові уточнення до розуміння тоталітаризму, як феномену. На його думку, «тоталітарний контроль охоплює не лише армію і засоби масової комунікації, але також усі громадські організації, окрім того він не обов’язково здійснюється

політичною партією, а може знаходитись в руках будь-якої правлячої в даній державі еліти» [219, с.14].

Саме через таке зауваження почав також змінюватись контекст вивчення тоталітарного феномену. У середині 1960-х років класичні підходи до вивчення тоталітаризму стала предметом глибокої кризи. Втрата чітких критеріїв до оцінки та перетворення терміну на загальновживаний негативний епітет поставили під сумнів його наукову цінність. Зникнення або трансформація класичних тоталітарних режимів завдала серйозної шкоди усім концепціям тоталітаризму. Відзначилися заклики відмовитись від вживання цього терміну і використовувати теорію тоталітаризму в наукових цілях як штучну конструкцію, мертву схоластичну схему з псевдонауковими постулатами, релікт протистояння часів «Холодної війни».

Дж. Каутський в середині 1960-х рр. вважав, що поняття «тоталітаризм» має лише прикладне значення, яке як поняття, виникло в 1930-і рр. для визначення класичних тоталітарних режимів, а в «1960-і рр. воно вже не відповідало рівню теоретичних знань, недостатньо враховувало відмінності між комуністичною та фашистською системами» [4].

Саймон Тормей у своїй праці «Осмислення тиранії» посилався на невідповідність традиційних підходів та стереотипів класичної західної політології до реалій. С. Тормей стверджував, «що теза Л. фон Мізеса і Ф. фон Хаєка про централізоване планування економікою, яке нібито є «шляхом до рабства», суперечить фактам, адже нацистська Німеччина – один з класичних прикладів тоталітарної держави – не мала централізованого планування, водночас як після II Світової війни західні демократії здійснювали значно більш масштабне втручання в економіку, і не ставали при цьому тоталітарними. На його думку, Г. Арендт настільки захопилась описом Радянського Союзу і нацистської Німеччини як імперій, в яких управляла ідеологія, звільнена від традицій і будь-яких проявів людської натури, що вона виявилась неспроможною осягнути і зрозуміти їх

справжній реальний характер. Якщо К. Фрідріх, Зб. Бжезінський та Г. Арендт вважали, що тоталітаризм намагався зруйнувати традиційне суспільство і перетворити населення на маргіналізовані маси, то С. Тормей у своїй роботі доводив, що нацистський режим відбудовував і реставрував багато елементів традиційного німецького суспільства, перешкоджаючи його модернізації» [257, с.19-20].

В додаток новим запереченям, американський політолог Г. Спіро, узагальнюючи для «Міжнародної енциклопедії суспільних наук» різноманітні концепції тоталітаризму пише: «використання поняття «*тоталітаризм*» стає все більш проблематичним і разом із зникненням тоталітарних країн, можливо, скоро взагалі зникне із вжитку і сам термін» [257, с.16].

Так, в науковий дискурс виходять представники філософських шкіл з бажанням переосмислити та адаптувати тоталітарну форму під нові часи. Так, представник «Франкфуртської школи» Еріх Фромм, ще у 1941 році у своїй роботі «Втеча від свободи», досліджуючи питання індивидуума у соціумі пише : «сучасна людина перебуває в такому становищі, коли багато з того, що «вона» думає і говорить, є речами, які думають і говорять усі інші; … що лише надає значення його заяві про те, що ніхто не може втручатися у вираження його думок» [221, с.63].

Таким чином, мислення індивіда не є оригінальним, а тоталітарна влада здатна нав’язувати хід думок та залежність від державного керованого простору.До цих філософських переосмислень спонукало і зауваження Г. Арендт у роботі «Витоки тоталітаризму». Вона пише: «Безсумнівно…тоталітарне правління … спирається на масову підтримку... Нещодавно опубліковані секретні доповіді про стан громадської думки в Німеччині…Вони демонструють, по-перше, що населення було дуже добре поінформоване про так званні таємно-масові вбивства євреїв у Польщі, підготовці нападу на Росію та інше, а по-друге, ту «ступінь, в якій

піддаються пропагандистської обробки зберігали здатність до формування незалежних суджень» [1, с.3].

Отже, і хоча народ мав можливість до альтернативного ставлення щодо подій в Нацистській Німеччині, проте цілком достатньо підтримував такі рішення без масових спроб до опіру. Еріх Фромм, у роботі «Здорове суспільство» у 1956 році продовжує декларувати індивідуальну співзалежність людей із тоталітарною владою, зокрема «індивідуум змушують почувати себе безсильним і незначним, але привчають направляти всі свої людські сили на постать лідера, держави, «батьківщини», яким він повинен підкорятися і яким він повинен поклонятися» [220, с.230]. Аналізуючи феномен тоталітаризму крізь історико-філософську призму, Е. Фромм доречно вийшов за межі суто інституційного розуміння цього явища.

Герберт Маркузе продовжив змінювати аспект дослідження тоталітаризму у власній роботі «Одновимірна людина» через філософський підхід Франкфуртської школи та писав, що «виробничий механізм прагне стати тоталітарним тою мірою, якою він детермінує не лише суспільно-потрібні спеціальності, вміння й установки, а й потреби й прагнення індивіда» [69, с.92-93]; адже «тоталітарне» тут означає… «нетерористична економіко-технічна координація, яка діє шляхом маніпуляції потребами з боку підприємців» [69, с.96] Отже, тоталітаризму сприяє не тільки специфічна форма уряду або правлячої партії, але «особлива форма виробництва і розподілу, що добре може бути сумісним з «плюралізмом» партій, газет, «конкуруючих сил» тощо».

Здатність тоталітарних проявів до мімікрії у ліберально-демократичних режимах призводить до того, що «Тоталітарні тенденції одновимірного суспільства роблять традиційні способи й засоби протесту недієвими – можливо, навіть небезпечними» [69, с.131].

Французький філософ Мішель Фуко, вивчаючи та розглядаючи власну «дисциплінарну» концепцію влади у роботі «Наглядати і карати»

також змінив акцент вивчення проблематики, тоталітаризм в його роботі постає не як продовження еволюції влади, що набирає нових форм *тотального контролю через дисциплінарні інститути***,** такі як : в'язниці, школи, лікарні, армія. Він дійшов висновку, що на прикладі тюремної паноптичної системи нагляду та споглядання за ув'язненими Єремії Бентама люди стають назкрізь скореними. Фуко пише: «У дисципліні суб'єкти повинні бути видимими. Їхня видимість забезпечує утримання влади, яка здійснюється над ними. Сам факт постійної видимості підтримує дисциплінована людину в її підпорядкуванні» [214].

Паноптичний підхід ставлення до людей з боку влади постійно зводить індивіда до сприйнятя власного підпорядкування всім державним інституціям через дисципліну, просторовий контроль та безперервний нагляд за кожним рухом.

Жиль Дільоз у власному есе Постскриптум до «Суспільств контролю», апелючи до концепції дисциплінарної влади Фуко, пише: «У дисциплінарних суспільствах увесь час доводилося починати спочатку (від школи до казарми, від казарми до фабрики), тоді як у суспільствах контролю ніколи нічого не закінчується — корпорація, освітня система, збройні сили є метастабільними станами, що співіснують в одній модуляції, як універсальна система деформації» [201]. Прогресуючи разом із НТР та ІКТ владні та державні інституції на думку Ж. Дільоза – не тільки тримають дисципліну, а ще й формують тотальний контроль за суспільством.

Вже у 1992 році Ж. Дільоз вбачав майбутні перетворення тоталітарних форм влади описуючі усі прояви втручання у сферах життєдіяльності суспільств: «У тюремній системі… спроба знайти покарання «заміни», принаймні, за дрібні злочини, та використання електронних нашийників, які змушують засудженого залишатися вдома у певний час. Для шкільної системи: безперервні форми контролю та вплив на школу постійного навчання, відповідну відмову від усіх університетських досліджень, запровадження «корпорації» на всіх рівнях

навчання. Для лікарняної системи : нова медицина «без лікаря та пацієнта», яка виділяє потенційно хворих людей та суб'єктів ризику, яка аж ніяк не свідчить про індивідуалізацію – як вони кажуть – але замінює індивідуальне чи числове тіло кодом «індивідуального» матеріалу, що підлягає контролю. У корпоративній системі нові способи поводження з грошима, прибутком і людьми, які більше не проходять через стару фабричну форму» [201].

Аналіз доробків у вивчені тоталітарних режимів дає можливість, на думку дисертанта, підкреслити, що починаючи з другої половини 1980-х років, у дослідницькому полі західної політології відбувся помітний зсув акцентів: увага провідних аналітиків поступово зміщувалася від глибокого вивчення природи та внутрішньої логіки функціонування тоталітарних режимів до аналізу процесів демократизації, політичної лібералізації та трансформаційних змін у посттоталітарних суспільствах. Такий поворот у науковому дискурсі був зумовлений, як кризовими тенденціями в соціалістичному таборі, так і новими методологічними викликами, що поставали перед дослідниками в умовах зміни глобального ідеологічного клімату.

Особливої актуальності набули дослідження, присвячені механізмам переходу від авторитарних/посттоталітарних форм правління до плюралістичних моделей політичної організації, пошуку інституційної спадкоємності та формування нової легітимності в посттоталітарному просторі.

Разом із тим, несподіваний та фактично не передбачений жодною з основних парадигм крах СРСР у 1991 році став серйозним викликом для наукового дискурсу. Ця подія не лише поставила під сумнів аналітичну ефективність і прогностичну здатність багатьох західних підходів до вивчення феномену тоталітаризму, як політичної системи, а й завдав потужного удару по науковому авторитету класичних дослідників, які впродовж десятиліть спеціалізувалися на аналізі тоталітаризму, структури влади та державної політики.

У результаті наукова спільнота була змушена переглянути методологічні основи дослідження тоталітарних режимів і шукати нові інтерпретації для пояснення як процесів занепаду тоталітарних систем, так і характеру перехідних політичних форм, що виникали на їхньому місці.

Отже, критичний аналіз еволюції поняття «тоталітаризм» у його класичних трактуваннях є необхідним аналітичним кроком на шляху до дослідження його новітніх проявів у цифрову добу.

У більшості визначень, запропонованих провідними дослідниками, наголошується, що *тоталітаризм* — це специфічна форма суспільно-політичного устрою, за якої держава не просто виконує функції управління, а прагне до всебічного, тотального контролю над усіма сферами життя суспільства — від економіки та політики до культури, освіти, релігії та приватного простору особистості. Такий контроль реалізується через монополізацію ідеології, репресивний апарат, централізовану владу, систему масового нагляду, а також постійне втручання у свідомість і поведінку громадян.

Рубіж XX–XXI століть став важливою віхою у розвитку західної політичної теорії, зокрема в аспекті переосмислення концепту тоталітаризму. Сучасні зарубіжні дослідники, такі як, Ш. Зубофф, Ю. Харарі Д. Хелбінг,В. Хендрікс, М. Вестергард, Й. Седраті та вітчизняні дослідники, такі як О. Добродум, Т. Комарова, С. Наукмкіна, О. Об’єдков, все більше зміщують акценти з аналізу інституційно-правових аспектів функціонування тоталітарних режимів на вивчення глибинних ідейних та ціннісних засад, які обґрунтовують їхню легітимність та впливають на суспільну свідомість. Увага фокусується не лише на механізмах організації влади, а передусім на ідеологічних, комунікативних та символічних практиках, через які ця влада підтримується, нормалізується та відтворюється.

Значний інтерес викликає також виявлення структурної подібності між різними формами тоталітаризму – як історичними, так і новітніми, які

набувають особливої актуальності в умовах цифровізації політичного управління. Зокрема, йдеться про способи формування колективної ідентичності, централізованого управління знаннями, технології масової комунікації, що дозволяють здійснювати як маніпуляцію свідомістю, так і контроль за інформаційними потоками.

Таким чином, сучасна наукова дискусія навколо тоталітаризму виходить за межі класичного уявлення про репресивну владу та набуває більш складного, багатовимірного характеру, що поєднує в собі аналіз політичних інститутів, соціокультурних практик та технологічного впливу. У різних наукових джерелах використовуються декілька варіантів цього поняття: «цифровізація», «діджиталізація», «інформатизація» тощо.

Поняття «діджиталізація» – з англ. *«didgitalization»*, перекладається як *«digital»* – «цифра», а суфікс *«-ization»* означає процес. Тобто можна констатувати, що це «оцифровування» – переклад аналогових даних у цифровий вигляд. Нині ця тенденція спостерігається в усьому світі, зокрема і в Україні, вона виникла і застосовується завдяки новим розробленим цифровим технологіям, що дозволяють людям оброблювати, зберігати й використовувати необхідну інформацію [5].

Однак не можна обмежуватися тільки таким визначенням, адже процес цифровізації суспільства відноситься не лише до пристроїв. Він також стосується людей, які активно користуються цифровими технологіями. Така взаємодія є безпосереднім контактом, що дозволяє цифровим технологіям і людям впливати однин на одного або групи людей на групу і взаємопроникати один в одного.

Слід погодитися із дослідниками, що «цифрові інновації, зокрема розвиток інформаційних технологій, спричинив формування та зародження світової цифровізації й визначив появу феномена – інформатизованого сучасного суспільства. Відтак цифровізація абсолютно усіх процесів проникла в усі сфери людського життя й змінила світ. Тепер всі інноваційно-технологічні процеси тісно пов’язані між собою та

переплітаються з так званою «цифровою трансформацією», що є вираженням масштабної цифрової революції – діджиталізації суспільства, в якому живе і будуть жити нові покоління. У результаті цього виник новий тип реальності, електронні інформаційні ресурси, технічні засоби комунікації і мережева мова, що призвело до істотних змін в соціальному житті суспільства [15, с.13].

«Цифровий тоталітаризм» як феномен народжується завдяки сучасним інформаційним та комунікаційним технологіям, що знаходиться через підтримку незадоволених прошарків населення, що відчувають загрозу ззовні, наприклад, «через неконтрольоване поширення небезпечних хвороб та вірусів, а тому позитивно сприймаючої запровадження механізму електронного відстеження хворих; або людини, наляканої поширенням небезпечних ігор для дітей, таких як «Тихий дім», «Розбуди мене о 4:20», «Море китів», «Чумацький шлях», «NaN», «F57», та інших, а тому позитивно сприймаючої запровадження механізму електронного втручання та контролю на загальнонаціональному рівні» [136, с.13].

Дірк Хелбінг – німецький вчений, вивчаючи питання цифрового тоталітаризму – виділяє наступні риси сучасних цифрових тоталітарних суспільств, а саме:

1) масове стеження;

2) неетичні експерименти з людьми в рамках існування соціальної інженерії;

3) Соціальна інженерія;

4) примусове підпорядкування людей;

5) пропаганда та цензура;

6) існування «доброзичливої» диктатури;

7) поліцейська діяльність, тобто наявність «поліцейської держави»;

8) виборче застосування забезпечення прав людини [227].

Сучасна американська дослідниця, професорка, соціальний психолог, Шушана Зубофф у роботі «Наглядовий капіталізм» торкається тематики

цифрового тоталітаризму, замінюючи це поняттям «інструментарної влади» (*instrumentarian power*), яка відрізняється від традиційного тоталітаризму тим, що не прагне до ідеологічного контролю над свідомістю, а зосереджується на поведінковому впливі через цифрові технології.

Вона стверджує, що ця нова форма влади загрожує індивідуальній автономії та демократичним цінностям. «Я називаю це інструментарною владою, на відміну від тоталітарної влади. Інструментарна влада хоче контролювати вас, але їй байдуже, чи завдає вона вам шкоди. Вона хоче контролювати вас для забезпечення гарантованих комерційних результатів. Ви стаєте засобом для досягнення комерційних цілей інших» [263].

Ш. Зубофф також попереджає про небезпеку злиття державної влади з можливостями ТНК (транс-національних коропрацій), цифрових корпорацій, які можуть призвести до нової форми контролю, яку вона називає «сценарієм злиття» (*fusion scenario*). У цьому сценарії державна влада використовує цифрові технології для посилення контролю над громадянами, що має подібності до тоталітарних практик. «Капіталізм нагляду – це ляльковод, який нав'язує свою волю через повсюдний цифровий апарат» [263].

Українська дослідниця С. Наумкіна описуючи приклади «цифрового тоталітаризму», як системи обмеження, контролю та спостереження, що порушують фундаментальні права та свободи людей, а також обмежують права вільного користування світовими сервісами – посилається на встановлені таких режимів «більшості країни світу: США, Великобританії, Німеччини, Франції, Китаї, РФ, Україні, Кубі, Ірані та ін» [78, с.151].

Юваль Ной Харарі – ізраїльский військовий історик та футуролог, виступаючи з темою-застереження «Як вижити у XXI столітті» на Давоському Форумі у 2020 році , виділив майбутні загрози людству : ядерна війна, екологічний колапс і технологічний зрив. І якщо, перші дві загрози, на думку, вченого вже давно відоми, то остання – максимально актуальна сьогодні. Він застереджує про потрясіння на соціально-економічному рівні,

про Революцію ШІ, яке може створити безпрецедентну нерівність не лише між класами, а й між країнами, про зростання цифрових диктатур, які постійно стежитимуть за всіма**.** Також, науковець підкреслює, що потенціал та сила сучасних технологій у руках урядів та ТНК можуть привести до «найгіршого тоталітарного режиму в історії людства» [251]. О.Добродум активно наголошує, що «цифровий тоталітаризм у політичній площині може вбачатися через підтасовування під час виборчого процесу та електоральні фальсифікації у зв'язку з підрахунком результатів голосування» [29, с.52].

Такі застереження відносять нас до творів XX століття, як «Суспільство спектаклю» Гі Дебора [200] та «1984» Джоржда Оруєлла , в яких автори описують суспільства, котрі контролюються через дієві апарати, накшталт «телекранів» у Оруєлла [83] та методів «телематичного контролю» Дебора.

Отже, ретроспективний аналіз еволюції концепту тоталітаризму, а також його сучасного переосмислення у світлі стрімкого розвитку інформаційно-комунікаційних технологій засвідчує, що поняття «тоталітаризму» перестає бути виключно історичним або політико-ідеологічним явищем. Натомість, воно набуває нового, складнішого змістовного наповнення, у якому класичні риси репресивного режиму поєднуються з інноваційними цифровими інструментами соціального контролю.

Дисертант вважає, що сучасний «цифровий тоталітаризм» перестає бути лише домінуванням однієї партії чи концентрацією влади – він трансформується у розгалужену систему соціотехнічного впливу, де контроль реалізується через алгоритмічне управління поведінкою громадян, збір та аналіз персональних даних, моделювання публічного дискурсу, а також нормативне та технічне обмеження доступу до інформації.

У рамках цієї моделі особистість втрачає автономію, оскільки будь-яка форма інакомислення або незалежної дії розглядається як загроза для політичної системи. Держава в умовах тоталітаризму не визнає жодних меж

для своєї влади та активно підмінює собою інститути громадянського суспільства. Саме через таку всеосяжну інтеграцію державної влади в тканину суспільного життя тоталітаризм вважається найбільш жорсткою і радикальною формою політичного панування, яка базується на примусі, страху та системній ізоляції індивіда від альтернативних джерел інформації чи форм самоідентифікації.

Ця особливість робить тоталітаризм фундаментально відмінним від інших недемократичних режимів – зокрема авторитаризму чи класичних диктатур, – що передбачає необхідність чіткого теоретико-історичного розмежування між цими поняттями в межах політичної науки.

У таких умовах цифрові технології – від систем розпізнавання облич до штучного інтелекту та великих даних – стають не лише інструментом прогресу, а й потенційною загрозою правам і свободам особистості. Це вимагає глибокого переосмислення підходів до захисту прав людини, адаптації існуючих політико-правових теорій до нових умов, а також консолідованої реакції з боку демократичних інституцій, академічної спільноти та громадянського суспільства на глобальні виклики, пов’язані із цифровим домінуванням.

Таким чином, на нашу думку, дослідження цифрового тоталітаризму як явища, як феномену сучасного суспільства, що водночас черпає своє ідейне підґрунтя у класичних формах політичного панування і активно реалізується за допомогою високих технологій, відкриває нові горизонти для міждисциплінарного аналізу, зокрема в політичній науці, правознавстві, філософії та соціології.

1.2. Інформаційне суспільство як цифровий етап розвитку демократії та загроз для неї

У сучасних умовах інформаційні технології відіграють ключову роль у трансформації суспільного розвитку, що набуває особливого значення в контексті демократичних процесів. Йдеться не лише про технологічну зміну

середовища людського існування, що оптимізує процеси комунікації, освіти, виробництва та інших сфер життєдіяльності, але й про фундаментальне переосмислення базових понять, цінностей і способу буття людини.

Формування інформаційного суспільства супроводжується глибокими трансформаціями у всіх сферах соціального життя, внаслідок чого виникають нові морально-етичні виклики та посилюються суперечності між усталеними традиційними і новітніми інноваційними ціннісними орієнтирами. Особливої актуальності набувають питання діджиталізованого спілкування, кіберзлочинності, забезпечення інформаційної безпеки, контролю за приватним життям індивіда, відповідності його поведінки в реальному та віртуальному просторах, а також феномену створення віртуальних або псевдоособистостей.

Сьогодні беззаперечним визнається факт необхідності впровадження та повсюдного використання інформаційних технологій. Проте, цей процес вимагає чіткого нормативного регулювання, що повинне враховувати моральні вимоги в новому соціально-комунікативному контексті. У зв’язку з цим наукове гуманітарне знання покликане здійснити ціннісне осмислення цифрових трансформацій, сформувати відповідні етичні орієнтири та виробити нормативні підходи до нових соціальних практик, які виникають унаслідок стрімкого розвитку інформаційних технологій. Це особливо важливо в контексті забезпечення збереження демократичних інститутів і цінностей, що опиняються під загрозою в умовах феномену цифрового тоталітарного впливу на суспільну свідомість і поведінку. Упродовж XX століття широкого поширення набула концепція, згідно з якою науково-технологічний прогрес став фундаментальним чинником суспільного поступу.

Ще у 1627 році, Френсіс Бекон у роботі «Нова Атлантида» вперше, чітко подав тезу про те, що «прогрес людства, джерело його постійного

процвітання забезпечується шляхом розвитку науки і технології: «знання – сила» [166, с.6].

Спираючись на доробоки Сен-Симона *«Про теорії суспільної організації»*, *«Про промислову систему»* , *«Катехізис промисловців»* (1819 – 1823) [230], Герберт Спенсера «*Основи соціології*» [138], Еміля Дюркгайма «Про поділ суспільної праці» [204], та Огюст Конта «*Курс позитивної філософії*» [195] було сформовано та закріплено поняття *індустріального суспільства* – «соціальної системи, в якій основним видом господарської діяльності є промислове виробництво» [166, с.7].

Вже тоді філософи виказували думку про те, що новий клас індустріалів, має нову органічну форму солідрності та здатен забезпечити прогрес та добробут в індустральних суспільствах.

Подальше вивчення та фіксація ступінів розвитку індустріальних суспільств була в роботі Волта Вітмена Ростоу «Стадії економічного росту», який виокремив 5 стадій економічного зростання, а саме :

1) Традиційне суспільство;

2) Період до передумов;

3) Період зсуву;

4) Рух до зрілості;

5) Вік високого масового споживання [166].

Саме остання стадія описувала новий перехідний етап від індустріального суспільства до нової формації.

У 1960 – 70-х роках передові західні країни почали переживати етап стрімкого економічного та науково-технологічного зростання, це було пов’язано із процесами масової комп’ютеризації управлінських процесів, усебічного розвитку телекомунікацій, та зміни в структурі зайнятості – перехід робітничих прошарків населення у сферу послуг із поступовим розмиттям класових відміностей.

Саме такий перебіг подій було зафіксовано амереканським соціологом Деніелом Беллом у власній роботі «Прихід постіндустріального

суспільства» [173] він, «сформулював основні ознаки нового суспільства – створення економіки послуг, домінування прошарку науково-технічних спеціалістів, центральна роль теоретичного знання як джерела новацій і політичних рішень у суспільстві, можливість самопідтримуючого технологічного зростання, створення *інтелектуальної» техніки*» [166, с.12-13].

Вже у статті «Соціальні рамки інформаційного суспільства» рефліксуючи на зміни за короткий термін часу, він пише, що «знання та інформація стають стратегічними ресурсами та агентом трансформації постіндустріального суспільства» [7, с.312]. Також автором було доцільно підкреслено, що еліти та політики використовуючи нові знання в нових інформаційних суспільствах будуть мати владу «в межах інститутів», і хоча Д. Белл в силу обставин не приділяє увагу силі та можливостям пов'язаних з владою та силою влади у постіндустріальних інформаційних суспільствах, все ж таки, він, підкреслює: «у світі великої політики вона володіє... впливом...» [7, с.314] .

Японський соціолог та футуролог Йонезі Масуда у власній книзі «Інформаційне суспільство як постіндустріальне» також загострив увагу на терміні «інформаційное суспільство», вбачаючи новий прогрес капіталістичних та демократичних країн з часом.

«Інформаційне суспільство, – відкриває нове поняття свободи і рівності, що втілюватиме свободу прийняття рішень і рівність можливостей. Найбажанішою свободою буде та, яка передбачає вільний вибір людиною напряму реалізації цінності часу в процесі використання доступного для неї майбутнього часу. Назвемо це *свободою рішення*. Йдеться про вибір цілеспрямованої дії і право кожного вільно визначати, як використовувати майбутній час для досягнення мети» [70].

Розуміючи, на скільки інформаційні знання в нову епоху стають фундаментальнеми для людей, Й. Масуда в наступній роботі виводить для

себе новий вид людей, як «*Homo intelligens*», тобто, «Людина інтелектуальна».

Так, за цитатою українського дослідника В.Ляха «Найголовнішим завданням Homo intelligens стане розбудова суспільства нового типу. Це буде глобальна спільність громадян, котрі утворюватимуть поліцентроване, комбіноване суспільство, схоже на організм, з розгалуженою мережею прямого зв'язку, призначеного для забезпечення швидкої і динамічної відповіді на зміну зовнішнього середовища. На зміну різним державним установам і формам організації соціальної поведінки має прийти вільне об'єднання громадян, діяльність яких спрямовуватиметься на попередження й оптимальне розв'язання кризових явищ» [66, с.9].

Розуміючи, на скільки технології впливають на зміні індустріального суспільства Масуда вважав, що «інформаційному суспільстві» головним «суб'єктом соціальної активності стане «вільне співтовариство», а політичною системою – «демократія участі» [166, с.14].

Розуміючи та прогнозуючи встановлення інформаційного суспільства, автор також застерігає простеження коло питань, навколо так званих футурошоків, які «зумовлені неспроможністю людей адекватно відповісти на швидкі соціальні трансформації, дії індивідуальних і групових терористів, зазіхання на індивідуальну самотність та криза підконтрольності». Аналізуючи, обсяг використання комп'ютерних машин з технічної точки зору, також застерігав про контроль над суспільствами, щоможе стати дійсністю [129, с. 158-159].

Також, Масуда, вів у науковий обіг термін «к*омп'ютопію*» , під яким вважається нове утопічне технічно-інформаційне суспільство XXI століття. Паралельно з Масудою, поняття «*інформаційного суспільства*» довершував амереканський соціолог та футуролог Елвін Тоффлер. У власній роботі «*Третя Хвиля*» [270] він розглядає нову трансформаційну форму, як так звану «третю хвилю», яка може призвести, як до суперіндустріального суспільства або постіндустріального чи інформаційного. «Людство

зіткнулося з квантовим стрибком уперед. Воно зіткнулося з найглибшими соціальними потрясіннями та творчою перебудовою всіх часів. Не усвідомлюючи цього чітко, ми займаємося будівництвом чудової нової цивілізації з нуля. У цьому сенс Третьої Хвилі» [270].

Розуміючи зміни демократичних режимів з новими технологічними стрибками, автор пише «Усі структури доведеться фундаментально змінити не тому, що вони за своєю суттю злі, і навіть не тому, що їх контролює той чи інший клас чи група, а тому, що вони стають дедалі непрацездатнішими – більше не відповідають потребам радикально зміненого світу» [270, с.435].

Аналізуючи можливі трансформації, Тоффлер бачить демократію у XXI столітті у наступних формах :

1) Влада меншин. Той головний блок, який повинен за Тоффлером стати орієнтиром для нових владних структур через проблему залученості більшості в суспільстві до державних проблем. «Сьогодні, як ми бачимо… швидко стаємо демасифікованим суспільством. Як наслідок, стає дедалі важче – часто неможливо – мобілізувати більшість або навіть правлячу коаліцію» [270, с.436].

Через таку проблему, на думку автора, треба реформувати суспільства XXI століття у маленькі групи, які будуть об’єднуватись у час прийняті важливих політичних рішень «Замість високо стратифікованого суспільства, в якому кілька основних блоків об'єднуються, щоб сформувати більшість, ми маємо конфігуративне суспільство — таке, в якому тисячі меншин, багато з яких тимчасові, кружляють і формують дуже нові, швидкоплинні моделі» [270, с.436].

2) Сама демократія повинна стати «напівпрямою». Це другий блок, на якому має формуватись інформаційне суспільство XXI століття. В цілому, майбутні демократії, за думкую Тоффлера, мають зосередитись на питаннях розподілу прийнятя рішень, питаннях якісного розширення еліт та ролі використання технологій у процесах прийняття рішень. «Розпад переговорів, криза прийняття рішень, посилення паралічу представницьких

інституцій означають, що в довгостроковій перспективі багато рішень, які зараз приймаються невеликою кількістю псевдопредставників, можливо, доведеться поступово повернути до самого електорату. Якщо наші обрані посередники не можуть укладати угоди за нас, нам доведеться робити це самостійно. Якщо закони, які вони приймають, будуть дедалі віддаленішими від наших потреб або не відповідатимуть їм, нам доведеться приймати їх самостійно. Однак для цього нам також знадобляться нові інституції та нові технології» [270, с.444].

Виходячи з таких застережень, технології, які не будуть спрямовані на розширення участі громадян, а використовуватимуться для контролю, моніторингу та маніпуляцій (як у випадку з алгоритмічним управлінням, соціальним кредитуванням або цензурою в соцмережах), демократія може перетворитися на форму фасаду під якими влада може контролювати такі меншини. Також Тоффлер застерігає про те, що «політичний механізм прийняття рішень у країнах дедалі більше напружується, перевантажується, завантажується нерелевантними даними та стикається з незнайомими небезпеками» [270, с.410].

Тоффлер, став першим автором, який масштабно та системно описав *інформаційне суспільство як шанс для оновлення демократії*, але водночас попередив, що без адаптації політичних інституцій та освіти громадян ці можливості можуть бути зруйновані або викривлені. Він також наголошує, що технології, як такі, не врятують демократію — потрібне переосмислення й реформування, інфраструктурні зміни, так і культурні та освітні зрушення. Його роботи стали підґрунтям для подальших досліджень цифрової демократії та цифрового тоталітаризму.

Мануель Олівіан Кастельс – іспанський соціолог провів фундаментальні дослідження питання зародження, становлення, розповсюдження та майбутнього так званих «інформаційних суспільств» у власній роботі «*Інформаційна епоха : економіка, суспільство та культура*». В своїй роботі, він влучно аналізує комбінування проявів влади на рівні

політичних та суспільних інституцій та характеристик «інформаційних суспільств». За словами М. Кастельса, нові інформаційні суспільства , використовуючи Інтернет, як засіб комунікації стають «мережевими» із характерними ознаками :

1) Технології впливають на інформацію;

2) Всеохоплюючий ефект нових технологій;

3) Мережевий характер взаємодії технолгій;

4) Гнучкість інформаційно-технологічної парадигми;

5) Конвергенція технологій в інформаційному суспільстві;

Такі характеристики остаточно закріплюють рушійну роль інформаційно-технологічного прогресу в політичних змінах.

Сучасні технології призводять до «розмивання меж суверенності» , які ведуть до «невизначеності у процесі делегування волі народу» [191, с.501]. Тому за думкою автора «децентралізація владних повноважень та перехід їх до регіональних та локальних урядів створюють нову геометрію влади, можливо, породжуючи нову форму держави – мережева держава» [191, с.501].

За думкою автора, влада в інформаційному суспільстві «стає вписаною на фундаментальному рівні в культурні коди, за допомогою яких люди та інститути представляють життя та приймають рішення, включаючи політичні рішення» [191, с.502]. З урахуванням, порушення комунікації – як способі орієнтації в суспільстві «соціальні групи та індивіди відчужуються одна від одної і бачать в іншому чужинця, а потім і ворога». Безпосередньо, «суспільства дедалі більше структуруються навколо біполярної опозиції між Мережею та Я” » [191, с.27].

Таким чином, в нових мережевих суспільствах зростає рівень розшарування та фрагментації людей. Він пише про зростання несправедливості в розподілі благ, яка є невіддільним супутником вищезгаданих економічних перетворень. До того ж, суспільство стало

занадто захоплюватись феноменом іміджу (як у сфері культури, так і політики) та комерціалізації комунікативного простору [166, с.17].

Ян Ван Дейк, нідерландський професор комунікаційних наук, у власній книжці «The Network Society» приходить до висновків, «що сучасне суспільство перебуває в процесі перетворення на мережеве суспільство, так само як воно розвивається в інформаційне суспільство, що є пов'язаними концепціями» [237, с.241]. Тобто, стадія розвитку інформаційних суспільств, ще не закінчена. Сутність та нова складіність інформаційних суспільств – полягає в їхніїх мережевих зв’язках у вигляді біологічної нервової системи. В Інтернеті міжособистісна, організаційна та масова комунікація поєднуються.

Отже, діючими елементами з боку влади в мережі інтернет – є поєднання класичних та нових методів керування та контролю за суспілствами. І якщо, навіть існує робота над розмежуванням особистоті, кордонів та культур, «…все одно буде базуватися на тілах, розумі, правилах та ресурсах усіх видів» Автор також застережує, що «загальнодоступні комп’ютерні мережі, що використовуються, також втручаються в нашу особисту конфіденційність» [237, с.241].

Також, вважається, що інформаційні суспільства та зв’язки – є прогнозуючими та спланованими. Ван Дейк підкреслює, що «теоретично інформаційне та мережеве суспільство можна спроектувати до того, як воно буде впроваджено на практиці. Такі проекти насправді створюються в рамках низки політичних перспектив або моделей для побудови інформаційного суспільства, інформаційної супермагістралі, глобальної інформаційної інфраструктури» [237, с.244].

Новий етап розвитку інформаційного суспільства також супроводжується низкою проблем для сьогоденної демократії в контексті загроз «цифрового тоталітаризма» :

1) Девіантна поведінка в мережі Інтернет, яка супроводжується різкими змінами у поведінковому прояві через вплив ІКТ на людину.

«Сьогодні це прагнення задовольняється нав'язливим бажанням увійти в Інтернет, перебуваючи off-line, і нездатність вчасно відключитися від Інтернету, будучи on-line» [166, с.116].

2) Інтернет-залежність, яка стає причинно-наслідковим явищем за рахунок, розподілу на життя в ритмі on-line та off-line. Прояви залежності були описані американським психітаром Айвеном Голдберг у 1995 році, та визначено, як «патологію, розлад, надмірне використання цієї технології, включаючи широкий спектр поведінки та контролю імпульсів» [260].

3) Проблема ідентифікації в інтернеті. Так, відома американська дослідниця Шеррі Тьоркл, у своему дослідженні «Конструкції та реконструкції Я" в культурі віртуальної реальності Інтернету» пише, що ідентичність під впливом мережі Інтернет може «множиться і розкладається, залишаючи присмак тривоги і неспокою» [272, с.143].

4) Маніпуляція свідомістю та підсвідомістю людини у Інформаційному середивищі.

На думку українських вчених, Бордюгової та Штанько, «впровадження сучасних автоматизованих баз даних і знань, сучасних систем і засобів медіатизації та надпотужних обчислювальних центрів у сферу державного управління й контролю за діяльністю населення, підприємств, фірм та суспільних організацій висуває на авансцену політичного життя проблему трансформації політичних режимів» [166, с.82].

В контексті таких історичних зрушень переформатовувань, питань ідентифікації, самоідентифікації громадян в інформаційному суспільстві виникає нагальна потреба в аналізі загроз демократії.

Так автори розрізняють два спрямовані напрямки демократії в інформаційну епоху, а саме :

1) Покращення та підсилення демократії з характерними напрямками у бік зміцнення «прав людини та індивідуальної свободи і формування

суспільства, орієнтованого на реалізацію потенційних можливостей людини у відповідності з їх запитом з боку суспільства»

2) Трансформації та поштовх тоталітарних, авторитарних тенденцій з рисами «деградації демократії та підсилення поліцейського контролю над особистістю, формування суспільства з абсолютним контролем на підгрунті новітніх технологій» [166, с.82].

Вивчаючи поєднання інформаційно-комунікативних технологій, експератами-політологами було введено такі поняття, як електронна або е-демократія» та «цифрова демократія», «теледемократія», «віртуальна демократія» або «кібердемократія»[205], які з часом пройшли наукову дискусію та закріпились навколо перших двух понять.

Прийнято вважати , що «електронна демократія – це демократична політична система, в якій комп'ютери і комп'ютерні мережі використовуються для виконання функцій демократичного процесу, таких як поширення інформації та комунікації, об'єднання інтересів громадян і прийняття рішень (шляхом наради і голосування)» [132, с.8].

Ральф Ліндер та Георг Айхгольцер у своїй роботі «E-Democracy: Conceptual Foundations and Recent Trends» (2020) відмічають, що сподівання, які були покладені на зв'язок ІКТ з е-демократією є дуже «складними» та «суперечливими» через залежність можливої оцінки «ефектів» на демократію від самої моделі «демократії» до, якої вони відносяться [205].

У 2000 році, Кеннет Хакер та Ян Ван Дейк, у роботі «What is digital democracy?» підсумували такі очікування у власні твердження, а саме :

1) ІКТ збільшує масштаби та швидкість надання інформації. Це допомагає створити більш проінформованих громадян.

2) Політична участь стає легшою, а деякі перешкоди, такі як апатія, сором’язливість, інвалідність, час тощо, можуть бути зменшені.

3) СМС створює нові способи організації з тематично окресленими групами для обговорення, низькими витратами на розповсюдження тощо.

4) Мережа дозволяє новим політичним спільнотам виникати без втручання держави.

5) Ієрархічна політична система стає більш горизонтальною.

6) Громадяни матимуть більше голосу у створенні порядку денного для уряду.

7) СМС допоможе усунути посередників, які спотворюють ситуацію, таких як журналісти, представники та партії.

8) Політика зможе більш безпосередньо реагувати на занепокоєння громадян.

9) ІКТ допоможе вирішити проблеми представницької демократії, такі як територіальні основи виборчих округів, у противагу таких очікувань серйозною загрозою, яка привертає особливу увагу є зростаючий потенціал радикалізації та мобілізації Інтернету [205].

На думку І.М. Милосредної, «в умовах трансформації політики під впливом ІКТ разом з формуванням електронної демократії, електронного уряду та електронного урядування відбувається формування цифрової бюрократії, яка передбачає створення та впровадження нових алгоритмів взаємодії суб'єкта та об'єкта політико-управлінської діяльності» [74, с.108].

Розуміючи таку амбівалентність, італійський вчений Даніло Дзоло скептично відноситься до ідей електронної демократії: «Виникнення нових технологій інтерактивної комунікації телеконференції, системи опитування громадської думки, автоматизовані програми зворотного зв'язку, двостороннє кабельне телебачення і та інше), що дозволяють постійно консультуватися з громадськістю та проводити моментальні референдуми, не призвели до створення справжньої демократії» [132, с.12].

А. Бордюгова та В. Штанько, застерігають, що також існує загроза розділу суспільства на тих, хто володіє інформацією, і тих, хто не володіє нею (цифровий поділ), і, як наслідок, обмеження принципу демократії вибору.

Загрози пропаганди терористичних організацій, створення *електронних реєстрів* на громадян, відсутність чіткого захисту особистих даних в Інтернеті, поява ТНК можуть вести до того , «що вельми нешляхетні бізнесові магнати можуть зосередити в своїх руках величезну владу тим більше, що в багатьох державах світу поки ще не прийняті закони про свободу інформаці» [166, с.86].

У світлі таких міркувань міф про інформаційну нейтральність цифрового простору набуває дедалі більшої критики. Так, С. Балан, підкреслює, що «інформаційне суспільство» формується в «межах національних держав, які впроваджують відповідні політики і цим самим стимулюють розвиток досліджень, розробку й імплементацію технологій, а також їх функціонування» [2, с.157]. Тому, ідея про глобальну свободу слова, відкритість інформаційних потоків та демократичність віртуального середовища постає як ідеологічна конструкція, яка маскує фактичну наявність фільтрації, селекції та цензури. Ще одна загроза була описана В. Кудлай, яка стверджує, що : «різний доступ до інформаційно-комунікаційних технологій посилює соціальну стратифікацію різних прошарків населення у різних країнах світу» [62, с.41]. Через такий процесс соціальної стратифікація населення, несе прямі загрози різного розуміння, сприйняття та обробки інформації, яка надходить з електронних засобів комунікації. На думку О. Лозовицького , через персоналізацію політичних подій у користувачів ІКТ, значно знижується «здатність адекватного сприйняття інформації…», що також підкреслюється процесами «зрощення інтересів різних політичних груп з тими або іншими ЗМІ». [65, с.108]

Зокрема, йдеться про можливість цілеспрямованого блокування або обмеження та поширення соціально значущої політичної інформації, яка суперечить інтересам домінантних акторів – власників інтернет-платформ, керівників пошукових систем, адміністрацій соціальних мереж.

Таким чином, цифрова інфраструктура дедалі частіше використовується не як простір емансипації, а як механізм контролю та

управління публічним дискурсом. У результаті свобода інформації постає не як об’єктивно гарантоване право, а як умовна категорія, яка може бути суттєво обмежена або нівельована через вплив приватних корпорацій, що перебувають у тісній взаємодії з політичними елітами та силовими структурами.

Отже, аналіз концепцій інформаційного суспільства, сформованих зарубіжними вченими, такими як, Д. Беллом, Й. Масудою, Е. Тоффлером та М. Кастельсом та ін., а також вітчизняними вченими, такими як, С. Баланом, В. Кудлай, О. Лозовицьким, І. Милосредною та ін., окреслює складну та амбівалентну картину сучасних соціальних трансформацій. Складається таке розуміння, що з одного боку, ці теорії наголошують на потенціалі інформаційних технологій для розширення демократичної участі, розвитку інформаційного суспільства та формування нових форм соціальної взаємодії. З іншого – на практиці, виявляється зворотня тенденція: цифровізація все частіше використовується як інструмент централізованого контролю, масового стеження та маніпулювання поведінкою громадян. Поступова концентрація влади у руках державних структур і транснаціональних цифрових платформ призводить до делегітимації традиційних демократичних інститутів і формує підґрунтя для нового типу владних відносин — цифрового тоталітаризму.

Цей тип управління вирізняється прихованістю, алгоритмічністю та ефективністю контролю, що ґрунтується на збиранні, обробці та монетизації особистої інформації. Таким чином, концепції інформаційного суспільства не лише відкривають перспективу демократичного розвитку, але й виявляють структурні загрози, що постають у разі неконтрольованого впровадження цифрових технологій без належного нормативного регулювання та правового захисту прав людини.

1.3. Методологічні підходи дослідження процесів цифровізації влади та контролю

Питання методології дослідження цифровізації влади та контролю в контексті загроз демократії в інформаційному суспільстві з боку «цифрового тоталітаризму» є недостатньо дослідженим у сучасній політичній науці, адже вони стали предметом систематичних і поглиблених наукових пошуків лише обмеженого кола дослідників.

Як наслідок, в сучасній політологічній літературі можна спостерігати відносно низький ступінь теоретико-методологічної розробленості підходів, способів та основних принципів наукового пізнання явищ і процесів пов'язаних з цією проблематикою.

Наявний рівень наукового осмислення методології «цифровізації» та «контролю» істотно відстає від актуальних потреб сучасної практики та теорії, що проявляється у відсутності єдиних, чітко сформульованих методологічних концепцій, систематизованих наукових підходів та фундаментальних принципів аналізу актуальної проблеми. Вказана ситуація породжує низку проблем, які виражаються в недостатній узгодженості теоретичних і практичних аспектів політичної науки та негативно позначаються на ефективності вирішення сучасних глобальних проблем і правових конфліктів у міжнародній сфері.

Таким чином, стан методологічного забезпечення досліджень є незадовільним та потребує суттєвого вдосконалення й розвитку, що дозволить більш якісно вирішувати нові виклики сучасності. Головна проблема методології на наш погляд, є аксіологічною, через дихотомію процесу цифровізації влади та контролю.

З одного боку, цифровізація влади — є логічним рухом розвитку науково-технологічного прогресу, поєднання форм влади з технологіями, з другого боку – контроль за інформаційним суспільством має характер посилюючого, що невпино зростає разом із різноманітними формами спостереження та обмеження в правах та доступу до мережі Інтернет.

Визначаючи методологію дослідження наукової проблеми дисертаційної роботи, слід наголосити, що необхідною передумовою

дослідження особливостей прояву феномену цифрового тоталітаризму є, на нашу думку, концептуалізація загроз демократії в інформаційних суспільствах, яка сприймається дисертантом як процес осмислення, формулювання, систематизації характерних ознак визначенног феномену та виявлення його впливу на «розмивання» сутевих ознак демократії, її базових стандартів, зокрема порушення прав людини.

Стрімкий розвиток соціально-економічних процесів у світі дав поштовх до активного використання інформаційних та цифрових технологій, які є каталізаторами інноваційного розвитку в усіх сферах людського життя. Цифровізацією або діджиталізацією називають четвертою промисловою революцією. Цей процес швидко проник в кожен аспект життя суспільства і домінує в будь-якій сфері, неминуче трансформуючи суспільство. Цифровізація економіки характеризується технологічними проривами в сферах: нанотехнологій, квантових обчислень, штучного інтелекту і біотехнологій. Цифровізація та діджиталізація трансформувала економічні відносини, тобто надання послуг, продаж товарів і традиційне виробництво.

Крім того, виникнення цифрових технологій сприяло розвитку і поширенню нових форм організації праці, економічної ефективності, бізнесу та уряду. Незважаючи на перспективи, що постійно розширюються, діджиталізація може нести в собі загрози, оскільки вона є недослідженою концепцією з погляду змін на глобальному ринку праці. Іншими словами, діджиталізація впливає на процеси, які здешевлюють надання виробництва та продаж послуг, виробництва і продаж товарів та підвищення кваліфікації працівників. Одним із наслідків цифровізаційних процесів є підвищення рівня життя в суспільстві.

Тобто, цифрова трансформація – це неминучий процес, що відбувається в усьому світі. Високотехнологічні досягнення впроваджуються в наше життя безперервно. З розвитком технологій з’являється все більше пристроїв, так званих «ґаджетів», без яких сучасне

людство не уявляє своє життя. Термін «цифровізація» широко використовується в сучасних дослідженнях, але конкретне тлумачення цієї дефініції є предметом численних наукових дискусій.

Детальні дослідження особливостей процесів цифровізації економічних систем розглядаються в роботах С. Берна, Ж. Клерека [199], А. Мюррея [261], Ю. Рімана, Т. Окса [249], Ф. Скуотто [261] та ін.. Окремим аспектам цифровізації присвячені роботи У.Хуса, який досліджував вплив цифровізації на ринки праці та форми організації праці; Р. Аткінсона, який вивчав взаємозв'язок між інноваціями та інформаційними технологіями; С. Холройда, який детально розглядав взаємодію між глобалізацією та цифровізацією [3, с.190].

Розвиток сучасної теорії цифровізації підтримали такі вітчизняні вчені, як І. Дульська [33], А. Гуренко [26], С. Коляденко [51], В. Коренівська [56], О. Криворучко [58], В. Ляшенко [67], Н. Мешко [72], Г. Соколова [132] та інші.

Для комплексного розуміння понять «цифровізація» та «цифрова трансформація» значний внесок зробили С. Бреннан, Д. Крейс [175], Ю. Нікітін [80], Г. Ткачук [148],. Їхні напрацювання можуть бути покладені в основу визначення поняття цифрової трансформації. Серед сучасних вітчизняних дослідників можна виділити, О. Гудзь [25], В. Ляшенко [67]. Цифрова трансформація вченими зазвичай розглядається як сукупність сучасних інструментів та процесів, що допомагають розв'язувати низку проблем та задовольняти потреби клієнтів

Науковці С. Бреннен та Д. Крейс трактують діджиталізацію як прийняття або збільшення використання цифрових і комп'ютерних технологій, як спосіб перебудови багатьох сфер соціального життя навколо цифрових комунікацій та медіа інфраструктури. Зокрема С. Бреннен, давав визначення поняттю «цифровізація». Він наголошував, що це – процес з оцифрування, перетворення аналогових даних у цифрову форму [175]. Ж. Клерек визначив процес цифровізації як виробництво цифрової версії

аналога. Іншими словами, цифровізація – це перетворення нецифрових об'єктів у цифрову форму, щоб комп'ютерні системи можна було використовувати для досягнення різних цілей. На думку науковця, цифровізація – це «використання цифрових технологій і даних для отримання прибутку» [199]. На думку дослідника Дж. Вестермана, цифрова трансформація знаменує собою радикальне переосмислення того, як використовуються технології для людей та супутніх процесів.

Вагомий внесок у розуміння цифровізації зробили американські вчені, які запропонували концепцію цифрової економіки як нової формації та розвитку економічних відносин у суспільстві. Першими вченими, які активно досліджували особливості формування цифрової економіки в суспільстві, були Д. Тапскотт, А. Тапскотт, П. Самуельсон, Б. Налебуфф. Так, Д. Тапскотт розглядав поняття «цифровізація», як «епоху мережевого інтелекту», сутність якої «не тільки в мережевих технологіях ... але й у взаємодії людей за допомогою мережевих технологій», як «об'єкт, що поєднує інтелект, знання і творчість для здійснення прориву у створенні суспільного капіталу і благополуччя» [51]. Дослідник С. Криниця вважає, що цифровізація необхідна для оптимізації бізнесу зосереджуючись на «стандартизації та гармонізації «електронної комерції, фінансових ринків та платіжних систем у глобальному вимірі як основи розвитку конкуренції та зниження витрат», а також «на знятті бар'єрів на шляху цифровізації, коригуванні вад і провалів ринку, підтримці конкуренції, залученні інвестицій тощо» [60, с.55]. Він також зазначає, що цифровізація має стати пріоритетом у процесах державної промислової політики задля подолання «провалів» та «нерівностей» у процесах побудови цифрової економіки [60, с. 50].

Автор наукового дослідження «Цифрова економіка: передумови та етапи становлення в Україні та світі» С. Коляденко визначає цифровізацію як спосіб приведення різноманітної інформації до цифрової форми [51, с.107]. Схоже визначення можна знайти в монографії Н. Мешко «Стратегії

високотехнологічного розвитку в умовах глобалізації: національний та корпоративний аспекти», де автор визначає цифровізацію як процес, пов'язаний з тенденцією до оцифрування різних видів інформації [72]. У своїх дослідженнях Г. Соколова цифровізацію характеризує як створення цифрової (заснованої на байтах та бітах – мінімально адресованих одиницях інформації) версії аналогових речей на паперових документах, відео- та фотозображень, звуків [132, с.94].

Дослідник Ю. Нікітін цифрову трансформацію означав як процес переходу до нових способів діяльності шляхом впровадження цифрових технологій та цифрових сервісів, що базується на стратегічному партнерстві всіх зацікавлених сторін та одночасної розробки програмного забезпечення, цифрової трансформації та оцінки рівня цифрової трансформації [80, с.82].

На прикладі розвинених країн світу, які першими почали впроваджувати цифровізацію, науковці Т. Поснова, Г. Карчева, С. Веретюк, С. Коляденко, В. Апалькова, досліджуючи цифрову економіку з різних аспектів, деталізували її структурні компоненти та виявили чинники активізації розвитку. Науковці Н. Краус, Г. Карчева розкрили практичні аспекти реалізації можливостей цифрової економіки, навели приклади її функціонування за сучасних умов світового інформаційного простору [130, с.49].

У своїх наукових дослідженнях вітчизняні та зарубіжні вчені акцентують увагу на тому, що як світова, так і національні економіки зазнають масштабної трансформації внаслідок стрімкої еволюції та зростаючого використання інформаційно-комунікаційних і комп'ютерних технологій. Ці технології стають визначальними рушіями розвитку, оскільки сприяють глобалізації економічних процесів, інтеграції ринків та впровадженню нових підходів до організації виробництва, торгівлі, управління та комунікації.

Стрімке розширення цифрових можливостей та глибока діджиталізація сучасного суспільства відбуваються завдяки

всеохоплюючому збору, детальному аналізу та ефективному використанню різноманітної інформації. Одним із ключових механізмів цього процесу є збирання та обробка так званих «цифрових слідів» — сукупності даних, що залишаються в результаті діяльності користувачів у цифровому середовищі. Така інформація охоплює не лише особисті дані, поведінкові психологічні патерни та уподобання, а й детальні характеристики соціальних, економічних, культурних та політичних процесів в яких перебувають громадяни, суспільства та держави.

Аналіз цифрових слідів, здійснюваний за допомогою штучного інтелекту, технологій великих даних (Big Data) та алгоритмів машинного навчання, відкриває широкі перспективи для оптимізації різних сфер суспільного життя. Впровадження аналітичних цифрових інструментів дозволяє прогнозувати економічні тренди, покращувати ефективність управління державними процесами, удосконалювати фінансові системи та створювати нові бізнес-моделі.

Однак водночас активне проникнення цифрових технологій у всі сфери життєдіяльності суспільства породжує низку викликів і ризиків, пов’язаних із питаннями захисту персональних даних, приватності, інформаційної безпеки та етичності використання інформаційних ресурсів.

Таким чином, цифрова трансформація не лише змінює економічні та соціальні парадигми, а й формує нові виклики, які потребують комплексного дослідження, розробки відповідних законодавчих механізмів та адаптації існуючих правових норм до реалій цифрового суспільства. З іншого боку, в рамках цифровізації, активно вивчається питання контролю, як методу феномену «цифрового тоталітаризму».

Політичний контроль як метод або об'єкт наукового дослідження є однією з ключових категорій у політичній науці, особливо в контексті досліджень влади, легітимності, авторитаризму, тоталітаризму та новітніх цифрових технологій. В рамках державного функціонування та управління «к*онтроль* є неодмінним атрибутом суспільних відносин та функціонування

соціальних систем». Так, українська дослідниця Е.Мамонтова стверджує, що «*контроль* полягає у здатності інститутів влади стежити за виконанням їх розпоряджень», а політичне управління та керівництво працюють «через прийняття стратегічних і тактичних рішень до об'єктів влади, через організацію, регулювання та контроль їх розвитку»[68].

Карл Фрідріх та Збігнев Бжезінський у відомій роботі «Totalitarian Dictatorship and Autocracy» описуючи «тоталітаризм», акцентували на моделі «тоталітарного контролю», який реалізується через «монополію партії, ідеологію, контроль над ЗМІ, терором, контролем над економікою і монополією на насильство»[219].

Завдяки процесу *цифровізації влади* – контроль стає «фундаментальним» елементом такого процесу. Вивчення контролю через призму технологізації та цифровізації влади порушувало велика кількість світових та вітчизняних вчених.

Фукоянська концепція «політичного контролю» була прописана у творі «Наглядати і карати»[214], завдяки Паноптикопічній моделі влади – контроль здійснюється на усіх етапах існування владних стосунків. Завдяки цифровізації влади, цифрові методи контролю виводять методи Фуконяьскої концепції у нову цифрову реальність, роблячи Паноптикон – цифровим по сутності та природі. В свою чергу, Цифровий Паноптикон – «всеохоплююча та всепронизуюча систему спостереження за цифровим суспільством із використанням центричної системи споглядання та *контролем*» [134].

Жиль Дельоз описуючи процес цифровізації влади, переводить думку у всебічний контроль та спостереження серед акторів соціально-політичних відносин «замість того, щоб просто нормалізуватися, суб'єкти спостереження втягуються в «машину» *контролю*, якою є спостереження як управління» [201]. Славой Жижек торкається питання *контролю*, як механізму забезпечення та функціонування інформаційних суспільств в цифрових мережах [281]. Шошана Зубофф у власній статті «Великий інший:

Капіталізм спостереження та перспективи інформаційної цивілізації» описує *контроль*, як метод прояву «Інформаційного капіталізму», який має на меті передбачати та змінювати людську поведінку [282].

Узагальнення теоретичних підходів до вивчення політичного контролю як ключової складової функціонування сучасної влади, зокрема в умовах цифрової трансформації, окреслює важливість комплексного наукового підходу до цього явища та підводить до наступного висновку. Розмаїття форм контролю – від класичних адміністративно-силових механізмів до алгоритмічного нагляду та поведінкової інженерії — вимагає не лише концептуальної ясності, а й ретельного міждисциплінарного аналізу. Саме тому для належного осмислення феномену цифрового тоталітаризму як нового етапу у розвитку політичного контролю необхідно залучити широке коло методологічних інструментів, що дозволяють охопити як історичний, розвиток поняття, так і його сучасні прояви. Очевидно, що методологія подібного дослідження має передбачати:

1) *Використання історичного та компаративного методу аналізу,* котрі дозволили прослідити процес формування та розвиток феномену «цифрового тоталітаризму» , як версії «тоталітаризму» загрози демократії в інформаційних суспільствах в низці країн, які стикаються з активною дихотомією впилву цифрових технологій.

Наприклад, порівнюючи загрози «інформаційному суспільству» та феномену «цифрового тоталітаризму» важливим постає сам аналіз епохи поширення та розвитку інформаційних технологій. Значимим є порівняльний аналіз прогностичних ідей та теорій Елвіна Тоффлера [270], Мішеля Кастельса [191], Йонеджі Масуда [70], Юваля Харарі [251] на рахунок утворення нових форм «демократії», цифрових форм врядування та загрозам існуючому світовому порядку. Об’єктами *компаративного аналізу* стають національні емпіричні практики та програми щодо забезпечення інформаційної політики, систем контролю та спостереження країн, які активно використовують надбання ІКТ в інформаційній політиці.

2) з*астосування методів порівняльного аналізу та методу аналогії,* які дозволили на прикладі аналізу застосування ІКТ проаналізувати в політичній сфері найбільш високо розвинених країн світу (США, КНР, Німеччина, Франція, Канада, Велика Британія та ін.), а також проаналізувати існуючи результати впровадження інформаційно-комунікаційих технологій в політиці менш розвинених країн світу (в т.ч. України).

3) *методи дедукції та індукції, дескрипції, абстрагування та моделювання,* дозволили дослідити феномен цифрового тоталіатризму в контексті дихотомії систем розвитку та впровадження цифрових технологій та формування культури масового спостереження, контролю із суттєвими порушенням конфіденційності.

4) *дескриптивний метод* дозволив описати характерні ознаки цифрового тоталітаризму, як феномену, а методи абстрагування та моделювання дозволяють аналізувати процеси загроз демократії в інформаційному суспільстві, як глобальній проблемі в умовах некотрольованого технологічного прогресу кіберпростору.

4) *інституційний та структурно-функціональний методи аналізу*, дозволили проаналізувати процес формування та інституалізації систем загроз демократії та інформаційних суспільств.

5) культурологічнмй підхід доцільно продиктований у зв'язку з тим, що на міжнародному рівні встановлюються певні однакові системи реакцій та поведінки суб'єктів та об'єктів міжнародних відносин, різних правових культур та держав, що мешкають не тільки на території різних країн, а й континентів. Міжнародний політичний простір складається з різних країн, що в рамках ООН стають більш-менш рівноправними учасниками створення та розвитку систем міжнародних правових актів та рекомендацій. Культурологічний підхід важливий при вивченні спадковості в методах та формах режимів, які можуть представляти різні елементи народної культури та традицій, утворюючи своєрідну колективну меморіальну пам'ять

суспільств, що різні ставлення до тих чи інших правових регламентацій, законів на нормативно-правових актів.

6) цивілізаційний підхід доцільно використаний у якості провідного методологічного інструменту дослідження – орієнтований на визнання політичної різнобарвності та забезпеченості в якості основи та фундаментальної різниці у формах та ступенях розвитку сучасних систем захисту та методам реакцій на формування цифрових тоталітарних технологій та режимів.

7) історичний метод дозволив визначати орієнтири, в науковому доробку, які демонструють яким чином сучасні політичні системи складаються по відношенню до цифрових загроз, технологій та режимів і яким чином вони розвиваються з часом.

Методологія дослідження феномену цифрового тоталітаризму, як загрози демократії в інформаційному суспільстві та світі включає в себе різноманітні підходи та методи, які допомагають розуміти історію та сучасні тенденції в цій галузі.

Аналіз сучасного стану методологічного забезпечення дослідження цифровізації влади та контролю виявляє суттєвий дефіцит теоретико-методологічної узгодженості в політологічній науці. Попри стрімкий розвиток цифрових технологій та їх активне проникнення в усі сфери суспільного життя, наукове осмислення цих процесів, зокрема в контексті формування новітніх загроз демократії, залишається фрагментарним і недостатньо систематизованим. Поняття цифровізації, цифрової трансформації, а також політичного контролю набувають дедалі складнішого змістовного наповнення, що вимагає міждисциплінарного підходу, здатного поєднати інструменти політичної теорії, правознавства, соціології, філософії, інформаційних технологій та міжнародних відносин.

Запропонована в роботі методологія дослідження ґрунтується на поєднанні загальнонаукових, компаративних, інституційних, культурологічних, цивілізаційних та критичних підходів, що дозволяє

комплексно дослідити феномен цифрового тоталітаризму як сучасну форму соціотехнічного впливу. Особливу увагу зосереджено на аксіологічному аспекті, який розкриває дихотомію цифровізації влади: між легітимним прагненням до ефективного управління і латентною загрозою посилення інструментів нагляду, контролю та обмеження прав і свобод людини.

Цифрова трансформація виступає не лише як чинник модернізації політичної влади, а й як потенційне джерело політичного ризику, зумовленого можливою концентрацією владних повноважень у руках акторів, що мають доступ до масивів персоналізованих даних та алгоритмічних механізмів впливу на громадську свідомість. В таких умовах методологія дослідження повинна не лише фіксувати емпіричні прояви контролю, а й критично осмислювати його нормативні, правові та ціннісні засади.

Важливим завданням є не просто опис трансформацій, а виявлення механізмів, що можуть призвести до ерозії демократичних інститутів, легітимації авторитарних практик у цифровому середовищі та закріплення нових форм нерівності у доступі до інформації, участі в управлінні й контролі над інформаційною інфраструктурою.

Таким чином, актуальність і складність дослідження цифрового тоталітаризму обумовлює необхідність переосмислення методологічних підходів у сучасній політичній науці. Формування системної методології, що враховує динаміку технологічного розвитку та зростаючу взаємозалежність між інформаційною сферою та політикою, є ключовим кроком до глибшого розуміння і протидії загрозам, які постають перед демократичними суспільствами в умовах нової цифрової реальності.

Висновки до першого розділу. Узагальнюючи результати аналізу класичних концепцій тоталітаризму, теорій інформаційного суспільства та сучасних підходів до дослідження цифровізації влади й контролю, можна зробити висновок, що цифровий тоталітаризм формується як особливий тип політичного режиму, у якому поєднуються елементи традиційної політичної

репресії з інноваційними соціотехнічними засобами впливу. Якщо класичний тоталітаризм функціонував переважно через відкриту політичну репресію, ідеологічну монополію та силове примушення, то цифровий тоталітаризм здійснює контроль приховано — через алгоритми, масовий збір і обробку даних, соціальне профілювання, керування інформаційними потоками та моделювання публічного дискурсу.

У цьому контексті концепції інформаційного суспільства, попри свій прогресивний і демократичний потенціал, виявляються двозначними: цифрові технології, з одного боку, розширюють можливості для участі громадян у прийнятті рішень, з іншого — створюють передумови для централізованого нагляду, маніпуляцій та порушення базових прав і свобод. Поступова делегітимація традиційних демократичних інститутів унаслідок концентрації цифрової влади в руках держав і транснаціональних платформ зумовлює необхідність глибокого переосмислення нормативних засад функціонування демократії в нових умовах.

Сучасне політологічне знання ще не сформувало цілісної методології для вивчення цього феномену. Виявлений дефіцит міждисциплінарної узгодженості та концептуальної чіткості свідчить про необхідність розробки комплексного підходу до аналізу цифрового тоталітаризму, що враховує не лише технологічні аспекти, а й аксіологічні, правові, культурні й цивілізаційні виміри. У цьому процесі ключовою є критична рефлексія над тим, як цифрові технології впливають на природу влади, легітимність політичних режимів і майбутнє демократичних інституцій.

Отже, цифровий тоталітаризм не є лише гіпотетичним сценарієм майбутнього, а вже тепер постає як реальна й багатоаспектна загроза, яка потребує належної наукової уваги, нормативного регулювання та інституційної відповіді з боку демократичної спільноти.

РОЗДІЛ 2
ІНСТРУМЕНТИ ТА ЗАГРОЗИ ЦИФРОВОГО ТОТАЛІТАРИЗМУ

2.1. Технологія масового спостереження як інструмент політичного управління

Необхідність створення умов захисту людини в контексті використання її персональних даних іншими людьми та суб’єктами влади з політико-правового погляду досліджувалася та визначалася протягом значного історичного часу. Це пов’язано з поступовим і доволі тривалим становленням конституційних прав людини та спрямованості на формування правових засад недоторканності приватного життя. Важливим, при цьому, є те, що особиста свобода невід’ємна від небезпеки. І справа з обмеження свободи, з одного боку, є справою зміцнення безпеки людини, а з іншого — визначається потребами національної безпеки держави.

У сучасному суспільстві культура масового спостереження поступово перетворилася на важливий та невід'ємний елемент нашої повсякденної дійсності. Значний технологічний прогрес останніх десятиліть, а саме стрімкий розвиток мережевих інформаційних технологій, широке впровадження камер відеоспостереження у громадських просторах, а також поширення соціальних медіа-платформ як засобів комунікації, створив принципово нові можливості для фіксації, зберігання, аналізу та швидкого обміну великими обсягами інформації. Внаслідок цього з'явилися суттєві трансформації у ставленні суспільства до фундаментальних понять, таких як право особи на конфіденційність та приватність. Якщо раніше ці права вважалися абсолютними і такими, що не можуть бути порушеними без поважних причин, то сьогодні суспільство поступово звикає до постійної присутності різноманітних форм спостереження.

Цей процес провокує дискусії про необхідність пошуку балансу між забезпеченням безпеки та збереженням індивідуальної свободи і приватного

життя, а також стимулює перегляд традиційних правових норм та етичних стандартів у сфері захисту персональних даних.

Цифровізація, як провідний елемент сучасного розвитку людства, торкається усіх сфер життя суспільства. «Як тренд розвитку світової економіки і суспільства, цифровізація по-різному впливає на різні сфери. А від ступеня впливу цифровізації на національне, економічне та соціальне життя залежить місце кожної країни у світовому співтоваристві» [30, с.99].

Термін «privacy» використовують у законодавстві США, англомовних країнах, публічних виданнях Європи, і еквівалентний словосполученню «недоторканність особистого життя». «Цей термін запозиченний з латинської мови «privaus» – «приватний», «особистий» та трактується як: особистість, інтимність, таємність, самітність, власність, міжособисті відносини» [12, с. 33].

У сучасному науковому та юридичному дискурсі до сьогодні не сформувалося єдиного, чітко узгодженого трактування чи юридичного визначення поняття «privacy». Це зумовлює наявність значної кількості різноманітних інтерпретацій і дефініцій цього терміну. Серед найбільш поширених його визначень зустрічаються такі варіанти, як: «особисте життя», «право на приватне життя», «недоторканність приватного життя», «право на самоту» [12, с. 34].

За цитатою, авторів В. Брижко та В. Пилипчука зазначається, що : Зокрема, у авторитетному українському довідковому виданні «Юридична енциклопедія» поняття «privacy» (транскрибоване українською як «прайвесі») інтерпретується як «приватна справа, таємниця, усамітненість» [12, с. 34]. Відзначається, що це особлива правова категорія, яка сформувалася в англо-саксонській правовій традиції та безпосередньо пов'язана із захистом інтимної сфери життя людини.

Натомість «Великий юридичний словник» пропонує ще більш широке та варіативне тлумачення цього терміну, визначаючи «privacy» як «таємницю, самоту, приватне життя» [12, с. 34]. Автори словника

підкреслюють, що дана категорія має особливий юридичний характер і передбачає захист особистого простору та інтимного життя людини від втручання з боку третіх осіб. При цьому вказується, що термін може бути застосований для позначення різних понять: в одних випадках він означає безпосередньо приватне життя людини, в інших – право особи на це приватне життя, а у третіх – право на захист і забезпечення недоторканності приватної сфери.

У 1990 році, у Звіті Комітету Британії по конфіденційності та суміжних питань, було зазначено, що за результатами проведених досліджень трактувань “privacy” в рамках різних епох, культур та політичних систем «ніде не знайдено абсолютно прийнятного правового визначення цього поняття» [12, с. 34].

Історично приватність не відігравала провідної ролі у житті людей, оскільки практичні потреби виживання та забезпечення безпеки часто переважали над особистим бажанням усамітнення. Цікаво також, що у класичній латинській мові епохи Середньовіччя відсутній прямий еквівалент сучасного поняття «приватність». Найближчим терміном було «privatio», значення якого полягало у позбавленні чогось або у віднятті.

Одним із найпопулярніших і поширених у сучасній науковій і юридичній практиці тлумачень поняття «privacy» є трактування приватності як «права бути наданим самому собі». Згідно з цим визначенням, кожна людина повинна володіти гарантованим правом на свій власний особистий простір, який є захищеним від несанкціонованих втручань, довільних зазіхань чи втручань із боку третіх осіб.

Очевидно, що конфіденційність даних є невід'ємною та обов'язковою умовою для будь-якої організації, підприємства або фізичної особи, які збирають, обробляють або використовують особисті дані чи будь-яку іншу приватну інформацію. Незважаючи на це, більшість сучасних компаній і надалі не приділяють достатньо уваги та ресурсів своїм програмам з

забезпечення конфіденційності, що призводить до систематичного невиконання ними своїх зобов'язань щодо захисту персональних даних.

В умовах цифрової епохи виникає нагальна необхідність переосмислення та уточнення самої концепції приватності, що неодмінно передбачає одночасне врахування як описового, так і нормативного вимірів цього поняття. У теоретичному плані ці два аспекти конфіденційності є досить чітко розмежованими. Перший, описовий вимір, стосується оцінки та аналізу рівня приватності, що фактично має місце в суспільстві, не висловлюючи при цьому конкретних нормативних суджень щодо бажаного чи оптимального ступеня приватності.

Другий, нормативний вимір, натомість концентрується на обґрунтуванні причин, чому саме приватність є необхідною умовою повноцінного, гідного життя людини. Втім, зазначена відмінність між цими двома аспектами не повинна приховувати важливий факт, що саме поняття конфіденційності не є нейтральним; воно завжди має певну позитивну конотацію та асоціюється із захистом чогось цінного і значущого.

Так, наприклад, втручання або вторгнення в приватну сферу життя людини завжди розглядається як порушення фундаментальних прав особистості, яке потребує активного запобігання та захисту. Водночас теоретичні дискусії навколо концепції приватності порушують питання щодо сутнісних підстав її збереження та захисту, змушуючи суспільство замислитися над тим, чому саме приватність необхідна для існування та розвитку особистості.

З іншого боку, цифровізація сьогодні постає беззаперечним рушієм розвитку сучасного суспільства та всіх його складових. Цей процес відкриває величезні можливості для економічного зростання, створення нових робочих місць, розвитку ринку праці та підвищення ефективності економіки в цілому. Поширеною аксіомою стало твердження про те, що інвестиції в цифрові активи забезпечують значно вищий рівень прибутковості порівняно з інвестиціями у традиційні, нецифрові сектори

економіки. Крім того, саме сектори, пов’язані з цифровими технологіями, демонструють суттєво більший приріст робочих місць та рівень зайнятості, ніж це спостерігається у світовій економіці загалом.

«Про «право бути наданим самому собі» вперше заговорили з 15 грудня 1890 року, коли американські юристи Луїс Брендейс і Семюель Воррен опублікували в юридичному журналі Гарварда «Harvard Law Review» статтю «Право на приватність». Вони писали, зокрема, що: «Інтенсивність і складність життя, пов’язані з розвитком цивілізації, сформували необхідність у самоті, і люди, під впливом культури, стали більш чутливими до публічності, через що самота й конфіденційність стали більш важливими для індивідуума; але сучасні підприємства й винаходи, вторгаючись в особисте життя людини, піддають його щиросердечному болю й стражданням, набагато більшим, ніж могли б заподіяти йому тілесні ушкодження» [12, с. 34].

У сучасному контексті, коли культура масового спостереження стала повсякденною нормою, висновки американських юристів набувають особливої гостроти й актуальності. Сучасні технології, такі як соціальні мережі, камери спостереження та цифрові платформи, стали інструментами не лише покращення комунікації чи безпеки, але й посиленням контролю над приватним життям громадян.

Саме через це межі між публічною та приватною сферами дедалі більше стираються, що неминуче спричиняє «щиросердечний біль і страждання», про які попереджали Брендейс і Воррен.

Ця ситуація актуалізує необхідність переосмислення меж втручання держави та корпорацій у приватність індивіда, створення нових, більш ефективних механізмів захисту конфіденційності, а також стимулює суспільну дискусію про те, як знайти баланс між правом людини на приватність і суспільною потребою в безпеці та доступі до інформації.

Відтак, на тлі культури масового спостереження, цінності, сформульовані понад століття тому, не лише залишаються актуальними, але

й стають критично важливими для розуміння й вирішення сучасних викликів цифрової епохи.

Далі, вже у 1928 р. суддя та член Верховного суду США Луїс Брендейс, стверджував : … «що право на недоторканність приватного життя не можна ставити у залежність від способу, яким здійснюється отримання інформації про людину» [12, с.34].

Особливу увагу необхідно звернути на те, що сутність права людини на конфіденційність спілкування полягає не стільки у специфічних технічних чи технологічних способах збору інформації (таких, наприклад, як приховане знімання чи прослуховування), скільки у принциповому положенні, що кожен індивід має право очікувати та розраховувати на таємницю свого приватного спілкування.

Варто підкреслити, що ця ідея була сформульована та обговорювалася в ті історичні часи, коли поняття на кшталт «інформатизація», «телекомунікації», «Інтернет», «штучний інтелект» та інших технологічних новацій, які визначають сучасний інформаційний простір, ще навіть не виникли. Тоді дискусії зосереджувалися винятково на питаннях «особистої недоторканності» людини в її традиційній, «не віртуальній» життєдіяльності.

Зокрема, видатний американський правознавець Луїс Брендейс, який по праву вважається одним із засновників сучасного поняття права на приватність, безперечно, випереджав свій час.

Незважаючи на прогресивність та далекоглядність його ідей, висловлених у статті «Право на приватність», на момент публікації цей матеріал не набув значного суспільного резонансу чи широкої популярності серед загалу. Публікації та обговорення, що з'являлися тоді в засобах масової інформації, не отримали широкого поширення й не викликали особливого інтересу громадськості.

Втім, сьогодні ці погляди, викладені понад століття тому, набули нового значення та актуальності, враховуючи нинішній рівень розвитку

інформаційних і цифрових технологій, які зробили право на конфіденційність одним із фундаментальних викликів сучасності.

Так, на думку В. Брижко та В. Пилипчуку, термін «privacy» – «це право на недоторканність приватного життя, тобто «право на себе», що спрямовано на можливість людини «бути залишеною у спокої» [12, с.35].

Сьогодні, у контексті стрімкого розвитку цифрових технологій та активного поширення цифрових форм комунікації, поняття «приватність» набуває особливого значення, стаючи однією з ключових правових категорій міжнародного права, що гарантує захист особистого життя людини від втручання державних або інших суб'єктів. У міжнародно-правовій сфері це право закріплене у низці фундаментальних нормативно-правових актів.

Так, право людини на повагу до приватного життя, захист від необґрунтованого втручання та забезпечення особистої недоторканності закріплене у статті 12 *Загальної декларації прав людини* від (1948) року, яка наголошує, що «ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканість його житла, таємницю його кореспонденції або на його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань» [38].

Крім цього, важливими нормативно-правовими документами у сфері захисту приватності особи є Європейська *Конвенція з прав людини та основоположних свобод* 1950 року, яка у статті 8 визначає :

«Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції» [52], а у статті 12:

«гарантує право на укладення шлюбу та заснування сім'ї, що також пов'язано із широким розумінням приватності як фундаментальної цінності європейського правового простору» [52].

Окрім цього, в умовах сучасних європейських інтеграційних процесів важливим документом, який забезпечує захист приватності громадян

Європейського Союзу, є Хартія основних прав Європейського Союзу 2000 року, яка містить цілу низку статей, що стосуються цього питання.

Зокрема, Стаття 6. *Право на свободу та безпеку*. Кожна людина має право на особисту свободу та безпеку.

Стаття 7. *Повага до приватного та сімейного життя*. Кожна людина має право на повагу до його приватного та сімейного життя, його житла та його спілкування.

Стаття 8. *Захист персональних даних*. 1. Кожна людина має право на захист персональних даних щодо неї.

2. Такі дані мають використовуватися належним чином для визначених цілей та на підставі згоди такої людини або інших обґрунтованих підставах, встановлених законом. Кожна людина має право на доступ до даних, зібраних щодо неї, та право на виправлення в них помилок.

3. Дотримання цих правил підлягає контролю з боку незалежного державного органу» [154].

Стаття 11. *Свобода вираження поглядів та свобода інформації.*

1.Кожна людина має право на вираження своїх поглядів.

Це право включає свободу дотримуватися своїх поглядів, отримувати та розповсюджувати інформацію та ідеї без будь-якого втручання державних органів та незалежно від державних кордонів.

2. Дотримуються свобода та плюралізм засобів масової інформації [154].

Ця стаття також тісно пов'язана з правом на «приватність», оскільки забезпечує можливість вільно висловлювати думки без ризику незаконного втручання. Водночас варто зазначити, що сучасна міжнародна практика демонструє постійну динаміку у розширенні трактування цього права з огляду на появу нових цифрових технологій, що збільшують можливості для втручання у приватне життя громадян.

Саме тому Європейський Суд з прав людини через прецедентну практику постійно уточнює межі застосування окремих положень Конвенції та Хартії, що допомагає забезпечити адекватний рівень захисту приватності у світлі нових викликів цифрової епохи. В умовах цифровізації сучасного суспільства такі уточнення дозволяють адаптувати традиційні правові механізми захисту приватності до нових реалій цифрового середовища, тим самим гарантувавши ефективне функціонування базових прав людини.

Європейський суд з прав людини (ЄСПЛ) у своїй практиці з 1992 року розглянув низку справ, які стосувалися різних аспектів права на приватне життя, закріпленого в статті 8 Європейської конвенції з прав людини. Нижче наведено приклади таких справ із відповідними посиланнями на рішення Суду:

1) Справа «К.Б. проти Франції» (B. v. France): розглядалася зміна статі та внесення відповідних виправлень в акти цивільного стану [177].

2) Справа «Мікуліч проти Хорватії» (Mikulic v. Croatia): заявниця прагнула встановити батьківство та доступ до інформації про своє походження [187].

3) Справа «Йоссіфова проти Болгарії» (Yossefova v. Bulgaria): стосувалася можливості заперечування батьківства [189].

4) Справа «Янкович проти Хорватії» (Jankovic v. Croatia): заявник скаржився на примусове психіатричне лікування [181].

5) Справа «Гласс проти Великої Британії» (Glass v. the United Kingdom): стосувалася медичних втручань без згоди пацієнта [186].

6) Справа «Лопес Отін та інші проти Іспанії» (Lopez Ostra v. Spain): розглядалися екологічні права та вплив забруднення на приватне життя [183].

7) Справа «фон Ганновер проти Німеччини» (von Hannover v. Germany): стосувалася публікації фотографій приватного життя відомої особи [190].

8) Справа «Ротару проти Румунії» (Rotaru v. Romania): заявник скаржився на зберігання та використання його особистої інформації спецслужбами [185].

9) Справа «Амманн проти Швейцарії» (Amann v. Switzerland): стосувалася спостереження та зберігання даних про приватні телефонні розмови [176].

10) Справа «Гаскель та інші проти Сполученого Королівства» (Gaskin v. the United Kingdom): заявник прагнув отримати доступ до своїх дитячих соціальних записів [180].

11) Справа «Одієр проти Франції» (Odièvre v. France): стосувалася права на доступ до інформації про біологічних батьків [184].

12) Справа «Даджен проти Сполученого Королівства» (Dudgeon v. the United Kingdom): заявник оскаржував криміналізацію гомосексуальних відносин [179].

13) Справа «Ласкі, Джагард і Браун проти Сполученого Королівства» (Laskey, Jaggard and Brown v. the United Kingdom): стосувалася садомазохістських практик за згодою [182].

14) Справа «Німітц проти Німеччини» (Niemietz v. Germany): розглядалася межа між професійним та приватним життям у контексті обшуку офісу адвоката [188].

15) Справа «Копланд проти Сполученого Королівства» (Copland v. the United Kingdom): заявниця скаржилася на моніторинг її телефонних дзвінків та електронної пошти на робочому місці [178].

Ці справи ілюструють широкий спектр питань, пов'язаних із правом на приватне життя, які розглядав ЄСПЛ, та підкреслюють важливість захисту цього права в різних аспектах людського життя.

Європейський суд з прав людини (ЄСПЛ) у своїй практиці неодноразово розглядав питання щодо недоторканності особистої *кореспонденції* відповідно до статті 8. Європейської конвенції з прав людини та основоположних свобод 1950 року.

Одним із ключових рішень у цій сфері є справа «Класс та інші проти Німеччини» (Klass and Others v. Germany), рішення у якій було ухвалене 6 вересня 1978 року [238].

Розглядаючи справу, суд надав коментар стверджуючі, що «законні інтереси, які можуть виправдати втручання в приватне життя, вичерпно перераховані у другій частині статті 8. Боротьба з тероризмом незмінно розглядається Судом в розумінні цього положення як законна мета, оскільки вона підпадає під категорію захисту національної безпеки та охорони громадського порядку» [238].

Рішення Європейського Суду з прав людини у справі «Класс та інші проти Німеччини» демонструє глибоку напругу між прагненням держави до забезпечення національної безпеки й потребою захисту фундаментальних прав людини на приватність та конфіденційність комунікацій. Це рішення є особливо важливим у сучасному світі, коли культура масового спостереження набуває все більшого поширення та інтегрується в повсякденне життя громадян.

Якщо у 1970-х роках йшлося здебільшого про обмежене стеження з боку державних спецслужб, то сьогодні масштаби такого нагляду значно ширші: йдеться вже про автоматизований збір і аналіз персональних даних, використання штучного інтелекту для профілювання особистості та прогнозування поведінки, що може натякати на керовані процесі соціально-культурної інженерії.

За думкою, В. Брижко та В. Пилипчук, щоб перехоплення не було порушенням, воно має здійснюватися :

1. «На підставі закону». Будь-яке спостереження має проводитися згідно національного закону, що має задовольняти наступні вимоги: доступність – громадянин повинен мати можливість переконатися, що прослуховування відповідає нормам закону; передбачуваність – громадянин повинен бути здатний (при необхідності за допомогою адвоката)

передбачити наслідки будь-якої можливої дії; якість – закон повинен мати ефективні заходи проти можливих зловживань.

2. «Як необхідність у демократичному суспільстві». Прослуховування має бути: - тільки такою мірою, яка необхідна для безпеки демократичних інститутів;

- за виняткових умов та в інтересах національної безпеки й/або попередження безладу або злочинів» [12, с.36].

Зокрема, це означає, що законодавство має чітко визначати правові межі втручання держави у приватне життя людини шляхом проведення прослуховування чи моніторингу її комунікацій.

По-перше, закон має наводити вичерпний та конкретизований перелік злочинів, за вчинення чи підозру у здійсненні яких правоохоронні органи можуть отримати дозвіл на проведення прослуховування. Це має запобігати свавільному використанню засобів спостереження за громадянами з політичних, економічних чи інших неправомірних мотивів.

По-друге, законодавчо мають бути встановлені чіткі критерії для прийняття рішення щодо початку прослуховування, які повинні включати наявність вагомих фактичних доказів або обґрунтованих підозр у вчиненні особою конкретних тяжких злочинів. Прослуховування не може виступати як превентивний чи профілактичний захід на основі абстрактних або загальних підозр.

По-третє, прослуховування повинно санкціонуватися виключно за рішенням суду або іншого незалежного органу, що не належить до структури виконавчої влади. Таке рішення має схвалюватись на підставі письмової заяви високопосадовця із детальним обґрунтуванням необхідності втручання.

По-четверте, закон повинен обов'язково вказувати перелік часових обмежень на проведення прослуховування, що передбачає конкретний період часу, після якого така діяльність повинна бути припинена або повторно обґрунтована відповідною процедурою. Це гарантуватиме

недопущення постійного моніторингу за громадянами без об'єктивної потреби. Крім того, необхідно встановлювати суворі правила складання та зберігання звітів щодо результатів прослуховування, що дозволить контролювати правомірність використання зібраних даних.

Важливо, щоб були чітко прописані процедури обмеження на обмін інформацією, отриманою в результаті прослуховування, між державними органами, а також порядок знищення матеріалів, які вже не мають доказового значення або можуть призвести до порушення права особи на приватність.

Особливо актуальним є врегулювання ситуації, коли особу, яка піддавалася прослуховуванню, буде виправдано: в такому випадку закон має передбачати чіткі гарантії повернення або знищення матеріалів прослуховування, щоб уникнути їх неправомірного використання у майбутньому.

Нарешті, кожній особі, яка перебуває в юрисдикції країни, що допускає таємне прослуховування, повинно бути гарантоване право заявити про себе як про потенційну жертву такого втручання, без необхідності надавати докази здійснення щодо неї фактичного моніторингу, оскільки сама можливість застосування таких практик може створювати атмосферу постійного психологічного тиску і страху.

Всі зазначені вище положення є важливими, оскільки за умов стрімкого розвитку цифрових технологій та розширення можливостей масового спостереження з боку державних структур питання правового захисту приватності й конфіденційності стає надзвичайно актуальним, вимагаючи чіткого законодавчого регулювання та прозорості процедур, пов’язаних з втручанням у приватну сферу життя людей.

В умовах сьогоденного суспільства, поняття «необхідності» та «винятковості» заходів втручання держави в приватне життя громадян, особливо в контексті цифрової культури масового спостереження, набувають особливої актуальності та потребують поглибленого аналізу.

Разом із тим, сучасна культура масового спостереження, яка значно розширила свої масштаби завдяки цифровим технологіям, створює середовище, де межі між захистом демократичних інститутів та втручанням у приватне життя громадян стають дедалі менш очевидними. Можливість держави у постійному режимі отримувати доступ до величезних масивів персональних даних і комунікацій за допомогою штучного інтелекту, великих даних (Big Data) та алгоритмів машинного навчання створює ситуацію, коли обґрунтованість і доцільність таких заходів потребує постійної публічної дискусії й прозорого правового контролю.

Важливо враховувати, що зловживання або недостатньо вмотивоване застосування масового спостереження може негативно впливати на фундаментальні демократичні цінності, такі як свобода вираження поглядів, право на приватність,свобода зібрань, а також формувати в суспільстві культуру страху та самоцензури.

Сьогоднішне массовое стеження у поєднанні з досягненнями науково-технічного прогресу не знає меж. Так, у КНР з 2014 року існує та розвивається система соціального кредитування населення. Сутність системи полягає у формування слухняного суспільства через цифрову дисципліну, використовуючи практики «соціальної надійності» громадян. Система соціального кредиту пов’зяна також з масовим моніторингом, який дає можливістю розпізнавати обличчя громадян, аналізувати їхню *надійність* в мережі Інтернет, а також отримувати платіжну історію та інформацію громадян [266].

США також використовують програми массового стеження за громадянами. Так, ще у 2013 році, колишній розвідник АНБ США Едвард Сноуден, розкрив діялність системи PRISM, яка покликана збирати дані про електрону комунікацію мільйонів громадян в соціальних мережах та програмних додатків накшталт Microsoft, Skype, PalTalk, Facebook (Meta), Youtube, тощо [136, с.84].

Російська Федерація з 2020 року використовує систему під назвою «Orwell», яка направлена на масове стеження за власними громадянами. Тільки в Москві було встановлено понад 200 тис. камер з системами розпінавання облич [258].

Країни, які активно цифровізують систему управління та врядування, активно застосовують камери, як головний інструмент масового стеження, таким чином продовжуючи нагальний розвиток дихотомії права на приватність серед громадян.

«Сьогодні приватність розглядається, як фундаментальне право людини й перебуває в одному ряді із правом на життя, свободою переконань, власністю на майно та особисті здобутки на результати інформаційної та інтелектуальної праці» [15, с.37].

У сучасних умовах стрімкої цифровізації суспільства важливого значення набуває проблема зростання кіберзлочинності, яка має різноманітні форми та механізми реалізації. Серед найбільш поширених і водночас складних для ідентифікації кіберзлочинів є незаконне втручання у роботу інформаційних систем, зокрема, несанкціонований доступ до інформації, а також незаконне копіювання та використання програмних продуктів, даних та іншого електронного контенту.

Особливу складність становить розмежування таких понять, як несанкціонований доступ та крадіжка інформації, оскільки копіювання цифрових даних фактично не залишає очевидних слідів, на відміну від фізичної крадіжки. Основними способами такого втручання можуть бути викрадення і використання чужих паролів і логінів шляхом фізичного доступу до документації, підслуховування телефонних розмов, перехоплення електронних комунікацій, підглядання інформації безпосередньо з монітора комп’ютера або навіть збирання та аналіз «сміттєвих» даних. Також можливим є дистанційний злам системи через незахищені канали зв’язку або використання спеціалізованої апаратури для запису та прослуховування каналів передачі даних.

Другим поширеним видом злочину є незаконна модифікація або підробка комп’ютерної інформації. Вона може здійснюватися різними категоріями осіб – як зовнішніми зловмисниками, так і законними користувачами чи навіть розробниками програмного забезпечення, зокрема платформ, таких як 1С. Особливо небезпечними є випадки, коли вихідні дані або програмні продукти навмисно змінюються для імітації повноцінної роботоздатності з метою шахрайського отримання фінансової вигоди від замовників. Подібні маніпуляції можуть застосовуватись не лише в економічних цілях, але й для впливу на суспільні процеси, наприклад під час виборів або інших суспільних процедур.

Ще однією формою кіберзлочинності є створення та застосування шкідливого програмного забезпечення, серед якого особливе місце займають так звані «логічні» та «часові бомби». Такі програми запускаються за певних визначених умов або у визначений час, здатні частково або повністю виводити інформаційні системи з ладу. Відмінним різновидом такого програмного забезпечення є «троянські коні» – програми, які таємно інтегруються в інші програмні продукти та забезпечують прихований доступ до конфіденційної інформації, що зберігається на комп'ютері. Подібні шкідливі елементи дуже важко ідентифікувати та ліквідувати, оскільки вони можуть бути приховані навіть у звичайних електронних документах, листах, мультимедійних файлах або інших електронних повідомленнях, а після виконання завдання знищуватись самостійно, залишаючи мінімальні сліди.

Не менш вагомою є проблема розробки та поширення комп'ютерних вірусів, які здатні серйозно пошкоджувати програмне забезпечення та завдавати значних збитків бізнесу та приватним особам. Наслідки дії таких вірусів можуть варіюватися від незначних технічних збоїв до повного знищення важливих цифрових даних і баз інформації. Зокрема, вірусні атаки на програмні продукти типу 1С є прикладом реальних загроз для функціонування бізнес-середовищ. Діапазон їхньої шкоди може бути від

невеликих втручань до серйозних наслідків, таких як знищення баз даних, що призводить до порушення нормальної діяльності підприємств. Сучасні загрози також включають у себе шифрувальні віруси, які блокують доступ до інформації та вимагають виплати викупу за її повернення, що ще більше поглиблює складність забезпечення інформаційної безпеки.

Таким чином, з огляду на стрімкий розвиток інформаційних технологій та цифрового простору, кіберзлочинність продовжує залишатися серйозним викликом, що потребує розроблення новітніх технологічних рішень та ефективного законодавчого регулювання з метою захисту прав людини та забезпечення безпеки інформаційного суспільства.

Злочинна недбалість у сфері розробки, створення та експлуатації комп'ютерних систем і програмного забезпечення являє собою особливий різновид правопорушень, що характеризуються недостатньою відповідальністю та необережністю розробників, програмістів чи адміністраторів інформаційних ресурсів, наслідком яких можуть стати серйозні негативні наслідки для інформаційної безпеки, порушення нормальної діяльності підприємств, установ та навіть завдання значних матеріальних чи репутаційних збитків організаціям чи приватним особам. Водночас слід наголосити, що унікальною особливістю сфери інформаційних технологій є те, що цілковито безпомилкових програмних продуктів не існує у принципі, адже в процесі розробки та експлуатації неможливо абсолютно виключити наявність певних помилок і вразливостей у програмному забезпеченні.

Разом із тим, юридична відповідальність виникає у ситуаціях, коли розробники або адміністратори програмних продуктів проявили недостатній рівень професійної відповідальності та не вжили необхідних заходів для запобігання негативним наслідкам через недоліки у програмному забезпеченні. Для встановлення вини у такій формі злочинної недбалості, яка пов'язана саме з розробкою програмного забезпечення, правоохоронні органи можуть враховувати кілька важливих критеріїв.

Зокрема, до них належать наявність доказів того, що помилки, допущені у програмному коді, могли бути передбачені розробниками та виявлені за умови достатньої ретельності і відповідального ставлення до роботи. Показником вини у цьому контексті є передусім ситуації, коли у проектній документації або технічних завданнях уже містилися чіткі попередження чи рекомендації щодо конкретних загроз, ризиків і потенційних вразливостей, однак належних заходів щодо їх усунення чи попередження реалізовано не було.

Також важливим доказом наявності злочинної недбалості з боку розробників є можливість виявлення та попередження помилок за допомогою вже наявних технологічних чи методичних інструментів тестування та перевірки програмного забезпечення. Тобто, якщо конкретна помилка могла бути легко виявлена шляхом ретельного аналізу коду, тестування програми на різних етапах її створення та експлуатації, але цього не було зроблено, така недбалість визнається юридично значущою і може призводити до відповідальності за завдані збитки.

Окремим і особливо небезпечним проявом недбалості розробників та програмістів є навмисне створення або залишення без належного контролю у програмному забезпеченні так званих «люків», або «чорних ходів». Під цими термінами розуміють приховані та зазвичай недокументовані точки входу до програмних модулів, які первинно створюються для полегшення процесу тестування та відлагодження коду, або для швидкого доступу розробників до внутрішніх структур програмного забезпечення. Проте, залишені без належного контролю та документації, такі «люки» або «чорні ходи» можуть стати серйозною загрозою безпеці інформаційних систем, оскільки їх часто використовують кіберзлочинці або несанкціоновані особи для отримання нелегального доступу до конфіденційних даних чи здійснення інших протиправних дій. Крім того, можливість несанкціонованого використання таких прихованих інструментів доступу може створювати умови для потенційних витоків конфіденційних даних,

порушення правил захисту інформації та загального зниження довіри до системи інформаційної безпеки підприємств і організацій [15].

З метою запобігання таким випадкам необхідно проводити регулярний та всебічний аналіз вихідного програмного коду, ретельні перевірки із залученням спеціалізованих програмних та технічних засобів, а також здійснювати моніторинг і контроль за діяльністю персоналу, відповідального за розробку, адміністрування і підтримку програмного забезпечення та інформаційних систем. Лише такий комплексний підхід дозволить знизити загрози негативних наслідків злочинної недбалості у цифровій сфері, що у свою чергу сприятиме підвищенню рівня інформаційної безпеки та забезпеченню приватності користувачів.

У сучасному цифровому суспільстві серйозні та непередбачувані наслідки можуть виникати не лише через недбалість чи помилки програмістів і розробників комп'ютерних систем, але й через халатність безпосередніх користувачів інформаційних технологій. Важливим аспектом визначення дій користувачів як таких, що містять ознаки халатності, є наявність у цих осіб достатньої та доступної інформації про потенційні негативні наслідки порушення встановлених інструкцій або правил експлуатації комп’ютерних систем. Це означає, що користувач повинен мати чітке розуміння ризиків і небезпек, пов'язаних з невиконанням конкретних вимог безпеки, і попри це, він свідомо ігнорує ці правила. Крім того, для визначення халатності важливо враховувати реальну можливість користувача фізично та психологічно виконувати встановлені вимоги і правила користування інформаційними системами. Якщо встановлено, що виконання цих вимог було цілком здійсненним та не вимагало особливих зусиль, але користувач проявив свідоме або необережне ігнорування таких вимог, його дії можуть бути кваліфіковані як халатні.

Окрему категорію становлять комп'ютерні злочини, які здійснюються за допомогою глобальної мережі Інтернет, яка сьогодні є не тільки важливим інструментом комунікації та ведення бізнесу, але й майданчиком

для здійснення різних видів протиправних дій. Виокремлення саме цієї категорії злочинів зумовлене специфікою та реаліями функціонування сучасного інформаційного середовища. Насамперед, Інтернет дедалі частіше використовується як засіб скоєння традиційних кримінальних правопорушень, таких як промисловий шпіонаж, саботаж економічної діяльності підприємств, поширення дитячої порнографії та інших видів незаконного контенту. Однак одним з найпоширеніших видів комп'ютерних злочинів в мережі Інтернет є різноманітні форми шахрайства, від яких потерпає понад третина користувачів мережі.

Відносно новим, але надзвичайно ефективним механізмом шахрайських дій є створення різноманітних сумнівних інвестиційних пропозицій та продаж фіктивних активів. До таких прикладів належать пропозиції щодо придбання нерухомості в Еквадорі, нафтових свердловин в Антарктиді чи кокосових плантацій у Коста-Риці, а також побудова фінансово-інвестиційних пірамід. Широке поширення отримали шахрайські схеми з продажу акцій маловідомих компаній, коли брокери навмисно завищують їх цінність шляхом штучного створення ажіотажу, що призводить до втрати значних сум грошей інвесторами. Сотні тисяч користувачів отримують рекламні листи або посилання на такі сайти, а відсутність належної інформаційної грамотності та довірливість значної кількості людей створюють сприятливе середовище для масштабного шахрайства [15].

Ключовим елементом більшості таких шахрайських схем є отримання несанкціонованого доступу до персональних даних користувачів, що відкриває додаткові можливості для зловживань та маніпуляцій. Наприклад, дуже часто користувачів просять заповнити різноманітні анкети або форми, які містять особисту інформацію, контактні дані, а в окремих випадках і фінансові реквізити, зокрема інформацію про банківські картки. В результаті особа, яка надала таку інформацію, стає потенційною жертвою подальших шахрайських маніпуляцій, що може призвести до прямих

фінансових втрат або інших негативних наслідків. Найбільш вразливими в такому контексті є довірливі користувачі, які надають свої платіжні реквізити та інші фінансові дані, які дозволяють шахраям безпосередньо отримувати доступ до коштів постраждалих осіб.

Отже, актуальність цієї проблематики вимагає здійснення цілеспрямованих заходів щодо підвищення рівня інформаційної безпеки, впровадження ефективних освітніх програм для користувачів щодо інформаційної грамотності та ретельнішого правового регулювання у сфері захисту персональних даних в умовах цифрового суспільства. Тільки за умови комплексного підходу можна суттєво знизити загрози, пов’язані з комп'ютерними злочинами та шахрайством у мережі Інтернет.

У зв'язку з інтенсивним поширенням глобальної мережі Інтернет і посиленням її ролі у житті сучасного суспільства, зростає кількість злочинів, що безпосередньо пов'язані із самим фактом її існування та функціонування. Окрім традиційних форм злочинних дій, таких як поширення комп'ютерних вірусів або несанкціоноване проникнення («зламування») на веб-сайти та цифрові платформи, існують також інші специфічні види протиправних дій, зумовлених можливостями й особливостями глобального цифрового простору. «Серед них слід виокремити наступні:

- «нюкання» (від англійського «nuke», ядерна зброя) – програмна атака на іншого користувача Інтернет, у результаті якої його комп'ютер втрачає зв'язок з мережею або «зависає»;

- «спам» (від англійського «spam») або «junk mail» (пошта з мотлохом, непотрібна кореспонденція) – варіант багаторівневого маркетингу в мережі. Спаммерів можна поділити на дві групи. Першу становлять новачки, які тільки-но одержали доступ до Мережі та усвідомили, що можуть розсилати повідомлення куди завгодно і кому завгодно. Другу групу утворюють професіонали, які заробляють гроші на заздалегідь неправдивій рекламі типу «Отримай премію...», «Розбагатій...», «Швидко зароби...» і т. ін. Про

нечесність таких «бізнесменів» говорить хоча б їх небажання вказати свої справжні ім'я та координати;

- «винюхування» («sniffing») – сканування пакетів, які передаються в мережі для одержання інформації про користувача (-ів);

- «серверний трикутник» (Web-spoofing, Web-мистифікація) – зловмисник, який проникає на сайт, змінює механізм пошуку так, що вся інформація, що її запитують користувачі, передається через якийсь інший сайт, де її, до того ж, можуть певним чином «обробити»;

- мережні атаки, спрямовані на «зависання» серверів («Denial of service attack», DOS-attack, атака, що спричинює відмову від обслуговування) або уповільнення їхньої роботи різними способами («повені»). Найчастіше для реалізації таких атак використовуються пакети технологічної інформації та самі правила взаємодії серверів за мережними протоколами» [15, с. 7].

Такі злочинні практики, свідчать про те, що у цифрову епоху межі особистого простору та приватності стають дедалі більш вразливими та прозорими для зовнішніх впливів. Кожен із цих злочинів не лише є вторгненням у приватне життя користувачів, але й створює умови для тотального контролю над інформаційною поведінкою людей, обмежуючи їхню можливість вільно й безпечно використовувати цифрові технології.

Сучасні дослідження «приватності» розглядають це поняття як багатовимірний феномен, який охоплює різні сфери життя людини та передбачає захист особистості від втручання з боку суспільства, держави чи інших осіб. Зокрема, варто погодитися із тим, що « фізична приватність – це умови захисту від примусових для людини процедур, зокрема медичних» [15, с. 37].

Проте, ця форма приватності не є абсолютною, оскільки держава, враховуючи суспільний інтерес, може встановлювати певні обмеження та винятки. Наприклад, правомірними визнаються Так, «поліції надане право

зняти в арештованого відбитки пальців або узяти в нього аналіз ДНК для включення в національну базу даних і т.п»

Окрім фізичної приватності, важливе місце у структурі захисту особистого життя займає «територіальна та майнова приватність, яка традиційно трактується як право особи на «...недоторканність фізичних речей та житла» [12, с.37].

Однак це право поширюється не лише на приватні будинки чи квартири, а й на інші простори, які особа тимчасово займає і вважає приватними — наприклад, робоче місце, номер у готелі або купе в поїзді. Важливим аспектом цієї категорії приватності є право володіння та розпорядження майном, що охоплює як фізичні об'єкти, так і об'єкти інтелектуальної власності. При цьому законодавче визначення права власності на інформаційні продукти сьогодні залишається неврегульованим, попри те, що інформація давно стала об'єктом комерційного обігу.

Найбільш актуальною і складною у сучасних умовах інформаційного суспільства є проблема «інформаційної приватності, яка передбачає «захисту прав людини та свобод в інформаційній сфері, її уявлень та намагань покращити своє життя» [12, с.37].

Інформаційна приватність тісно пов’язана із забезпеченням свободи самовираження, формування власних поглядів, ідей, прагнень та умов для самовдосконалення і реалізації життєвих планів без стороннього втручання та контролю».

Окремою важливою складовою загальної концепції приватності є «приватність комунікацій, яка стосується захисту конфіденційності процесів спілкування за допомогою технічних і технологічних засобів, таких як телефонні розмови, поштові відправлення або електронні повідомлення. Цей різновид приватності, можливо, є найбільш вразливим у сучасних умовах масового використання Інтернету та цифрових технологій, оскільки саме інтернет-простір створює безпрецедентні можливості для

несанкціонованого спостереження, втручання, маніпуляцій та контролю з боку різних суб’єктів, включаючи державні органи, комерційні структури чи окремих осіб».

Розглядаючи ці категорії приватності, слід зазначити, що кожна з них у цифрову епоху стикається із суттєвими викликами, пов'язаними зі швидким розвитком технологій масового спостереження, кіберзлочинністю та інформаційною експансією, що робить необхідним не лише юридичне закріплення відповідних гарантій, але й розвиток технічних та освітніх механізмів захисту приватності. Лише комплексний підхід, що включає правове регулювання, технологічні засоби та формування культури поваги до приватності, може забезпечити реальну дієвість цього фундаментального права людини в умовах сучасних цифрових реалій.

Зазначені дії та заходи безпосередньо пов'язані з актуальною проблематикою забезпечення ефективного захисту інформаційної приватності та конфіденційності персональних даних громадян в Україні, що є ключовою складовою більш широкого питання гарантування інформаційної безпеки особистості, суспільства і держави загалом. У контексті активного розвитку цифрових технологій, зростання ролі інформації в усіх сферах суспільного життя, а також посилення глобальних загроз у кіберпросторі, інформаційна приватність та захист персональних даних перестають бути лише індивідуальною або корпоративною справою і набувають статусу національно значущих пріоритетів. Від того, наскільки ефективно та комплексно вирішуються питання захисту приватної інформації, залежить не тільки збереження прав і свобод людини, але й довіра громадян до державних інституцій, стабільність соціально-економічних процесів, а також репутація України на міжнародній арені.

Таким чином, посилення нормативно-правових, організаційно-технічних та інформаційних механізмів захисту інформаційної приватності стає важливою умовою зміцнення національної безпеки, оскільки потенційні загрози витоку чи несанкціонованого використання

персональних даних можуть спричинити серйозні політичні, економічні та соціальні наслідки для держави.

Відповідно, державна політика України у сфері інформаційної безпеки повинна активно орієнтуватись на створення ефективних інструментів захисту приватності персональних даних, удосконалення відповідної законодавчої бази, розробку сучасних технологій і програм, а також формування високої культури інформаційної безпеки серед населення, що сприятиме успішній протидії загрозам у кіберпросторі. Конфіденційність персональних даних є одним із ключових питань сучасного українського законодавства, що підтверджується значною кількістю нормативно-правових актів, які стосуються захисту інформації про фізичну особу.

Зокрема, згідно зі ст. 10 Закону України «Про інформацію» (2016) [104], одним із видів інформації про «фізичну особу», які становлять основу будь-яких професійних таємниць та підлягають конфіденційному захисту відповідно до ст. 21 цього ж Закону.

В цій статі також визначається порядок поширення конфіденційної інформації, а саме :

- за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом» [105].

Однак, українське законодавство не має чіткого визначення (дефініції) поняття «конфіденційна інформація», хоча цей термін активно використовується в багатьох нормативних актах.

Наприклад, Конституція України (ст. 32) передбачає :

«Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав

людини» [54]. Водночас, термін «*приватність*» у Конституції не використовується.

Кримінальний кодекс України (ст.182) також оперує терміном «*конфіденційна інформація*», визначаючи кримінальну відповідальність за незаконне її використання або зберігання, але не уточнює змістовного наповнення цього поняття [59].

Цивільний кодекс України (ст. 895) лише згадує поняття *конфіденційних відомостей*, тобто «Виконавець і замовник зобов'язані забезпечити конфіденційність відомостей щодо предмета договору на виконання науково-дослідних або дослідно-конструкторських та технологічних робіт, ходу його виконання та одержаних результатів, якщо інше не встановлено договором.

Обсяг відомостей, що належать до конфіденційних, встановлюється договором» [159]. Проте і цей Кодекс не надає дефініції терміну «конфіденційності».

Податковий кодекс України ст. 17.1.9 «на нерозголошення контролюючим органом (посадовими особами) відомостей про такого платника без його письмової згоди та відомостей, що становлять конфіденційну інформацію, державну, комерційну чи банківську таємницю та стали відомі під час виконання посадовими особами службових обов'язків, крім випадків, коли це прямо передбачено законами» [85].

Термін «*конфіденційність*» згадується щонайменше тричі у Кодексі але також не дається конкретної дефініції. Аналогічна ситуація спостерігається і в Митному кодексі України, де термін згадується, щонайменше 16 разів але без належної дефініції.

Закон України «Про інформацію» (ст. 11) подає перелік персональних даних, що належать до конфіденційних (національність, освіта, сімейний стан тощо), але містить невизначеності через використання терміну «зокрема», що передбачає відкритий перелік [104].

Закон України «Про доступ до публічної інформації» (ст. 7) надає лише процесуальну дефініцію конфіденційності, визначаючи її як «інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов» [94].

Крім цього, термін «*конфіденційна інформація*» згадується у законах «Про друковані засоби масової інформації (пресу) в Україні», [96] «Про телебачення і радіомовлення», [119] «Про свободу пересування та вільний вибір проживання в Україні» [115], «Про загальнообов'язкове державне соціальне страхування» [100], «Про звернення громадян» [103], «Про загальнообов'язкове державне пенсійне страхування» [99], «Про недержавне пенсійне забезпечення» [111], «Про оплату праці» [112], «Про лікарські засоби» [107], «Про біженців та осіб, які потребують додаткового або тимчасового захисту», [91] «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві» [99], «Про державний захист працівників суду і правоохоронних органів» [93], «Про доступ до судових рішень» [95], «Про Всеукраїнський перепис населення» [92], «Про поховання та похоронну справу» [114] та інших, проте у жодному з них не представлено повного та системного визначення конфіденційності.

Єдиний формальний нормативний документ, що надає загальну дефініцію поняття «конфіденційна інформація», є ДСТУ 3396.2-97 «Технічний захист інформації. Терміни та визначення», згідно з яким конфіденційна інформація визначається як : «Інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава» [28].

Однак ця дефініція має лише технічний характер і не підкріплена відповідними нормами сучасного законодавства України, що суттєво ускладнює ефективний захист інформації у сучасному цифровому середовищі.

Відсутність чіткої законодавчої дефініції поняття «конфіденційна інформація» у нормативно-правовому полі України створює потенційні загрози у контексті масового спостереження та контролю за громадянами в умовах сучасного цифрового суспільства.

У ситуації, коли державні або приватні організації отримують доступ до персональних даних без чіткого визначення меж допустимого втручання, існує реальна загроза зловживання конфіденційною інформацією, що може призвести до порушення фундаментальних прав людини, включаючи право на приватність і свободу самовираження. Зростання культури масового спостереження підсилює ці загрози, адже відсутність чітких законодавчих норм призводить до неконтрольованого збору та використання даних, які можуть використовуватися як інструмент політичного, економічного чи соціального впливу.

Таким чином, для України надзвичайно важливим є вдосконалення чинного законодавства, впровадження чітких нормативних визначень та гарантій конфіденційності персональних даних, що дозволить ефективно протидіяти негативним наслідкам культури масового спостереження та забезпечити дотримання основоположних прав людини у цифрову епоху.

Отже, культура масового спостереження не є новим явищем, проте вона набула нових рис з розвитком інформаційних технологій. Раніше масове спостереження зазвичай відбувалося за допомогою камер спостереження на вулицях та в об'єктах загального користування. Зараз же велика кількість людей веде активне онлайн-життя, ділиться особистими даними в соціальних мережах, а їхні кроки в інтернеті можуть бути легко відстежені.

З одного боку, культура масового спостереження відкрила нові можливості для комунікації та обміну інформацією. Вона дозволила зв'язати людей з різних кінців світу і забезпечила доступ до неймовірної кількості знань і ресурсів. Проте, з іншого боку, це також створило загрозу для приватності і конфіденційності.

Збільшення кількості даних, які ми ділимося в інтернеті, робить нас більш вразливими перед можливими порушеннями приватності. Компанії збирають великі обсяги інформації про користувачів для рекламних цілей, а деякі з них можуть навіть продавати ці дані третім сторонам. Це породжує питання про те, наскільки ми контролюємо власні особисті дані та кому ми довіряємо їх зберігання.

Питання конфіденційності також виникають в контексті масового спостереження. У деяких країнах влада здійснює широкомасштабне спостереження за громадянами без їхньої належної обізнаністю до контролю. Це може призвести до порушення основних прав і свобод людини, таких як право на приватність, свободу слова та свободу об'єднання.

Для забезпечення захисту прав конфіденційності та приватності людей в умовах культури масового спостереження важливо приділяти увагу цьому питанню. Споживачі повинні бути обізнані щодо своїх прав, пов'язаних з приватністю, і дотримуватися заходів безпеки в інтернеті. Законодавчі органи також мають розробити ефективні закони та регулювання, щоб забезпечити захист особистих даних громадян.

2.2. Алгоритмічна цензура, маніпуляція інформацією та контроль політичного дискурсу

Право на свободу слова, як фундаментальне право людини, відіграє особливу роль у демократичному суспільстві, забезпечуючи не лише вільний розвиток особистості, але й слугуючи необхідною умовою для повноцінної реалізації інших основоположних прав і свобод громадян. В умовах сучасного суспільного розвитку право на свободу вираження поглядів, думок і переконань набуло додаткового значення, особливо у зв'язку з поширенням та розвитком глобальної інформаційної мережі Інтернет. Це спричинило необхідність переосмислення традиційних

підходів до нормативно-правового регулювання вказаного права, створення нових механізмів та інструментів його забезпечення у цифровому середовищі.

Упродовж останніх двох десятиліть питання правового регулювання реалізації права на свободу слова в Інтернеті стало предметом активних обговорень на міжнародному рівні. Наслідком цього стала розробка низки міжнародних актів, рекомендацій та резолюцій авторитетних міжнародних організацій, таких як ООН, Рада Європи, ОБСЄ тощо.

Незважаючи на це, до сьогоднішнього дня так і не було створено комплексного міжнародного правового документа, який би повною мірою регулював усі аспекти реалізації права на свободу вираження поглядів саме у цифровому середовищі, що є серйозною проблемою в умовах глобалізації інформаційного простору.

У сучасну епоху цифрової трансформації інформаційні суспілства усе частіше стають ареною політичної боротьби, де традиційні інструменти цензури поступаються місцем алгоритмічним механізмам впливу. Алгоритми – це автоматизовані системи, які керують видимістю, поширенням і пріоритетністю контенту в онлайн-середовищі — дедалі активніше використовуються не лише для комерційних цілей, а й як інструмент політичного контролю.

На відміну від прямої цензури, алгоритмічна цензура є менш помітною, але не менш ефективною формою обмеження свободи слова та маніпуляції громадською думкою. Цей феномен проявляється у формуванні так званих «інформаційних бульбашок», практиці shadow banning (прихованого обмеження контенту), алгоритмічному заниженні рейтингів політично небажаних матеріалів та автоматизованому виявленні «чутливих» тем [158].

Як свідчать численні дослідження, така цензура здійснюється як державними структурами, так і приватними технологічними корпораціями, часто без прозорих механізмів контролю та відповідальності. Так,

Угорщина під керівництвом Віктора Орбана значно зазнала згортання медіа-плюралізму. Компанія втручання у роботу більшісті великих медіа полягає у переході під контроль урядових союзників, а алгоритми Facebook використовуються для поширення пропагандистських меседжів.

Так за даними незалежної оціночної компанії RSF (Report without borders) у 2024 році був проаналізований стан та « Індекс свободи ЗМІ» , стверджувалось, що Віктор Орбан побудував «медіа-імперію» KESMA (Центральний європейський пресхолдинг) в склад якої входять сотні ЗМІ, які транслюють однакові наративи серед громадян [255].

Відсутність комбінованої роботи з KESMA зі сторони опозиційних або нейтральних ЗМІ, угорська держава «вистежує» журналістів за допомогою програмної системи Pegasus. Крім того, в контексті наклепницьких кампаній журналісти, які критикують уряд, піддаються переслідуванням в Інтернеті з боку прихильників правлячої партії [255].

Таким чином, Угорщина має можливість активно вплипвати на процеси контролю політичного дискурсу в середині держави та заздалегідь маніпулювати інформацією, яка розповсюджується через підконтрольні уряду ЗМІ.

Російська Федерація активно використовує підконтрольні ЗМІ для поширення урядових наративів в соціальних мережах та формування керованої реальності серед людей в країні.

Так, за звітами Freedom House, за останні роки (2022-2024) «уряд продовжував блокувати критичні сайти новин і розробляв все більш складні технічні та законодавчі заходи для блокування віртуальних приватних мереж (VPN). Державні органи докладають величезних зусиль для стеження за тими, хто критикує уряд у мережі. Суди також ухвалили ув'язнювати онлайн-критиків повномасштабного вторгнення на Україну та уряди в цілому» [216].

Польща упродовж останнього десятиліття зазнє значної політичної трансформації, зокрема після закріплення у влади консервативної партії

Право і справедливість (PiS). Водночас зросли занепокоєння з боку міжнародних організацій щодо спроб уряду контролювати інформаційний простір, впливати на незалежні медіа та використовувати цифрові платформи для маніпуляцій громадською думкою. Так, у 2022 році, уряд Польщі під керівництвом PiS здійснив радикальну реформу державного телебачення та радіо, перетворивши їх на інструмент політичної пропаганди. Цей контент, що широко поширюється в цифровому середовищі (зокрема в YouTube, Facebook, Twitter), просувається за допомогою алгоритмів соцмереж, які автоматично підсилюють матеріали з великою кількістю взаємодій, лайків і репостів [215].

Державний канал TVP Info, систематично публікує контент з антиопозиційною або антиєвропейською риторикою. Аналітики виявили, що подібний контент активно просувався в соцмережах, часто випереджаючи незалежні джерела через використання ботів, таргетованої реклами та алгоритмічну перевагу емоційного або поляризуючого контенту [215].

У цьому контексті важливо звернути увагу на ситуацію в Україні, яка, попри наявність демократичного устрою та задекларовану орієнтацію на європейські стандарти, також стикається з викликами, пов’язаними з балансуванням між цифровою безпекою, захистом державного суверенітету та забезпеченням основоположних прав і свобод громадян.

В Україні право на свободу слова гарантується на рівні Конституції (стаття 34 Конституції України), однак серед правознавців та експертів існує думка щодо наявності певних неузгодженостей між нормами Конституції, які встановлюють обмеження права на свободу думки та слова, і відповідними положеннями міжнародних правових актів, таких як Європейська Конвенція з прав людини та основоположних свобод.

Внаслідок цього можуть виникати труднощі у процесі імплементації міжнародних стандартів у національну правову систему України.

Крім конституційного рівня, в Україні існує низка нормативних актів, які певною мірою регулюють питання реалізації свободи слова в Інтернеті, однак практика показує, що чинної нормативно-правової бази є недостатньо для ефективного розв'язання нових викликів, що виникають у цифровому просторі.

Однією з основних проблем при реалізації права на свободу слова в українському сегменті Інтернету є надмірні обмеження, блокування ресурсів та фільтрація контенту, які нерідко здійснюються без достатнього правового обґрунтування або суперечать міжнародним стандартам.

Зокрема, яскравими прикладами є блокування доступу до іноземних сайтів, закриття файлообмінних ресурсів, непрозорі перевірки бізнесу та інші обмежувальні заходи, що викликають занепокоєння серед правозахисних організацій та експертного середовища.

Зазначені негативні тенденції підтверджуються також відповідною судовою практикою Європейського суду з прав людини, який неодноразово у своїх рішеннях вказував на неприпустимість невиправданих або надмірних обмежень свободи вираження поглядів у мережі Інтернет.

Окрім цього, звіти та дослідження міжнародних правозахисних організацій, таких як Freedom House та Reporters Without Borders, констатують недостатній рівень свободи Інтернету в Україні, наголошуючи на існуванні численних ризиків і загроз, які пов'язані із запровадженням обмежувальних законодавчих ініціатив. Ці ініціативи не відповідають міжнародно визнаним стандартам та створюють потенційні загрози для демократичного розвитку суспільства.

Таким чином, Україна не є унікальним прикладом, адже проблема забезпечення права на свободу слова у цифровому середовищі актуальна для багатьох країн світу. Різні держави стикаються з труднощами у створенні належного нормативно-правового регулювання, яке б враховувало як необхідність захисту прав громадян, так і гарантування суспільних інтересів та національної безпеки.

Тому подальше вдосконалення законодавства у сфері Інтернету, імплементація міжнародних стандартів та принципів є надзвичайно актуальним завданням для України та інших країн світу з метою забезпечення реальної свободи слова та поваги до фундаментальних прав людини в умовах цифрового суспільства. Інтернет, як всесвітня мережа, що виникла у другій половині минулого століття, стрімко інтегрувалась у повсякденне життя людей та значною мірою трансформувала майже всі аспекти суспільного існування.

Цифрова революція, що супроводжувалася безпрецедентними темпами зростання, кардинально змінила соціальні, політичні, економічні, освітні, культурні, наукові та інші суспільні процеси, створивши новий, до цього часу невідомий, простір взаємодії. Проте надзвичайно високі темпи технологічного розвитку Інтернет-сфери суттєво ускладнюють можливості адекватного та своєчасного правового регулювання суспільних відносин, які перенеслися у цифровий простір.

Таким чином, менш ніж за півстоліття, була створена глобальна комунікаційна система, що виходить далеко за межі традиційного сприйняття суспільних відносин і ставить перед державами та міжнародним співтовариством завдання пошуку нових, більш ефективних підходів до регулювання цифрових взаємовідносин.

В умовах зазначених трансформацій особисті права і свободи людини також набувають нових форм свого вираження, що потребує відповідного перегляду і адаптації існуючих правових концепцій і механізмів їх захисту. Особливого значення набуває право людини на свободу слова, що на сьогодні визнається і закріплене в конституціях усіх демократичних держав світу та гарантується міжнародними правовими актами.

В минулому можливість поширення інформації була обмежена чітко визначеним колом реципієнтів: слухачами певного заходу, читачами друкованих видань, аудиторією конкретного телеканалу або слухачами радіо.

Проте сьогодні, завдяки мережі Інтернет, інформація стала практично миттєво доступною для мільярдів людей у всьому світі. Така глобалізація комунікативного простору докорінно змінила не тільки сам процес реалізації права на свободу вираження думок, а й у геометричній прогресії загострила всі супутні складнощі, пов'язані з його ефективним захистом і забезпеченням.

Однією з ключових характеристик цифрового простору є фактична можливість уникнути багатьох традиційних механізмів контролю за інформаційним контентом. Якщо раніше публікація будь-якої інформації зазвичай вимагала отримання схвалення від відповідального редактора або іншої уповноваженої особи, то сьогодні, в епоху Інтернету, кожен користувач отримує безпосередній доступ до глобальної аудиторії, що робить процес поширення інформації практично неконтрольованим.

Крім того, можливість розміщення інформації анонімно або під вигаданими іменами суттєво ускладнює процес ідентифікації автора, що додатково посилює загрози поширення неправдивої інформації, втручання в особисте життя або порушення права на повагу до людської гідності. Таким чином, у сучасних умовах надзвичайно важливим завданням стає пошук балансу між правом на свободу слова та іншими особистими правами громадян, зокрема правом на невтручання у приватне життя, правом на захист персональних даних та правом на повагу до гідності особистості. Адже відсутність ефективного регулювання може призвести до зловживань, дискредитації осіб чи поширення інформації, що має потенціал порушувати інші фундаментальні права людини.

Отже, необхідність створення чітких, ефективних і одночасно гнучких правових механізмів захисту стає очевидною, оскільки лише за таких умов можливо забезпечити як повноцінну реалізацію свободи слова, так і захист інших базових прав у цифрову епоху.

Питання процесів правового обмеження свободи слова та вираження поглядів в мережі Інтернет активно досліджуються сучасними науковцями.

Різні аспекти цієї проблематики проаналізовані у працях В. Брижко, В. Гавловського, В. Гриценка, Р. Калюжного, О. Дашковської, А. Червяцової, О. Турути, О. Малигіна, О. Нестеренко та ін. [165].

Проте зазначене питання у наукових працях здебільшого висвітлювалося фрагментарно, частково або ж обмежувалося переважно теоретичними аспектами, без глибокого аналізу практичних механізмів та наслідків застосування відповідних правових норм у конкретних ситуаціях.

Відповідно, з огляду на стрімкий розвиток інформаційно-комунікаційних технологій і зростання кількості нових викликів, які виникають у процесі реалізації прав і свобод людини в цифровому середовищі, стає очевидною потреба в подальшому комплексному дослідженні даної тематики. Особливу увагу слід приділити пошуку нових джерел, що дозволяють краще зрозуміти правову природу відносин, що формуються в Інтернет-просторі, а також визначенню оптимального співвідношення чинних правових норм з реальними ситуаціями, що виникають на практиці.

Подальше опрацювання цього питання дозволить не тільки усунути існуючі теоретичні прогалини, але й запропонувати практичні рекомендації щодо вдосконалення чинного законодавства з метою ефективного захисту прав і свобод людини, зокрема права на свободу слова, в умовах сучасних цифрових трансформацій суспільства.

Право на свободу слова є фундаментальним правом людини, закріпленим у низці міжнародно-правових актів, до яких приєдналася Україна.

1) Загальна декларація прав людини (1948 р.) Стаття 19. «Кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів» [39].

Ця стаття підкреслює універсальність та безмежність права на вираження думок, незалежно від національних кордонів.

2) Конвенція про захист прав людини і основоположних свобод (1950 р.) Стаття 10 визначає:

«1. Кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх переконань, отримувати та передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів» [52].

Це положення стало основою для численних рішень Європейського суду з прав людини, які стосуються захисту свободи вираження в різних контекстах, включаючи Інтернет.

3) Міжнародний пакт про громадянські та політичні права (1966 р.) Стаття 19 закріплює:

«1. Кожна людина має право безперешкодно дотримуватися своїх поглядів.

2. Кожна людина має право на вільне вираження свого погляду; це право включає свободу шукати, одержувати і поширювати будь-яку інформацію та ідеї, незалежно від державних кордонів, усно, письмово чи за допомогою друку або художніх форм вираження чи іншими способами на свій вибір» [75].

4) Конституція України (1996 р.) На національному рівні, стаття 34 Конституції України гарантує:

«Кожному гарантується право на свободу думки і слова, на вільне вираженнясвоїх поглядів і переконань» [54].

Крім того, ця стаття забезпечує право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб на власний вибір. Варто зазначити, що формулювання «незалежно від кордонів», яке міститься в міжнародних актах, дало змогу Європейському суду з прав людини поширити дію цих положень на

випадки, пов'язані з Інтернетом, визнаючи його важливим засобом реалізації права на свободу вираження.

Таким чином, право на свободу слова закріплене в ключових міжнародних та національних правових актах, що підкреслює його фундаментальне значення для демократичного суспільства та розвитку особистості.

Доктор юридичних наук В. Буткевич досліджуючи питання неузгодженості положень Конституції України та положень міжнародно-правових актів пише : «Внаслідок таких неузгодженостей конституційні формулювання дуже часто призводять до конфлікту Конституції і міжнародних зобов’язань України.

Скажімо, у Конвенції про захист прав людини і основоположних свобод можливість обмеження свободи думки передбачена лише у чотирьох випадках:

1) в інтересах громадської безпеки;

2) для охорони публічного порядку;

3) для охорони здоров’я чи моралі;

4) для захисту прав і свобод інших осіб. У Конституції до цих випадків додано:

5) національну безпеку;

6) територіальну цілісність;

7) запобігання заворушенням і злочинам;

8) захист репутації інших;

9) запобігання розголошенню інформації, одержаної конфіденційно;

10) підтримку авторитету і неупередженості правосуддя. Таких і стільки обмежень не знає законодавство демократичних держав навіть на випадок воєнного стану. Нерідко обмеження подаються за формулою: «за винятком обмежень, які встановлюються законом», без визначення тих сфер, у яких це можна робити на підставі закону. Таким чином, обмеження стають необмеженими» [165,с.54].

Згідно із Рекомендацією № CM / Rec (2015) 6 Комітету міністрів Ради Європи «Про вільний транскордонний рух інформації в Інтернеті» [128].

У першому положенні стверджує, що «Право на свободу висловлення переконань, зокрема отримувати і передавати інформацію та думки без втручання і незалежно від кордонів, є наріжним камінням демократичного суспільства і однією з основних умов для його стійкого розвитку і вдосконалення, а також для розвитку кожної людини» [128].

Положення про права і свободи, установлені Європейською конвенцією про захист прав людини і основоположних свобод і в ст. 19 Міжнародного пакту про громадянські і політичні права, застосовуються як в режимі онлайн, так і офлайн.

Також вводить принципі Вільного транскордонного руку інформації в Інтернеті, а саме :

1) Принцип належної обачності;

2) Принцип Цінності саморегуляції;

3) Принцип Просування передового технічного досвіду;

4) Принцип Міжнародного діалогу та політики;

А також стверджує та вводить загальні принципи:

«1.1. Держави зобов'язані гарантувати кожній людині, яка перебуває під їхньою юрисдикцією, право на свободу вираження поглядів та право на свободу зборів та об'єднань у повній відповідності до статей 10 та 11 ЄКПЛ, які однаково застосовуються до Інтернету. Ці права та свободи повинні бути гарантовані без будь-якої дискримінації за ознакою статі, сексуальної орієнтації, раси, кольору шкіри, мови, релігії, політичних чи інших переконань, національного чи соціального походження, належності до національної меншини, майнового стану, народження чи іншого статусу.

1.2. Держави повинні захищати та заохочувати глобальний вільний потік інформації в Інтернеті. Вони повинні гарантувати, що втручання в інтернет-трафік на їх території переслідує законні цілі, викладені у статті 10 ЄКПЛ та інших відповідних міжнародних угодах, і не має непотрібного

чи непропорційного впливу на транскордонний потік інформації в Інтернеті» [128].

Через недосконаліть та фрагментарність законодавчої бази в галузі регулювання цифрового простору, а також внаслідок відсутності чітко визначених юридичних критеріїв і стандартів застосування обмежувальних заходів, у сфері забезпечення свободи слова відбуваються серйозні порушення, що набувають форми або необґрунтовано надмірного обмеження і фільтрації інформаційного контенту, або ж, навпаки, здійснення таких обмежень для досягнення цілей, які не мають чіткого правового обґрунтування чи не пов'язані з необхідністю гарантування суспільної безпеки та національних інтересів.

Подібна ситуація породжує численні загрози для реалізації основоположних прав людини, зокрема, права на вільне вираження поглядів, що є фундаментальною основою демократичного суспільства.

Тому існує нагальна потреба у виробленні чітких, об’єктивних та прозорих юридичних критеріїв, які дозволили б ефективно й обґрунтовано здійснювати диференціацію інформації та визначати межі допустимого втручання у сферу свободи вираження поглядів.

Важливим аспектом такого підходу має стати чітке визначення законодавцем переліку легітимних цілей, досягнення яких може бути підставою для обмеження або блокування доступу до інформації в мережі Інтернет. Також важливо закріпити механізми контролю та нагляду за законністю та обґрунтованістю застосування таких обмежень, забезпечивши ефективний судовий і громадський контроль за їх реалізацією.

Запровадження зазначених змін на рівні законодавства сприятиме не лише забезпеченню права на свободу слова, але й дозволить уникнути свавільних обмежень свободи інформаційного обміну, що відповідає міжнародним стандартам прав людини та принципам демократичного правління.

У Рекомендації № CM/Rec (2014) 6 Комітету міністрів Ради Європи «Про Керівництво з прав людини для користувачів Інтернету» [127] вказується, що обмеження можуть застосовуватися до вираження думок, в яких міститься заклик до дискримінації, ненависті або насильства.

Ці обмеження повинні бути законними, мати вузькоспрямований характер і виконуватися під наглядом суду; органи державної влади зобов'язані поважати і захищати свободу вираження думок і свободу інформації, будь-які обмеження цієї свободи не повинні бути довільним і повинні переслідувати законні цілі у відповідності з Європейською конвенцією про захист прав людини і основоположних свобод.

Крім того, вони повинні бути доведені до громадян разом з інформацією про те, як отримати консультації та відновити себе в цих правах, не повинні бути ширше або застосовуватися набагато довше, ніж це необхідно для досягнення законної мети [165, с. 55].

Аналізуючи право на свободу слова в контексті міжнародних і національних правових актів, необхідно зазначити, що, попри чіткі формулювання та універсальність, у практичному вимірі дане право часто стикається із суттєвими обмеженнями, особливо у цифровому просторі.

Сучасний Інтернет-простір, який створювався як інструмент вільного обміну інформацією та ідеями, все частіше стає ареною боротьби між правом на свободу вираження думок та спробами різних державних органів і приватних компаній здійснювати контроль за інформаційними потоками.

Процеси обмеження свободи слова в Інтернеті зазвичай проявляються у таких формах, як цензура, блокування веб-сайтів, обмеження доступу до соціальних мереж чи блог-платформ, фільтрація контенту, впровадження обов'язкових заходів ідентифікації користувачів, а також переслідування осіб, що висловлюють погляди, які суперечать офіційній позиції держави. У низці країн, включаючи й Україну, такі обмеження нерідко аргументуються міркуваннями національної безпеки, захисту суспільної моралі чи боротьбою із дезінформацією та пропагандою.

Особливо загрозливими стають процеси придушення інакомислення, коли державні або приватні структури використовують інструменти контролю Інтернету з метою не лише обмеження поширення певного контенту, а й повного блокування альтернативних думок чи критики на свою адресу. Такі дії мають потенціал підривати демократичні принципи, що закріплені у згаданих міжнародних документах, а також у Конституції України, і можуть призводити до суттєвого погіршення стану свободи слова та розвитку суспільства загалом.

Отже, у контексті описаних нормативних актів, особливого значення набуває необхідність ефективної та прозорої регламентації процесів, пов’язаних з обмеженням свободи вираження думок у мережі Інтернет. З одного боку, державі необхідно забезпечити баланс між захистом суспільних інтересів та національної безпеки, а з іншого – гарантувати реалізацію права на свободу слова, уникаючи надмірного або необґрунтованого обмеження цього фундаментального права. Тому сьогодні надзвичайно важливим є встановлення чітких юридичних меж таких обмежень, що відповідатимуть стандартам міжнародного права та запобігатимуть свавільному придушенню інакомислення у цифрову епоху.

Основними законодавчими актами, що регулюють сферу Інтернету в Україні, є:

1. Закон України «Про телекомунікації»: Цей закон визначає повноваження держави щодо управління та регулювання телекомунікаційної діяльності, а також права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у цій діяльності [120].

2. Закон України «Про основні засади забезпечення кібербезпеки України». Цей закон встановлює правові та організаційні основи захисту життєво важливих інтересів людини і громадянина, суспільства та держави у кіберпросторі, визначає основні цілі, напрями та принципи державної

політики у сфері кібербезпеки, а також повноваження державних органів, підприємств, установ, організацій та громадян у цій сфері [113].

Однак, жоден із цих законів не містить чіткого переліку інформації, доступ до якої заборонений, або критеріїв, за якими повинна здійснюватися фільтрація Інтернет-контенту.

Відсутність чітких законодавчих критеріїв та визначеного переліку інформації, доступ до якої має бути обмежений у мережі Інтернет, створює потенційну загрозу для прав людини і свободи слова в Україні.

В умовах, коли норми, що регулюють сферу цифрового контенту, допускають неоднозначне трактування, відкривається простір для зловживань з боку органів влади або інших суб'єктів, які мають змогу довільно інтерпретувати законодавство, часто керуючись політичними чи іншими мотивами.

Така ситуація посилює загрози надмірного обмеження та фільтрації інформації, яка може бути незручною для владних структур або тих, хто має важелі впливу. Унаслідок цього спостерігається тенденція до придушення інакомислення через необґрунтоване блокування Інтернет-ресурсів, що суперечить базовим демократичним принципам. Відсутність прозорості в застосуванні таких заходів знижує можливості громадськості та незалежних інститутів ефективно оскаржувати подібні рішення та здійснювати контроль за діями держави у сфері цифрових комунікацій.

Таким чином, нагальною є потреба у розробленні чітких, прозорих і доступних законодавчих критеріїв, які б визначали, яка саме інформація підлягає обмеженню, та у яких випадках це виправдано. Це дозволить забезпечити більш справедливий баланс між потребою у захисті національної безпеки, прав інших осіб та основоположним правом на свободу слова, зменшуючи при цьому ймовірність довільного придушення інакомислення в Інтернет-просторі.

Згідно із щорічними звітами міжнародної правозахисної неурядової організації FreedomHouse «Freedom on the net», Україна визнається «partly

free/частково вільною» за рівнем свободи Інтернету у 2024 році, Україна отримала 59 балів із 100.

У звіті звертається увага на те, що «за останнє десятиліття Україна провела низку реформ для вирішення таких проблем, як поширена корупція, політизована судова система та напади на журналістів, активістів та представників етнічних та інших меншин» [217].

Враховуючи події з 2022 року, а саме повномасштабне вторгнення РФ на території України, а також урядові блокування багатьох російських та проросійських веб-сайтів, які пов’язані з поширенням наративів з боку держави-агресора. Freedom House вважає, що фактична реалізація блокування веб-сайтів була непослідовною, заперечувалося в суді, і ніколи не контролювалися належним чином.

Також, посилаючись на власні розслідування, організація стверджує :

«Уряд іноді передає контент третім особам, вимагаючи його видалення. Протягом періоду висвітлення соціальні медіа-платформи та пошукові системи також видаляли неавтентичний контент у відповідь на російське військове вторгнення в Україну» [217]. «Відразу після повномасштабного вторгнення Росії в Україну 24 лютого 2022 року Уряд України також безпосередньо втрутився у приватний медіапростір. Три найбільші приватні медіа-організації (StarLightMedia, 1+1 медіа та Inter Media Group) приєдналися до суспільних мовників UA:Перший та Українського радіо для забезпечення єдиного цілодобового висвітлення подій в рамках проекту «*Єдині новини*» [34, с.76].

Організація FreedomHouse вважає, що більшість заборон та обмежень, які існують на сьогоднішній стан продиктовано, саме існуючою повномасштабною агресією з боку РФ, наявністю корупції та політичного втручання в українські суди, які підривають здатність до захисту основних прав громадян.

Питання реалізації та обмеження права на свободу слова у мережі Інтернет є актуальним і актуалізується не лише в українських реаліях, а й у

світовому масштабі. Проблематика регулювання Інтернет-простору та відповідні правові підходи до обмеження контенту безпосередньо пов’язані з рівнем демократичного розвитку суспільства, гарантіями забезпечення прав і свобод людини та історико-культурними особливостями тієї чи іншої держави.

Сполучені Штати Америки є федеративною республікою, державно-політичний устрій якої заснований на демократичних принципах народного суверенітету та плюралістичної політичної системи, що забезпечує динамічну конкуренцію між різноманітними політичними силами. У цій державі традиційно міцно укорінені основи верховенства права, що виражається у безумовному дотриманні закону та незалежності судової системи. Значне значення приділяється свободі вираження поглядів, що гарантується

Першою поправкою до Конституції США проголошувалися загальні свободи громадян, а також свобода релігійних переконань, яка захищається на державному та федеральному рівнях. Крім того, громадяни США мають змогу користуватися широким спектром інших фундаментальних громадянських свобод і прав, таких як свобода зібрань, свобода друку, право на приватність та право на захист від необґрунтованих втручань держави в особисте життя [218].

Ці особливості політико-правової системи США створюють сприятливе середовище для активного громадянського суспільства, сприяють відкритості та прозорості влади, а також забезпечують високий рівень захисту індивідуальних прав і свобод кожного громадянина, що, своєю чергою, є фундаментальною передумовою стабільного демократичного розвитку суспільства та держави загалом. Досліджуючи та аналізуючи стан розвитку США FreedomHouse пише : «Проте в останні роки її демократичні інститути зазнали ерозії, що знайшло відображення в зростаючій політичній поляризації та екстремізмі, партійному тиску на виборчий процес, поганому поводженні та дисфункції в системах

кримінального правосуддя та імміграції, а також зростаючій нерівності в багатстві, економічних можливостях та політичному впливі» [218].

Інтернет-простір у Сполучених Штатах Америки протягом тривалого часу зберігав свою яскравість, різноманітність контенту, а також загалом високий ступінь свободи та незалежності. Це значною мірою забезпечувалось завдяки наявності потужної правової бази, фундаментом якої є Перша поправка до Конституції США, що закріплює один із найсильніших у світі стандартів захисту свободи слова, включно зі свободою вираження поглядів у цифровому середовищі.

Незважаючи на це, останніми роками зросло занепокоєння через стрімке поширення помилкового, неправдивого, оманливого та конспірологічного контенту, що суттєво погіршує якість інформаційного середовища, підриває довіру громадян до демократичних інститутів та створює серйозні виклики, особливо напередодні важливих політичних подій, таких як вибори Президента США у листопаді 2024 року. Саме масова поява і швидке поширення фейків та маніпулятивної інформації в соціальних мережах призводить до створення атмосфери інформаційної ненадійності та дезінформації, що негативно впливає на суспільно-політичну стабільність.

Окрім цього, у Сполучених Штатах, як і раніше, зберігається серйозна прогалина в регулюванні конфіденційності персональних даних громадян, адже донині в країні відсутній єдиний, всеосяжний федеральний закон, який би комплексно регламентував питання приватності та забезпечував захист персональних даних користувачів Інтернету [218]. Конгрес США так і не здійснив необхідних реформ застарілої нормативно-правової бази щодо практик державного та приватного стеження, що дозволяє й надалі застосовувати недостатньо прозорі або навіть незаконні методи збору, обробки та зберігання персональних даних.

Така ситуація викликає постійну критику з боку правозахисних організацій та громадських активістів, які наполягають на необхідності

забезпечення більш високих стандартів захисту приватності громадян. В умовах затягування законодавчого процесу на федеральному рівні, уряди окремих штатів все активніше беруть на себе ініціативу щодо правового регулювання цифрового середовища, зокрема, ухвалюючи законодавчі акти, спрямовані на регулювання діяльності соціальних мереж, посилення відповідальності онлайн-платформ за поширення дезінформації, а також встановлення чітких норм щодо захисту конфіденційності персональних даних користувачів. Це свідчить про наростаючу потребу у більш гнучких і ефективних підходах до правового регулювання Інтернет-простору, які б відповідали сучасним викликам та тенденціям, і водночас не призводили до надмірного обмеження основоположних свобод громадян, зокрема свободи слова.

Повноваження державних органів США щодо проведення обшуку, вилучення майна та здійснення заходів спостереження за громадянами, як правило, обмежуються нормами Четвертої поправки до Конституції США, яка гарантує право людини на недоторканність особистого життя та житла, а також захист від необґрунтованих обшуків і конфіскацій майна [162]. Проте, попри наявність конституційних обмежень, на практиці правова основа, яка регулює сферу урядового нагляду та контролю за комунікаціями, залишається досить широкою, неоднозначною та відкритою для різного роду зловживань з боку органів державної влади.

Особливо актуальним це питання постає у контексті моніторингу соціальних мереж, де органи державної влади досить активно здійснюють збір інформації з мінімальним зовнішнім контролем, недостатньою прозорістю процедур та обмеженим громадським наглядом. Закони, що регулюють заходи зі спостереження, які проводяться американськими спецслужбами в інтересах іноземної розвідки, також мають певні прогалини, що на практиці дозволяють здійснювати збір та накопичення персональних даних не лише іноземців, але й громадян і постійних резидентів США.

Важливою правовою основою для таких заходів став Закон USA PATRIOT Act, ухвалений у 2001 році після терористичних атак 11 вересня, який суттєво розширив повноваження правоохоронних і розвідувальних органів щодо доступу до персональної інформації, телефонних розмов та електронних комунікацій громадян. Іншим ключовим нормативним актом, який регулює питання державного контролю комунікацій, є Закон США про свободу слова (USA FREEDOM Act) [277]. Згідно з цим законом, Агентство національної безпеки США (АНБ), яке займається збором інформації в інтересах зовнішньої розвідки, має право отримувати доступ до записів телефонних розмов, що зберігаються у базах даних телефонних компаній США.

Проте така процедура можлива лише за умови отримання спеціальної судової ухвали від Суду з нагляду за іноземною розвідкою (FISA Court) [213], створеного згідно із Законом про зовнішню розвідку (Foreign Intelligence Surveillance Act, FISA). Втім, на практиці цей суд зазнає значної критики через низький рівень прозорості та обмеженість механізмів громадського контролю за його діяльністю. Особливо варто наголосити на поширенні серед американських правоохоронних органів спеціальних технічних пристроїв, відомих як симулятори стільникових станцій або пастки IMSI (International Mobile Subscriber Identity), більш широко відомі під загальною назвою «скати» (за назвою одного з найпоширеніших брендів – «Stingray»). Ці пристрої здатні імітувати функції веж стільникового зв'язку, змушуючи мобільні телефони, що знаходяться у зоні їхнього покриття, передавати власну ідентифікаційну інформацію правоохоронним органам.

В результаті такої технології поліція отримує можливість не лише стежити за переміщеннями та діями конкретних осіб, але й отримувати інформацію про всіх людей, які перебувають у межах певної території, навіть якщо вони не є об'єктами конкретного кримінального розслідування. Використання таких технологій викликає активні дискусії в суспільстві,

оскільки межі між законними цілями державного нагляду та масовим порушенням права на приватність у цьому випадку стають досить розмитими.

Отже, хоча в США існують досить серйозні конституційні гарантії щодо захисту приватності, законодавчі прогалини та практика державних органів створюють загрози зловживання повноваженнями і викликають занепокоєння громадськості щодо збереження фундаментальних прав та свобод людини в умовах дедалі більшого технологічного розвитку засобів спостереження та моніторингу.

В умовах сучасної КНР громадяни регулярно зазнають серйозних правових та позаправових репресій, переслідувань та санкцій за їхню активність у цифровому просторі, яка в демократичних країнах зазвичай визнається цілком законною. Упродовж останнього десятиліття китайські інтернет-користувачі зіштовхнулися з безпрецедентними та найсуворішими у світі обмеженнями щодо інтернет-свободи. Зокрема, під ризиком перебувають особи, що займаються обміном новинами, висловлюють свої політичні та релігійні погляди, дискутують на чутливі для уряду теми, а також здійснюють комунікацію з членами родини чи іншими людьми, які проживають за кордоном.

Подібні дії можуть призводити до адміністративних штрафів, ув’язнення, або навіть до позасудового переслідування. Китайська влада має майже необмежені можливості та впливові механізми для контролю над інтернет-простором та технологічним сектором країни.

Регулярно використовуються такі засоби, як державні перевірки, розслідування, адміністративні санкції, а також жорсткі вимоги щодо видалення інформації, яка суперечить офіційним державним наративам або може підривати авторитет Комуністичної партії. Такі заходи дозволяють забезпечити повну відповідність поведінки технологічних компаній урядовим установкам та створюють атмосферу страху й самоцензури серед інтернет-користувачів, медіа-платформ, блогерів і приватних осіб.

Внаслідок цього цифровий простір Китаю характеризується надзвичайно низьким рівнем плюралізму та критичного обговорення суспільно-політичних питань, що має далекосяжні негативні наслідки для прав людини, свободи слова і вільного доступу до інформації. Інтернет-сектор Китаю уживається зі складною системою цензури, що складається з трьох базових елементів:

1) система фільтрації трафіка «Золотий щит» (вона ж «Великий китайський фаєрвол»);

2) система блокування пошуку небажаної інформації;

3) ручна система фільтрації контенту, що публікується в соціальних мережах і блогосфері.

Постійне блокування стосується найбільш чутливих тем, пов'язаних із критикою Комуністичної партії Китаю й питанням прав людини. «Приклади постійно заблокованих ключових слів: «*демократія*», «*диктатура*», «*мітинг*», «*червоний терор*», «*незалежність Тибету*», «*репресії*» тощо. Тимчасовому блокуванню піддаються слова й фрази, пов'язані з обмеженими в часі кризовими ситуаціями, незалежно від їх характеру. Може йтися про політичні виступи, екологічні лиха або корупційні скандали» [165, с.57].

Процеси обмеження свободи слова в Інтернеті та придушення інакомислення є однією з ключових загроз сучасному демократичному суспільству, оскільки вони безпосередньо зачіпають фундаментальні права людини. Поширення Інтернету призвело до того, що традиційні механізми державного контролю інформації стали менш ефективними, що змусило деякі держави шукати нові шляхи контролю інформаційних потоків, які нерідко призводять до порушення міжнародних стандартів свободи вираження поглядів.

На прикладі України ми бачимо, що відсутність чітких законодавчих критеріїв для обмеження Інтернет-контенту створює підґрунтя для зловживань з боку влади, що проявляється у вибірковості блокуванні,

недостатній прозорості рішень та потенційному придушенні критики й інакомислення. Хоча частина цих обмежень може мати обґрунтування в умовах національної безпеки, особливо під час воєнного стану та повномасштабного вторгнення з боку РФ, існує ризик виходу таких заходів за межі необхідності, що потенційно може призвести до зменшення рівня демократичних свобод у майбутньому.

Водночас, досвід США демонструє іншу проблему – навіть за наявності потужних конституційних гарантій свободи слова, держава продовжує використовувати технології спостереження за громадянами, що суттєво знижує рівень приватності і конфіденційності. Прогалини в американському законодавстві щодо захисту приватності та недостатня прозорість у діях державних органів також породжують загрози для демократичних свобод, посилюючи атмосферу суспільної недовіри та політичної напруги.

Найбільш жорстким та тривожним прикладом є Китай, де обмеження свободи слова набули системного характеру. Запроваджені державою механізми інтернет-цензури є не просто інструментом контролю за інформацією, але й засобом широкомасштабного придушення інакомислення та будь-якої критики влади. Це призводить до створення тоталітарної інформаційної реальності, у якій права людини стають жертвами політичної стабільності та контролю за суспільством. Отже, у глобальному масштабі ситуація зі свободою слова в Інтернеті потребує серйозного перегляду та посилення міжнародних механізмів захисту.

Україна, у свою чергу, повинна ретельно зважити загрози надмірних обмежень, навіть у ситуаціях кризового характеру, аби уникнути поступового руху до авторитарних практик. Забезпечення прозорості, чіткості та правової визначеності у сфері цифрових комунікацій є ключовим кроком для захисту демократичних цінностей та гарантії прав людини в умовах інформаційної епохи.

2.3. Технологічні корпорації як суб’єкти політичного впливу в умовах трансформації режимів інформаційного управління

Цифровий тоталітаризм представляє собою серйозну загрозу для сучасного суспільства та демократичних цінностей. У цьому підрозділі розглядається роль технологічних корпорацій, їхню роль в процесах сприяння та протидії цифровому тоталітаризму, як суб’єктів політичного впливу. Зокрема, приділено увагу впливу технологічних корпорацій на збереження особистих даних, свободу слова та інші аспекти цифрового тоталітаризму та пропонуються шляхи подолання цих проблем. З появою і поширенням цифрових технологій стало можливим збільшення кількості інформації, яка зберігається та обробляється в мережі. Однак цей процес також створює потенціал для зловживання та порушення прав людини, включаючи право на приватність та свободу слова.

Цифровий тоталітаризм – це феномен, в якому уряди або інші суб'єкти намагаються контролювати та обмежувати доступ до інформації та здійснювати масовий нагляд над громадянами через цифрові технології. Цифровізація світу безперечно змінила наше життя. Інтернет, смартфони, соціальні мережі і розширена реальність стали невід’ємною частиною нашого повсякденного існування. Проте, разом з безліччю нових можливостей, які нам принесла ця цифрова революція, виникли і серйозні питання стосовно збереження особистих даних.

Важливість особистих даних в сучасному світі не може бути недооціненою. Інформація про наші інтереси, звички, фізичний стан, географічне положення, і навіть наші думки і переконання стали об'єктом збору та обробки. Ця інформація використовується для багатьох цілей, включаючи маркетинг, аналітику, персоналізацію послуг і багато іншого.

Однак це створює проблему забезпечення конфіденційності та безпеки цих даних. Історії про витоки даних, хакерські атаки та недбале

ставлення до особистих даних свідчать про необхідність ретельного контролю за цією цінною інформацією. З одного боку, технологічні корпорації можуть сприяти поширенню практик цифрового тоталітаризму, якщо вони погоджуються на співпрацю з авторитарними режимами чи урядами, що прагнуть контролювати цифровий простір. Наприклад, компанії, які створюють технології для розпізнавання обличчя, аналітики даних чи соціального моніторингу, можуть використовуватися для стеження за населенням.

Китайська Народна Республіка активно впроваджує цифрові технології для посилення державного контролю над суспільством, що проявляється через кілька ключових механізмів. «Великий китайський брандмауер» (Great Firewall of China): Ця система інтернет-цензури блокує доступ до багатьох іноземних веб-сайтів та соціальних мереж, включаючи Google, Facebook, YouTube та Twitter. Метою є обмеження впливу зовнішньої інформації на громадян та контроль над внутрішнім інформаційним простором. Згідно зі звітом, «уряд блокує та фільтрує вихід країни до глобального Інтернету» за допомогою цієї системи [157].

Система соціального кредиту (Social Credit System). Ця система оцінює поведінку громадян та організацій, присвоюючи їм рейтинги на основі їхньої соціальної та економічної діяльності. Високий рейтинг відкриває доступ до різних привілеїв, тоді як низький може призвести до обмежень, таких як заборона на подорожі або обмеження в доступі до певних послуг. Наприклад, громадяни з низьким рейтингом можуть бути обмежені в можливості користуватися поїздами, літаками та іншими базовими потребами [131].

Моніторинг через цифрові платформи. Китайські платформи, такі як WeChat та Alipay, інтегровані в єдину систему контролю, де здійснюється автоматичний збір та аналіз інформації про поведінку користувачів. Це дозволяє державі відстежувати фінансові транзакції, комунікації та інші аспекти повсякденного життя громадян, створюючи базу для потенційних

репресій проти тих, хто відхиляється від державної ідеології чи правил суспільної поведінки.

Ці механізми демонструють, як цифрові технології можуть бути використані для встановлення тотального контролю над суспільством, обмежуючи особисті свободи та права громадян. Яскравим прикладом також є діяльність китайської компанії Hikvision, яка була заснована в 2001 році. Вона є одним із провідних світових виробників обладнання для відеоспостереження. Її продукція широко використовується в різних країнах для забезпечення безпеки та моніторингу. У Сіньцзяні, автономному регіоні на заході Китаю, проживає значна кількість мусульман-уйгурів та інших етнічних меншин. З 2017 року з'явилися численні повідомлення про масові затримання понад мільйона уйгурів у так званих «таборах перевиховання» без належних судових процедур. У цих таборах, за свідченнями очевидців, відбуваються серйозні порушення прав людини, включаючи примусову працю, обмеження релігійних практик та інші форми репресій [157]. Технології відеоспостереження Hikvision, зокрема камери з функцією розпізнавання обличчя, були встановлені по всьому Сіньцзян-Уйгурському автономному району (СУАР), включаючи мечеті та інші громадські місця.

Ці системи використовуються для масового стеження за населенням, що дозволяє владі відстежувати та контролювати пересування та діяльність уйгурів. Зокрема, система IJOP (Integrated Joint Operations Platform), яку використовує поліція СУАР, відстежує взаємодію людей та визначає підозрілі дії на основі широких та сумнівних критеріїв, таких як подорожі до певних країн або спілкування з особами, які мають «підозрілий» статус [163].

У відповідь на повідомлення про використання технологій Hikvision для порушення прав людини, низка країн та організацій вжили заходів проти компанії. У 2019 році уряд США вніс Hikvision до Entity List", що обмежує американським компаніям постачання компонентів та технологій для Hikvision без спеціального дозволу. Це рішення було обґрунтоване

роллю Hikvision у спостереженні за уйгурами та іншими етнічними та релігійними меншинами в Китаї [278]. Крім того, у 2021 році Європейський парламент вилучив камери Hikvision зі своїх приміщень, посилаючись на неприйнятний ризик того, що компанія, через свою діяльність у СУАР, сприяє серйозним порушенням прав людини [231].

Діяльність Hikvision у Сіньцзяні-Уйгурскому автономному районі є яскравим прикладом того, як технологічні компанії можуть бути залучені до порушень прав людини через постачання обладнання для масового спостереження. Міжнародна спільнота продовжує уважно стежити за такими випадками, наголошуючи на необхідності дотримання етичних стандартів та прав людини у сфері технологій [174].

Huawei, одна з провідних світових компаній у сфері телекомунікацій, зіткнулася з численними звинуваченнями щодо потенційних загроз національній безпеці через можливість вбудованих механізмів контролю в її обладнанні. Декілька країн висловили побоювання, що використання технологій Huawei може надати можливість для несанкціонованого доступу або шпигунства з боку іноземних держав. Наприклад, у 2020 році Велика Британія офіційно заявила про вилучення обладнання компанії Huawei у розбудові своєї 5G-інфраструктури, посилаючись на загрози для національної безпеки. Подібні рішення ухвалили й інші країни, включаючи США, Австралію та Канада, які обмежили або повністю заборонили використання обладнання Huawei у своїх телекомунікаційних мережах [231].

З іншого боку, технологічні корпорації також мають потенціал відігравати активну роль у протидії цифровому тоталітаризму. У сучасному цифровому середовищі технологічні корпорації відіграють вирішальну роль у забезпеченні балансу між підтримкою свободи слова, захистом приватності користувачів та виконанням вимог державних органів.

Компанія Apple є яскравим прикладом корпорації, яка активно відстоює права своїх користувачів, зокрема у питаннях шифрування даних

та доступу до них з боку урядових структур. У лютому 2025 року уряд Великої Британії, посилаючись на Закон про слідчі повноваження (Investigatory Powers Act), звернувся до Apple з вимогою створити «бекдор» – спеціальний доступ для правоохоронних органів — до зашифрованих даних користувачів iCloud. Це вимагало від Apple надати можливість доступу до особистих даних користувачів навіть при використанні наскрізного шифрування. У відповідь Apple прийняла рішення видалити функцію Advanced Data Protection (ADP) для користувачів у Великій Британії, яка забезпечувала наскрізне шифрування даних в iCloud. Цей крок дозволив компанії уникнути створення «бекдору», але водночас зробив дані користувачів більш вразливими до потенційних порушень безпеки та несанкціонованого доступу [271].

Дії уряду Великої Британії викликали критику з боку міжнародної спільноти. Директор національної розвідки США Тулсі Габбард засудила вимогу британського уряду, назвавши її порушенням приватності та громадянських свобод американців. «Будь-який обмін інформацією між урядом – будь-яким урядом та приватними компаніями повинен здійснюватися таким чином, щоб поважати та захищати закони США та конституційні права громадян США» [271]. Вона підкреслила, що такі вимоги суперечать двосторонній угоді між США та Великою Британією щодо обміну даними, відомій як Cloud Act, яка забороняє подібні вимоги стосовно даних резидентів США.

З іншого боку, існують приклади діяльності корпорації Meta (Facebook). У 2016 році, ця компанія опинилась в масштабному скандалі через справу «*Cambridge Analytica*», яка використовувала персональні дані мільйонів користувачів без їхньої згоди для мікротаргетингу політичної реклами. «Через компанію Global Science Research (GSR) у співпраці з Cambridge Analytica сотні тисяч користувачів отримали гроші за проходження тесту на особу та погодилися на збір своїх даних для академічного використання» [256].

Остані дані автоматично передавались на сайт Facebook, що надало можливості отримати дані понад 50 мільйонів зареєстрованих виборців США. Це дозволило створювати персоналізовані повідомлення, що маніпулювали емоціями користувачів для впливу на їхню політичну поведінку під час президентських виборів у США. Цей випадок підкреслює необхідність чіткого законодавчого врегулювання питань доступу до зашифрованих даних, яке б враховувало як потреби національної безпеки, так і фундаментальні права на приватність. Важливо, щоб такі рішення приймалися з урахуванням думки громадськості, експертів та правозахисних організацій, забезпечуючи баланс між безпекою та свободою в цифрову епоху. Всесвітньо відома технологічна корпорація

Компанія «Google» традиційно вважається головним розподільником інформації у мережі Інтернет. Їхні алгоритми ранжування визначають, яку інформацію бачать користувачі першою. У кількох дослідженнях (зокрема, Harvard’s Berkman Klein Center) зазначено, що Google може непропорційно просувати або знижувати видимість певних політичних джерел, формуючи громадське сприйняття через приховані механізми [248].

Найпопулярніша платформа серед молоді «TikTok», яка знаходиться під контролем з боку китайської материнської корпорації «ByteDance», неодноразово звинувачувався в прихованій модерації контенту, критичного до КНР, а також у використанні алгоритмів для пріоритизації розважального або деполітизованого контенту. Так, наприклад, уряди США, та низки європейських країн висловлювали занепокоєння, що додаток може слугувати інструментом політичного впливу, цифрового шпигунства, розповсюдження *залежності* у дітей та підлітків через надмірне використання додатку, пропагації розладу харчової поведінки, вживання тютюну, ідей самогубства, збіру та продажу даних [241].

Іран активно впроваджує цифрові тоталітарні методи, використовуючи сучасні інформаційні технології власних корпорацій для контролю та цензури інтернет-простору. Цей процес є частиною загальної

політики іранського уряду, спрямованої на обмеження доступу громадян до інформації та посилення моніторингу їхньої поведінки онлайн.

Іранській досвід показує нам неймовірні масштаби цензурування Інтернету, блокуючи численні міжнародні інформаційні ресурси та популярні соціальні мережі, такі як Facebook, Twitter, YouTube, Telegram, WhatsApp та Instagram. Ця цензура зазвичай посилюється під час періодів політичної нестабільності чи масових протестів. Так, наприклад, під час протестних акцій у 2019 році влада Ірану повністю обмежила доступ до Інтернету по всій країні, щоб зупинити поширення інформації та перешкодити громадянам координувати протестні дії [235].

Іранські спецслужби широко використовують технології підвласних корпорацій для глибокого інтернет-моніторингу, щоб контролювати соціальні мережі та виявляти політичних активістів, опозиційних журналістів і звичайних громадян, що висловлюють незгоду з офіційною політикою держави. Для цього використовується низка спеціальних програм і алгоритмів, які здатні аналізувати трафік даних, електронну пошту, повідомлення в соціальних мережах, а також визначати місцезнаходження користувачів. Зокрема, було повідомлено про використання іранським урядом систем DPI (Deep Packet Inspection), які дозволяють детально аналізувати трафік та блокувати небажаний контент.

Використовуючи зібрані в результаті моніторингу інформацію, іранська влада, проводить масштабні кампанії репресій проти дисидентів, журналістів та громадських активістів. Існують численні випадки арештів і засудження активістів за пости та коментарі в соціальних мережах. Зокрема, такі звинувачення, як «антидержавна пропаганда», «розповсюдження дезінформації» та «загроза національній безпеці», активно застосовуються для ув’язнення або інших форм переслідування громадян, що виражають критичні думки в Інтернеті [235].

Таким чином, цифрові тоталітарні тенденції в Ірані набувають яскраво вираженого характеру завдяки широкому застосуванню методів цифрової

цензури та моніторингу онлайн-активності, що є частиною систематичного підходу держави до контролю над інформаційним простором і свободою слова.

Туркменістан є однією з найбільш закритих країн світу щодо доступу до інформації та свободи Інтернету. Державна політика спрямована на суворий контроль інтернет-простору, що виражається в масштабній цензурі та обмеженні доступу до іноземних ресурсів. У Туркменістані доступ до багатьох популярних міжнародних веб-сайтів та соціальних мереж, таких як YouTube, Facebook, Twitter та LiveJournal, заблокований. Також обмежено доступ до месенджерів WhatsApp, WeChat та Viber. Крім того, багато іноземних компаній, що працюють у Туркменістані, втратили доступ до своїх корпоративних мереж через ці обмеження [13].

Ця політика спрямована на запобігання поширенню інформації, яка може бути критичною щодо уряду або суперечити офіційній державній ідеології. Окрім блокування популярних сайтів та сервісів, влада Туркменістану активно протидіє використанню технологій обходу цензури, таких як VPN та анонімайзери. З 2012 року почалась активна та велика кампанія по блокуванню багатьох анонімайзерів, а також активно блокуються VPN-сервіси. Користувачів, які намагаються обійти ці обмеження, можуть викликати до правоохоронних органів для проведення «профілактичних бесід» та оштрафувати на суму близько 350 манатів (приблизно 100 доларів США). У деяких випадках у громадян Туркменістану, які бажають підключитися до Інтернету, вимагають присягнути на Корані, що вони не будуть використовувати VPN [13].

Такі суворі обмеження значно звужують можливості громадян отримувати об'єктивну інформацію з незалежних джерел, обмежують свободу вираження думок та перешкоджають розвитку громадянського суспільства. Це призводить до ізоляції країни на міжнародній арені та обмежує можливості для соціально-економічного розвитку.

Таким чином, політика Туркменістану щодо контролю Інтернету є прикладом цифрового тоталітаризму, де державна влада використовує технологічні засоби для обмеження свободи інформації та контролю над суспільством. У сучасних умовах світової економіки суттєво посилюється значення соціальних та «хмарних» технологій, які стають одними з визначальних факторів розвитку інформаційної інфраструктури корпоративного сектору.

Активне впровадження цих технологій забезпечує не лише значну оптимізацію внутрішніх бізнес-процесів, але й формує новий тип взаємодії між суб'єктами господарювання та їхніми клієнтами, забезпечуючи швидку адаптацію до змін ринкового середовища, а також дозволяє створити більш динамічні, інтегровані та інноваційні моделі ведення бізнесу.

У свою чергу, застосування хмарних сервісів надає компаніям можливість ефективно знижувати витрати на підтримку власної інфраструктури, спрощує процедуру доступу до великих обсягів даних та полегшує організацію процесів комунікації як всередині підприємств, так і з клієнтами й партнерами. Водночас соціальні технології та платформи, що базуються на принципах Web 2.0 та Web 3.0, змінюють саму природу корпоративних комунікацій, роблячи їх більш відкритими, прозорими та інтерактивними.

У контексті цього цифровізація економіки та політичного простору передбачає комплексну перебудову всіх виробничих та управлінських процесів підприємств із застосуванням сучасних інформаційних рішень. Це сприяє переходу від статичних, ієрархічних організаційних структур до гнучких і адаптивних моделей, здатних ефективно реагувати на економічні виклики сьогодення, швидко змінюватися відповідно до потреб споживачів, а також реалізовувати персоналізовані стратегії взаємодії з клієнтами.

Головною метою таких трансформацій є формування висококонкурентної цифровізованої економіки, яка здатна забезпечити

стійке економічне зростання держави та ефективне функціонування корпоративного сектора у глобальному інформаційному просторі.

При цьому отримання очікуваних результатів цифровізації залежить не лише від технологічних інновацій, але й від їхнього правильного та етичного впровадження, захисту цифрових прав людини, гарантування кібербезпеки та попередження цифрових загроз, включаючи прояви цифрового тоталітаризму, монополізації цифрових ресурсів і порушення приватності.

Саме тому ключовими завданнями стають формування відповідної правової бази, створення механізмів захисту персональних даних, прозоре регулювання технологічного ринку, а також розвиток цифрових навичок і компетенцій громадян, що забезпечуватиме сталий розвиток цифрової економіки з урахуванням суспільних інтересів та міжнародних стандартів.

Цифрові тоталітарні тенденції, які сьогодні поширюються у різних державах світу, становлять серйозну загрозу фундаментальним громадянським свободам, правам людини та принципам демократичного управління. Ці тенденції виявляються через дедалі активніше застосування державами технологічних інструментів, що дозволяють контролювати інформаційний простір, обмежувати свободу слова та вираження поглядів, здійснювати масовий моніторинг приватних комунікацій громадян, а також обмежувати доступ до інформаційних ресурсів через різноманітні механізми цифрової цензури.

Наслідком таких дій є звуження простору громадянської активності, самоцензура громадян і, відповідно, послаблення демократичних інститутів та погіршення загального стану громадянських свобод у суспільстві. Проблематика цифрового тоталітаризму набуває особливої гостроти в умовах глобалізації інформаційного простору, коли цифрові технології та Інтернет стають невід'ємною частиною щоденного життя, економічної діяльності та політичних процесів.

Сьогодні вже не йдеться виключно про авторитарні режими, адже навіть країни з демократичною формою правління можуть демонструвати прояви цифрового авторитаризму, наприклад, через надмірне використання алгоритмічного контролю або збору персональних даних без належного громадського контролю та прозорості.

Це підтверджує, що загроза цифрового тоталітаризму є універсальною і може реалізовуватися як на рівні держав, так і у приватному корпоративному секторі, що ускладнює боротьбу із цим явищем та робить його особливо небезпечним для прав людини. Для ефективної протидії цифровим тоталітарним тенденціям надзвичайно важливим є формування та подальший розвиток глобальних стандартів захисту прав і свобод людини в онлайн-середовищі.

У цьому контексті важливу роль відіграють міжнародні організації, такі як Організація Об'єднаних Націй (ООН), Рада Європи, Європейський Союз та інші регіональні структури, які можуть не лише встановлювати норми та стандарти щодо кібербезпеки та приватності, але й контролювати їх виконання на міжнародному рівні. Значний вплив у боротьбі з цифровим тоталітаризмом мають також ініціативи з боку громадянського суспільства, правозахисних організацій та наукових спільнот, які привертають увагу до конкретних випадків порушень цифрових прав і здійснюють тиск на уряди та корпорації з метою гарантування прозорості та підзвітності у сфері використання технологій.

Крім того, протидія цифровому тоталітаризму потребує активного розвитку технічних засобів захисту конфіденційності й приватності користувачів у цифровому середовищі. Розвиток сучасних методів шифрування, таких як криптографічні алгоритми із відкритим ключем або наскрізне (end-to-end) шифрування, дозволяє суттєво зменшити ризик незаконного доступу до персональних даних користувачів, що робить спроби держав чи корпорацій здійснювати тотальний моніторинг менш ефективними.

Крім того, важливими є також технічні рішення, спрямовані на забезпечення анонімності користувачів у мережі, наприклад, використання віртуальних приватних мереж (VPN) чи браузерів, таких як Tor, що дозволяють громадянам обходити цензуру та безпечно отримувати доступ до інформації, захищаючи свої права та свободи. Таким чином, ефективна протидія цифровим тоталітарним тенденціям повинна базуватись на комплексному підході, який поєднує нормативне регулювання на міжнародному та національному рівнях, прозорість алгоритмічних систем, громадський контроль, освітні програми з розвитку цифрових компетентностей та етики, а також активне впровадження та використання технологічних засобів захисту приватності. Лише за умови всебічного підходу та активної взаємодії всіх зацікавлених сторін – від міжнародних організацій до кожного окремого користувача – можливо запобігти подальшому поширенню цифрових тоталітарних тенденцій та забезпечити сталий розвиток цифрових технологій, що поважає фундаментальні права і свободи людини.

У сучасному цифровому середовищі технологічні корпорації також відіграють ключову роль у забезпеченні свободи слова та інформаційної відкритості. Проте вони стикаються з низкою складних викликів, зокрема поширенням фейкових новин, маніпулятивного контенту, екстремізму та пропаганди.

Соціальні платформи, такі як Twitter і YouTube, постійно впроваджують нові алгоритми та інструменти для протидії дезінформації. Значну увагу в цьому контексті приділяє компанія Meta (раніше Facebook), особливо в боротьбі з фейками щодо COVID-19. З початку пандемії Meta реалізувала комплексний підхід для забезпечення достовірності інформації на своїх платформах: (Facebook, Instagram). Meta співпрацювала з організаціями охорони здоров'я, такими як Всесвітня організація охорони здоров'я (ВООЗ), для надання користувачам актуальної та перевіреної інформації про COVID-19.

Це включало створення спеціальних інформаційних центрів та розміщення достовірних даних у верхній частині стрічки новин користувачів. Компанія активно видаляла публікації, які містили неправдиві твердження про вірус, методи лікування або вакцини, що могли завдати шкоди здоров'ю людей. Це стосувалося контенту, який суперечив рекомендаціям авторитетних медичних установ. Meta впровадила систему маркування контенту, який міг містити сумнівну або неперевірену інформацію. Такі дописи супроводжувалися попередженнями та посиланнями на достовірні джерела, щоб користувачі могли самостійно оцінити їхню правдивість. У різних країнах Meta співпрацювала з незалежними фактчекінговими проєктами.

Наприклад, в Україні партнерами стали StopFake та VoxCheck, які отримали право позначати та знижувати поширення неправдивого контенту на платформі. Незважаючи на вжиті заходи, Meta зіткнулася з критикою щодо ефективності своїх дій. Деякі експерти вказували на затримки у видаленні або маркуванні дезінформації, що дозволяло фейкам швидко поширюватися серед користувачів. Алгоритми платформи не завжди точно ідентифікували неправдивий контент, що призводило до випадків як пропуску дезінформації, так і помилкового маркування достовірних публікацій. Деякі користувачі та організації висловлювали занепокоєння щодо можливого обмеження свободи слова через агресивну модерацію контенту [245].

Одним із способів захисту особистих даних в умовах цифровізації є освіта та підвищення обізнаності користувачів. Ці аспекти постійно підкреслюються в останніх звітах Freedom House. Люди повинні бути більш свідомими стосовно ризиків та наслідків недбалого ставлення до своїх даних. Це включає в себе використання надійних паролів, обережність при обміні інформацією в мережі та регулярну перевірку наявності оновлень на пристроях та програмному забезпеченні. Крім того, законодавча база та регулювання в галузі захисту особистих даних стали набагато суворішими.

Закони, такі як Загальний регламент з захисту даних (GDPR) в Європейському Союзі та Каліфорнійський Закон про конфіденційність споживача (CCPA) в США, вимагають від компаній більшої відповідальності стосовно збору та обробки особистих даних. Це включає в себе право на доступ до власних даних, право на їх видалення та право на контроль над їх використанням.

Технологічні рішення компаній також відіграють важливу роль у забезпеченні безпеки особистих даних. Шифрування, двофакторна аутентифікація, застосування блокчейн-технологій та інші інновації сприяють захисту даних від несанкціонованого доступу. Завдяки розвитку Інтернету та цифрових технологій, інформаційний простір став доступним для кожного індивіда. Онлайн-платформи, соціальні мережі та інші цифрові засоби комунікації надають голос кожному, хто має доступ до цих ресурсів.

Це створює потужний інструмент для виразу індивідуальних поглядів, розповсюдження новин та інформації, а також обговорення глобальних проблем.Свобода слова визнається однією з основних складових демократії. Вона забезпечує можливість висловлювати свої думки, навіть якщо вони є контроверсійними чи непопулярними. Це право не тільки сприяє вільному обміну ідеями, але і допомагає розкривати корупцію, порушення прав людини та інші недоліки суспільства. У світлі цифрової революції, інтернет надає можливість кожному громадянину брати участь у глобальному діалозі і впливати на прийняття рішень. Незважаючи на очевидні переваги цифрового віку для свободи слова, існують певні проблеми та обмеження.

Однією з головних є сприйняття та розповсюдження фейків і дезінформації. Цифрова сфера надає можливість поширювати брехню та маніпулювати громадською думкою швидше, ніж будь-коли. Це може вразити як демократичні процеси, так і інформаційний ландшафт загалом. Крім того, національні та міжнародні уряди знаходять способи обмежувати інтернет та цифрові комунікації в інтересах національної безпеки, громадського порядку або інших соціальних цінностей. Це може включати

в себе блокування доступу до певних інформаційних ресурсів, цензуру та моніторинг онлайн-активності громадян.

Забезпечення інформаційної свободи в цифровому світі, на думку дисертанта, вимагає балансу між правом на свободу висловлювання та необхідністю забезпечити якість та достовірність інформації. Для досягнення цього балансу, можливі підходи включають:

1. Медіаосвіту: збільшення медіаосвіти може допомогти громадянам розрізняти правдиву інформацію від фейків та дезінформації.
2. Законодавство: закони про інтернет-свободу та права на свободу слова мають бути розроблені та адаптовані до нових реалій цифрового світу. Законодавство повинно забезпечувати захист прав громадян на свободу слова, але також надавати можливість реагувати на зловживання та маніпуляції інформацією.
3. Саморегуляція інтернет-платформ: соціальні мережі та інші цифрові платформи повинні приймати активну роль у контролі якості інформації, що розміщується на їхніх сторінках. Вони можуть впроваджувати правила та алгоритми, щоб боротися з дезінформацією і ненависті в мережі.
4. Глобальне співробітництво: багатонаціональні організації та країни повинні співпрацювати для розробки стандартів і норм для цифрового простору. Це дозволить розробити спільний підхід до забезпечення інформаційної вільності на глобальному рівні.
5. Активна громадянська позиція: важливо, щоб громадяни були активними учасниками у формуванні інформаційного середовища. Вони повинні прагнути до інформаційної грамотності, вимагати від влади раціонального підходу до обмеження свободи слова та виступати проти цензури.

Свобода слова та інформаційна вільність залишаються однією з основних цінностей сучасного світу. У цифрову епоху вони набувають нового виміру, де доступ до інформації і можливість висловлювати свої

думки стають ще більш доступними, але й вразливими перед новими викликами. Забезпечення інформаційної вільності у цифровому світі вимагає спільних зусиль громадян, влади, технологічних компаній і міжнародних організацій. Тільки таким чином можна зберегти рівновагу між свободою слова і захистом громадських інтересів у цифрову епоху.

Прозорість – це ключовий аспект будь-якої функціонуючої демократії. У цифровому світі прозорість стає ще більш важливою, оскільки обробка та обмін даними стають невід'ємною частиною нашого життя. Важливо, щоб люди могли розуміти, як їхні дані використовуються, і мати можливість приймати інформовані рішення щодо своєї цифрової активності. Саме тут, прозорість, на думку дисертанту, розкривається у наступних технологічних аспектах :

1. Захист особистих даних*:* прозорість в обробці особистих даних – це необхідний елемент для забезпечення приватності користувачів. Регуляторні органи, такі як Загальний регламент з захисту даних (GDPR) в Європейському Союзі, встановлюють вимоги до компаній щодо збору та обробки даних, а також до повідомлення користувачів про цей процес.

2. Прозорість алгоритмів*:* багато онлайн-платформ використовують алгоритми для підбору контенту, який відображається користувачам. Прозорість у роботі цих алгоритмів важлива для уникнення фільтрування, ізоляції та формування інформаційної бульбашки. Відповідальність передбачає, що суб'єкти діяльності несуть відповідальність за наслідки своїх дій. У цифровому світі це означає, що як користувачі, так і організації повинні приймати відповідальність за свої цифрові дії та практики.

3. Кібербезпека: зростання кількості кібератак та порушень безпеки даних свідчить про необхідність відповідальності в цифровому просторі. Організації повинні приділяти належну увагу захисту своїх інформаційних ресурсів, а користувачі – дотримуватися базових правил кібербезпеки.

4. Розповсюдження дезінформації: цифровий вік дозволяє швидко поширювати інформацію, включаючи дезінформацію та фейки.

Відповідальність вимагає, щоб користувачі перевіряли інформацію перед її подальшим поширенням і не сприяли поширенню дезінформації.

Прозорість та відповідальність є необхідними складовими у цифровому світі. Інформаційна прозорість дозволяє користувачам розуміти, як їхні дані використовуються, і зберігати їхню довіру до цифрових платформ. Відповідальність передбачає, що всі учасники цифрового простору несуть відповідальність за свої дії і рішення. Ці два аспекти взаємодіють між собою і створюють здорову цифрову екосистему, в якій користувачі можуть вільно користуватися цифровими технологіями, знаючи, що їхні права та приватність захищені.

Забезпечення прозорості і відповідальності вимагає спільних зусиль суспільства, бізнесу та уряду. Наприклад, регуляторні органи можуть встановлювати правила та стандарти щодо обробки даних та кібербезпеки, а компанії повинні дотримуватися цих вимог і дотримуватися найкращих практик у галузі кібербезпеки. Якщо громадяни не знають, як і ким обробляються їхні персональні дані, то вони втрачають контроль над своїм цифровим слідом а отже, і над власною безпекою та свободою у цифровому просторі. Користувачі, повинні бути освічені щодо ризиків та плюсів цифрового світу та бути готовими відповідати за свою власну цифрову безпеку.

Сучасний світ переживає швидкий розвиток технологій та інтернет-комунікацій, що відкриває багато можливостей для розвитку суспільства, економіки і культури. Проте разом з цими позитивними змінами існує зворотній бік цифрової епохи, який загрожує, таким цінностям, як свобода, приватність і права людини. Один із таких негативних аспектів – це цифрові тоталітарні тенденції, які в деяких країнах стають все більш помітними.

У 2023 році провідна світова дослідницька та консалтингова компанія у сфері інформаційних технологій «Gartner» визначила десять основних технологічних тенденцій, згрупувавши їх у три ключові макрообласті: інтелект, діджиталізація та сітчаста мережа [77]

Ці макрообласті охоплюють тенденції, спрямовані на розширення можливостей штучного інтелекту (ШІ) та покращення процесів прийняття рішень. «Ключовим фактором для впровадження ШІ є дані. Великі дані – це «паливо» для ШІ. Машинне навчання вдосконалюється шляхом отримання більшої кількості та більш різноманітних даних» [18, с.25].

Один із варіантів, який застосовується на даний момент, це Адаптивний штучний інтелект (Adaptive AI), його системи здатні динамічно змінювати свої алгоритми та моделі відповідно до змін середовища, у якому вони працюють.

На відміну від традиційних ШІ-рішень, які потребують оновлення та перенавчання вручну, адаптивний ШІ може самостійно коригувати свою поведінку та навчатися у реальному часі. Цікаве те, що цей варіант ШІ вже застосовується у біржовій торгівлі, аналізуючи ринкові зміни в реальному часі та адаптуючи інвестиційні стратегії. Наприклад, *Hedge Funds*, такі як Bridgewater Associates, застосовують ШІ-алгоритми для автоматичного коригування портфелів залежно від макроекономічних факторів [245].

У січні 2025 року компанія висловила оптимізм щодо впливу нових ШІ-моделей на розвиток галузі, що свідчить про їхню увагу до технологічних інновацій. Крім того, Bridgewater заснувала підрозділ AIA Labs, який зосереджується на розробці та використанні ШІ та машинного навчання для генерування інвестиційних стратегій та аналітики. Це підкреслює прагнення компанії інтегрувати передові технології для підвищення ефективності управління інвестиціями [245].

ШІ почали використовувати для оптимізації руху транспорту. Світлофори та транспортні маршрути можуть змінювати свої налаштування на основі трафіку, прогнозів погоди та поточних заторів. «Штучний інтелект створює адаптивну основу для сайтів, активів і ринків, тоді як аналіз великих даних покращує прогнози споживання енергії та підвищує безпеку мережі. Споживачі зможуть використовувати технології plug-and-play43,

коли здійснюється інтеграція електромережі з розумними будівлями та електростанціями. Кінцевою метою, ймовірно, буде повна автоматизація з точки зору виробництва електроенергії, розподілу та управління послугами» [264, с.397]. Такий розвиток має і певні питання, які достатньо актуалізуються за умов розвитку ШІ та цифрових тоталітарних тенденцій у світі, а саме, розширене застосування ШІ в управлінні електромережами та розподілі енергоресурсів підвищує ризик централізованого контролю над цими системами.

Якщо державні органи або приватні компанії отримають монополію на алгоритмічне керування енергопостачанням, вони зможуть диктувати правила споживання, контролювати доступ до енергії, а в екстремальних випадках – обмежувати або відключати постачання енергії з політичних або економічних причин. У вже існуючих авторитарних режимах така ситуація може перетворитися на інструмент тотального контролю над громадянами.

Заміна традиційних методів управління електромережами повністю автономними ШІ-системами несе загрози алгоритмічних помилок або зовнішніх атак. Якщо енергосистема повністю покладатиметься на автоматизовані рішення, зловмисники або навіть державні актори можуть спробувати взламувати мережу, що потенційно також може спричинити широкомасштабні відключення електроенергії.

Такі атаки можуть бути використані не лише для саботажу, а й як інструмент гібридної війни або економічного тиску на цілі регіони та країни. Сучасні енергетичні системи збирають велетенські обсяги даних про споживання електроенергії користувачами, що дозволяє ШІ прогнозувати поведінку людей, аналізувати їхні звички та навіть передбачати, коли вони перебувають вдома або використовують певні пристрої.

Нас також цікавить питання розвитку та розповсюдження так званого Креативного ШІ (Generative AI), який може створювати новий контент на основі аналізу великих Дата Бази. Це можуть бути тексти, зображення, музика, коди програмного забезпечення та навіть тривимірні моделі.

Сучасні генеративні моделі, такі як OpenAI GPT-4, Claude від Anthropic, Google Bard у сфері текстової генерації, DALL-E, Midjourney, Stable Diffusion для створення графічного контенту, а також AIVA і Google Magenta в галузі музики, демонструють значний потенціал у прискоренні творчих процесів, автоматизації рутинних завдань та розширенні інструментарію професійної діяльності.

Водночас впровадження таких технологій у суспільне та економічне життя несе загрози, що безпосередньо пов’язані із цифровими тоталітарними тенденціями, які проявляються у централізованому контролі, цензурі, маніпуляції суспільною свідомістю та концентрації цифрової влади в руках невеликої групи технологічних корпорацій або державних установ.

Таким чином, генеративний ШІ є потужним технологічним інструментом, що здатен кардинально змінити спосіб створення контенту, автоматизувати інтелектуальну діяльність та розширити межі людської творчості.

Розуміючи під цифровими технологіями різні електронні інструменти, системи, пристрої та ресурси, які генерують, зберігають або обробляють дані, відзначимо, що вони створюють безліч можливостей для традиційних галузей і економік більшості країн світу. Прикладами вже визнаних на глобальному рівні цифрових країн світу сьогодні вважають Сінгапур, Данію, Швейцарію та інші, що посіли провідні місця в різних рейтингах, зокрема, Світового індексу цифрової конкурентоспроможності (World Digital Competitiveness Ranking) країн у 2024 року [280].

Саме з цифровими технологіями пов’язані більшість визначень цифрової (діджитал) економіки як явища в світі. Тобто, цифровий тоталітаризм – це ситуація, коли влада намагається оточити суспільство масштабними системами моніторингу, контролю та цензури в інтернеті та інших аспектах цифрової сфери. Основною метою таких дій є збереження влади та обмеження прав та свобод громадян.

Світовий досвід свідчить про те, що цифровий тоталітаризм може проявлятися у різноманітних формах та на різних рівнях, впливаючи на фундаментальні права та свободи громадян. Ці прояви включають цензуру Інтернету, масштабний моніторинг, ідентифікацію та репресії, а також використання штучного інтелекту для контролю інформаційного простору.

Цензура Інтернету є одним із найпоширеніших інструментів цифрового тоталітаризму. Багато держав вдаються до блокування доступу до певних веб-сайтів, соціальних мереж та онлайн-ресурсів з політичних мотивів, прагнучі обмежити доступ громадян до інформації та зберегти контроль над суспільством.

Такі заходи можуть включати фільтрацію контенту, обмеження доступу до міжнародних новинних ресурсів та блокування платформ, які вважаються небажаними або небезпечними для режиму. Масовий моніторинг є ще одним аспектом цифрового тоталітаризму, коли уряди використовують сучасні технології для всебічного спостереження за громадянами. Це може включати відстеження інтернет-активності, моніторинг соціальних мереж та використання систем відеоспостереження з технологіями розпізнавання обличчя. Такі практики дозволяють державам збирати великі обсяги даних про поведінку та комунікації громадян, що може призвести до порушення права на приватність та свободу вираження поглядів.

Ідентифікація та репресії стосуються практики, коли уряди вимагають від громадян надання особистої інформації для визначення їхньої особистості та політичних переконань. Це може включати обов'язкову реєстрацію в онлайн-сервісах під справжніми іменами, збір біометричних даних та створення баз даних з інформацією про політичну активність. Такі заходи можуть використовуватися для переслідування дисидентів, обмеження свободи слова.

Таким чином, цифровий тоталітаризм є багатогранним феноменом, що охоплює різні методи контролю та обмеження інформаційних свобод

громадян. Він вимагає пильної уваги з боку міжнародної спільноти, правозахисних організацій та суспільства в цілому для захисту фундаментальних прав людини в цифрову епоху.

У світі, де технології швидко розвиваються, прозорість та відповідальність лишаються актуальними завданнями. Забезпечуючи їх належним чином, ми можемо насолоджуватися всіма перевагами цифрової епохи, забезпечуючи при цьому нашу безпеку та приватність. Таким чином, важливо продовжувати дискусії, розробляти законодавство та вдосконалювати практики в цій сфері, щоб забезпечити стійкий та ефективний розвиток цифрового світу.

Перспективним напрямом протидії цифровому тоталітаризму є розробка та активне впровадження децентралізованих технологій, таких як блокчейн, криптографія та Web 3.0. Технологія блокчейн заснована на принципі розподіленого зберігання інформації, коли дані знаходяться не на одному централізованому сервері, а на багатьох вузлах (нодах) мережі. Це забезпечує високий ступінь прозорості, безпеки та надійності, а також ускладнює процес цензури або маніпуляції інформацією.

Прикладом застосування є платформа Ethereum, що дозволяє створювати децентралізовані програми (DApps), у яких відсутня центральна точка контролю. Внаслідок цього стає практично неможливим для урядів або корпорацій здійснювати цензуру чи блокування інформації. Особливого значення ця технологія набуває в країнах з високим рівнем цензури та репресій проти свободи слова.

Наприклад, у Китаї активісти використовували Ethereum-блокчейн для публікації матеріалів, які були під забороною, що робило практично неможливим їхнє видалення або блокування з боку уряду [283].

Криптографічні технології забезпечують конфіденційність інформації через її шифрування, що робить дані доступними лише для тих, хто володіє відповідним ключем. Шифрування є важливим інструментом у боротьбі з масовим наглядом і контролем. Одним із найяскравіших прикладів є

технологія наскрізного (end-to-end) шифрування, яка застосовується у месенджерах, таких як Signal, Telegram і WhatsApp.

Завдяки цьому доступ до повідомлень мають лише відправник та отримувач, що суттєво ускладнює спроби державних органів здійснювати масове стеження за громадянами. Особливо це стає помітно під час протестів, коли протестувальники використовують саме захищені криптографічні месенджери для координації своїх дій. Web 3.0 — це концепція наступного покоління Інтернету, яка ґрунтується на децентралізації, самоуправлінні та прозорості. Однією з ключових технологій у цій сфері є InterPlanetary File System (IPFS), яка забезпечує зберігання та обмін даними без використання централізованих серверів. IPFS дозволяє публікувати інформацію таким чином, що її неможливо цензурувати, видалити або змінити одним суб'єктом.

Як свідчать джерела, під час політичних протестів у країнах з обмеженням свободи слова, таких як Туреччина та Іран, активісти використовували IPFS для поширення матеріалів, які місцева влада намагалася видалити з мережі. Це дозволило зберегти доступ до важливої інформації та обійти цензуру [232].

Таким чином, технології Web 3.0, зокрема IPFS, відіграють важливу роль у забезпеченні свободи інформації та протидії цифровому тоталітаризму, надаючи користувачам можливість зберігати та поширювати дані без страху цензури чи видалення. Ці технології відкривають принципово нові можливості для захисту приватності, забезпечення прозорості, а також унеможливлюють централізований контроль над інформацією та цифровими ресурсами. Збереження особистих даних в умовах цифровізації світу стало однією з головних проблем нашого часу.

Важливо зберігати баланс між використанням цих даних для розвитку та покращення послуг і забезпеченням приватності та безпеки користувачів. Водночас освіта, правові норми і технологічні рішення спільно сприяють забезпеченню збереження особистих даних в цифровому світі.

Технологічні корпорації відіграють ключову роль в процесах сприяння та протидії цифровому тоталітаризму. Вони можуть забезпечити збереження особистих даних, підтримувати свободу слова та інформаційну вільність, і сприяти прозорості та відповідальності у своїй діяльності.

Однак, важливо також враховувати, що технологічні корпорації несуть велику відповідальність перед суспільством, і їхні дії можуть впливати на демократичні цінності та права громадян. Для подолання цифрового тоталітаризму, такі корпорації повинні співпрацювати з урядами, активістами і громадськістю для розробки ефективних стратегій та політик, які забезпечать збереження цифрових прав людини. Важливо також забезпечити розвиток та впровадження нових технологій, які допоможуть виявляти та запобігати цифровому тоталітаризму.

Отже, роль технологічних компаній у процесах сприяння та протидії цифровому тоталітаризму не може бути недооціненою. Вони мають унікальну можливість вплинути на цей процес, але разом з тим повинні дотримуватися високих стандартів прозорості та етичності в своїй діяльності. Тільки таким чином можна забезпечити захист демократичних цінностей та прав людини в цифровому світі.

Висновки до другого розділу. Отже, сучасний світ переживає революцію інформаційних технологій, яка впливає на всі аспекти суспільства, включаючи національну безпеку країн. У цьому контексті важливо підкреслити основні аспекти можливого впливу «цифрового тоталітаризму» на суверенітет і безпеку держав.

Цифровий тоталітаризм – як особливий тип політичного режиму характерезується станом, коли влада чи інші організації використовують цифрові технології для масового контролю над громадянами, обмеження їхніх прав і свобод. Ця практика може включати в себе масовий моніторинг комунікацій, обмеження доступу до інформації та репресії проти тих, хто висловлює критику чи несхвалення влади.

Цифровий тоталітаризм може впливати на національну безпеку країн у наступних аспектах :

- кіберзагрози: за допомогою цифрових технологій тоталітарні режими можуть здійснювати кібератаки на інші держави, підривати їхні комунікаційні інфраструктури та спрямовувати атаки на критичну інформаційну і кіберінфраструктуру;

- масовий контроль над інформацією: цифровий тоталітаризм може включати цензуру та обмеження доступу до інформації. Це може призвести до зміни дискусії і маніпуляції громадською думкою, що може вплинути на політичну стабільність країни;

- політичний контроль: тоталітарні режими можуть використовувати цифрові технології для контролю за політичними опонентами та обмеження їхньої діяльності. Це може призвести до пригнічення політичної опозиції та порушення прав людини;

- шпигунство і масовий моніторинг: влади можуть використовувати цифрові технології для масового моніторингу комунікацій громадян. Це створює загрозу для особистої приватності та може використовуватися для репресій;

- економічна безпека: цифровий тоталітаризм може мати негативний вплив на економічну безпеку країни, оскільки він може відлякувати інвесторів та завдає шкоди інноваціям та розвитку технологій.

Для боротьби з цифровим тоталітаризмом і збереження національної безпеки країн, необхідно впроваджувати ефективні кіберзаходи, зміцнювати права людини та свободу слова, і забезпечувати незалежність медіа. Міжнародне співробітництво також грає важливу роль у боротьбі з цифровим тоталітаризмом, оскільки кіберзагрози часто мають транскордонний характер.

Усвідомлення загрози цифрового тоталітаризму та прийняття заходів для її протидії є важливими завданнями для країн у забезпеченні національної безпеки. Тільки завдяки спільним зусиллям країн та

міжнародним спільнотам можна взяти під контроль цю загрозу і забезпечити збереження демократії, прав людини і свободи в інтернет-середовищі.

РОЗДІЛ 3
МЕХАНІЗМИ ЗАХИСТУ ПРАВ ЛЮДИНИ В УМОВАХ РОЗВИТКУ ЦИФРОВИХ ТЕХНОЛОГІЙ

3.1. Політико-правова база захисту прав людини в умовах цифрових трансформацій

Як світове, так і українське суспільство в останні декілька років зазнало повної цифрової трансформації, і тепер його прийнято називати інформаційним суспільством. Ми виробляємо, використовуємо, зберігаємо та обробляємо інформацію щодня у великих обсягах. Інформаційні дані постійно перетворюються на все більш важкий продукт, стан яких стає все більш перевантаженими для пересічних громадян суспільств, країн та держав.

Сьогодні роль інформації та інформаційних технологій у суспільному житті – це більше, ніж просто інформаційні технології. Вони важливі, мають вирішальне значення та пов’язані з багатьма процесами, що забезпечують життєдіяльність людей. Інформаційні технології потрібні нам не лише тому, що вони виробляють дані, але й тому, що пов’язані з ними інформаційні продукти та послуги, забезпечують розвиток національних економіки, світових відносин тощо.

«Нові цифрові технології та глобальні інформаційні мережі, які здійснили справжню революцію у сфері накопичення та обміну інформацією, як відмічають дослідники, – вимагають фундаментальних змін у підходах та принципах захисту прав інтелектуальної власності, яка створювалася в зовсім інших технологічних і світоглядних умовах. Глобальне середовище Інтернету та розвиток інформаційно-комунікаційних технологій потребують адекватного регулювання відносин із використанням інтелектуальної власності. Нові реалії сучасних ІТ-технологій та Інтернету, отримані знання у цій сфері ставлять нові завдання,

до виконання яких традиційний механізм захисту прав інтелектуальної власності не завжди пристосований» [146].

Інформаційно-цифровий простір світу, як середовище, у якому сьогодні живе й побутує віртуальне суспільство, став об'єктом постійних загроз та різноманітних атак.

Останнім часом суспільство дедалі частіше стикається з різноманітними видами кібератак: збої при наданні електронних послуг, блокування роботи державних органів, фішингові атаки електронною поштою, кіберзлочини, порушення цілісності та конфіденційності даних, інформаційно-психологічний тиск на населення, кібертероризм, кібершпигунство, інформаційна експансія у національний інформаційний простір країни, блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення й об'єктів підвищеної небезпеки.

Це значно дестабілізувало роботу не лише певних структур та організацій, а й окремих індивідів, соціальних груп та будь-якої країни в цілому. Інформаційна безпека в цьому плані стала важливим елементом. Тому протидія можливим і реальним загрозам є першочерговим завданням не тільки для окремих людей, структур, а й держави в цілому.

Під інформаційною безпекою прийнято пояснення, як – захищеність інформації, а також підтримуючої її інфраструктури від заподіяних впливів, які можуть задавати незрівнянної шкоди суб'єктам інформаційних відносин, в склад яких можуть входити, як власники так і користувачі інформації та підтримуючої інфраструктури інформаційного простору мережі Інтернет. «Захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки» [63].

Отже, з методологічної точки зору – вивчення та вирішення проблеми захисту інформації – починається з виявлення суб'єктів інформаційних відносин, а також усіх інтересів, які пов'язані з використанням різноманітних інформаційних систем у мережі Інтернет. Слід погодитися із

О. Кушнеровим, що потенційна загроза інформаційній безпеці — це зворотна сторона використання інформаційних технологій. З цього твердження можемо вивести два важливі аспекти:

- трактування проблем, пов’язаних з інформаційною безпекою, для різних категорій суб’єктів може суттєво відрізнятися. Для прикладу достатньо порівняти режимні державні організації та навчальні інститути. Режимні організації ставляться до безпеки на кшталт: «хай краще все зламається, ніж ворог дізнається бодай якусь секретну інформацію», інші ставляться таким чином: «у нас немає секретів, хоч би все працювало»;

- інформаційна безпека не зводиться виключно до захисту від несанкціонованого доступу до інформації, це значно ширше поняття.

Суб’єкт інформаційних відносин може постраждати (зазнати збитків та/або отримати моральні приниження) не тільки від несанкціонованого доступу, але й від поломки системи. Більше того, для багатьох відкритих організацій (наприклад, навчальних) власне захист від несанкціонованого доступу до інформації не перебуває на першому місці [63].

Таким чином інформаційна безпека – залежить не тільки від комп’ютерних пристроїв, а також від усіх інших підтримуючих інформаційно приймаючих та транслюючих пристроїв та носіїв інформації, а саме : системи постачання, кондиціонування, засобів комунікацій та персонал, що керує, спрямовує та обслуговує такі системи.

Об’єктом кіберзлочинів може стати будь-який користувач Інтернету. Найпоширенішими видами таких злочинів дослідники віокремлюють:

- *Кардинг* – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, «трояни», «боти»).

- *Фішинг* – вид шахрайства, відповідно до якого клієнтам платіжних систем надсилають повідомлення електронною поштою нібито від

адміністрації або служби безпеки цієї системи з проханням вказати свої рахунки та паролі.

- *Вішинг* – вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний міський номер, а при розмові запитуються конфіденційні дані власника картки.

- *Онлайн-шахрайство* – несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку.

- *Піратство* – незаконне розповсюдження інтелектуальної власності в Інтернеті.

- *Кард-шарінг* – надання незаконного доступу до перегляду супутникового та кабельного TV.

- *Соціальна інженерія* – технологія управління людьми в Інтернет-просторі.

- *Мальваре* – створення та розповсюдження вірусів і шкідливого програмного забезпечення.

- *Протиправний контент* – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства.

- *Рефайлінг* – незаконна підміна телефонного трафіку» [27, с. 447].

Витрачені зусилля на збільшення охоплення користувачів мережі та успішні онлайн кампанії сьогодні захоплюють результатами. Але, чим успішніша і більша онлайн присутність, тим небезпечніше забувати про її тіньову сторону – цифрові загрози.

Взаємодія в мережі з користувачами привертає не лише бажану увагу – вашу присутність також фіксують зловмисники, зокрема, фінансово вмотивовані кіберзлочинці, конкуренти, які намагаються злити засекречену інформацію різного роду хакерам.

Питання кіберзлочинності сьогодні стає надважливим у державних та громадських рівнях. Серед найчастіше вразливих до ударів кібератак стає критична інфраструктура, а саме :

«енергетичні об’єкти, транспорт та банківський сектор. Вартість захисту зазвичай у 10 разів дорожча за саму атаку. Тому пріоритетним напрямком в політиці багатьох держав є кібербезпека» [45].

Так, за позицією науковця А. Карачка, «для позначення різних категорій комп’ютерних злочинців використовуються різноманітні терміни: «хакери», «кракери», «пірати», «шкідники»» Хакери — на думку фахівця це – узагальнююча назва людей, які зламують комп'ютерні системи [45, с. 23]. Цим терміном також позначають спеціалістів-програмістів, які ставлять за мету своєї роботи зламування, як хобі. Так звані «кракери» - зламувачі вважаються більш професійними «спеціалістами», що на меті ставлять масові збої, злами та проникнення у дати бази із конкретними цілями та задачами.

«Найбільш криміногенною групою є *пірати* — професіонали найвищого ґатунку, які спеціалізуються на крадіжках текстів нових комерційних програмних продуктів, технологічних ноу-хау тощо. Така робота, природно, виконується на замовлення або передбачає реального покупця. За відсутності замовлень пірат може зосередитися на кредитних картках, банківських рахунках, телефонному зв’язку» [45, с. 23].

«Шкідники (вандали) намагаються реалізувати у кіберпросторі свої патологічні схильності – вони заражають його вірусами, частково або повністю руйнують комп'ютерні системи» [45, с. 23]. Дуже частим спонуканням до дії таких представників стає план помсти.

Також А. Карачка виділяє додаткову групу злочинців, яка посідає другорядне місце серед перелічених, та чий досвід ще далекий, проте також може нести небезпеку суспільствам та державним інституціям. «Ідеться про *експериментаторів («піонерів»*). Найчастіше це молоді люди, які під час освоєння інструментальних та інформаційних ресурсів мережі і власного комп'ютера бажають вчитися тільки на власних помилках, відштовхуючись від того, «як не можна». Основну частину цієї групи становлять діти та підлітки. Головною мотивацією у цій групі є гра. З експериментаторів

виходять професіонали високого класу, зокрема й законослухняні» [45, с.24].

Тож, щоб уберегтися від загроз, в першу чергу допоможе розуміння того, що та хто може потенційно загрожувати. Те, яким чином вибудовується цифровий захист держав залежить від зібраної оперативної інформації та превентивних дій проти цифрових атак. Звичайно, методи варіюються в залежності від розміру та масштабів організації, але є кілька фундаментальних концепцій захисту від цифрових ризиків, якими можна керуватися.

Забезпечення власної інформаційної безпеки, в першу чергу, можливо правовими методами та інструментами. Тому, кожна держава намагається створювати власне відповідне законодавство, яке регулює збір, зберігання та обробку персональних даних, а також визначає відповідальність за захист цифрової інформації та санкції за порушення законодавства. Якщо звернутися до законодавства *України*, то Закон № 2163-VIII «Про основні засади забезпечення кібербезпеки України» [113] в статті 1. надається визначення :

«індикатори кіберзагроз, інформація про інцидент кібербезпеки кібератака, кібербезпека, кіберзагроза, кіберзахист, кіберзлочин, кіберзлочинність, кібероборона, кіберпростір, кіберрозвідка, кібертероризм, кібершпигунство, критична інформаційна інфраструктура, тощо»

В свою чергу, «кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних» [113].

Кіберпростір для політичної системи є не лише місцем політичних технологій, тобто місцем впливу на свідомість та політичні процеси, це

також платформа для політичного маркетингу, де відбувається відповідна реклама послуг, які може надати кожен окремий політик чи політична сила, яку він представляє [36, с.146].

Таке середовище створюється та регламентується задля функціонування спільних комунікаційних систем в рамках всесвітньої мережі Інтернет або інших глобальних мереж передачі інформації.

Группа дослідників О. Трофименко, Ю. Прокоп, Н. Логінова, О.З адерейко, вивчаючи питання кібербезпеки України та аналізуючи її сучасний стан пишуть : «Задля готовності забезпечувати кібербезпеку і відбивати відкриту агресію в інформаційному просторі, Україна реалізувала цілий комплекс заходів для вирішення стратегічних, правових, політичних, технічних та організаційних питань з безпечного функціонування кіберпростору (рис. 3.1).

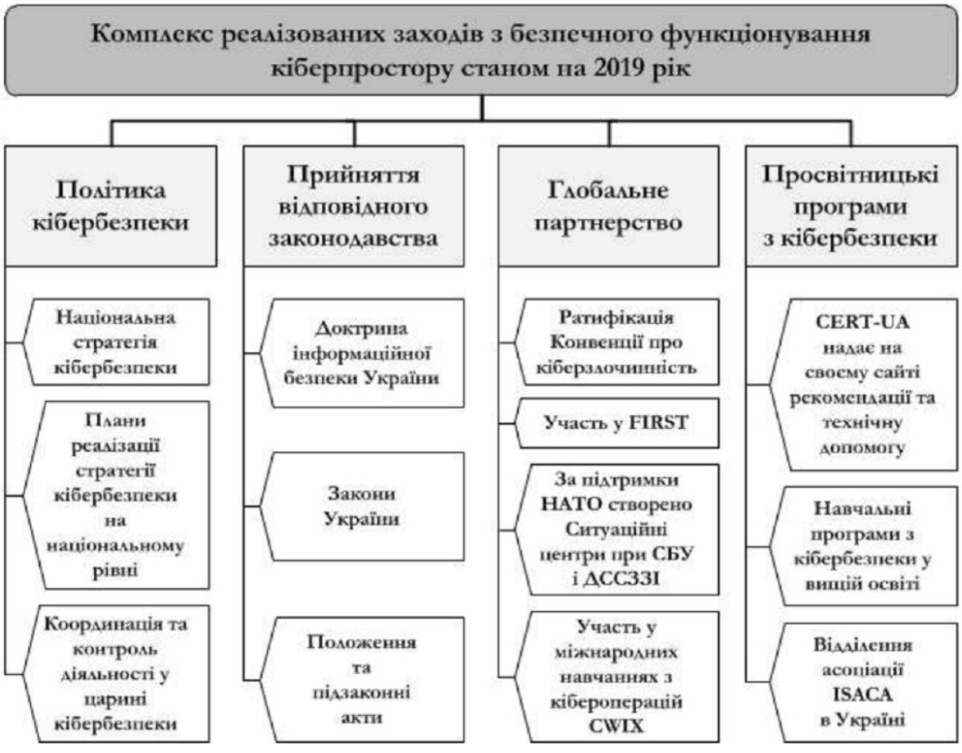

Рис. 3.1. Комплекс реалізованих заходів з безпечного функціонування інформаційного простору» [198].

Отже, важливим та беззаперечно ≠ критичним питанням стає процес побудови національної або державної програми кібербезпеки. В Україні

реалізується «Національна стратегія кібербезпеки» [113], яку започатковано з 2016 року. «Саме в ній кібербезпека та інформаційна безпека визнані як одні з головних пріоритетів у протидії загрозам національній безпеці» [198].

«Задля координації і контролю діяльності різних суб'єктів у царині кібербезпеки організовано роботу відповідних державних служб, за якими закріплено конкретні зобов'язання з дотримання вимог кібербезпеки:

- запроваджено певний механізм керівництва й організовано роботу Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України, який безпосередньо координує міжвідомчу взаємодію суб'єктів національної безпеки і оборони України під час кібератак та кіберінцидентів в інформаційно-телекомунікаційних системах об'єктів критичної інфраструктури задля покращення ефективності системи державного управління у формуванні та реалізації державної політики у сфері кібербезпеки під час реалізації Стратегії кібербезпеки України;

- функції державного контролю у сфері боротьби з кіберзлочинністю, кіберзахисту об'єктів критичної інформаційної інфраструктури, формування та реалізації державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації покладено на Державну службу спеціального зв'язку та захисту інформації України (ДССЗЗІ).

Саме вона координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту і здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти й кібератаки та усунення їх наслідків. ДССЗЗІ забезпечує функціонування урядової Команди реагування на комп'ютерні надзвичайні події України (CERT-UA) та Державного центру кіберзахисту, який здійснює впровадження організаційно-технічної моделі кіберзахисту як складової національної системи кібербезпеки.

Ядром цієї моделі є Центр реагування на кіберзагрози (Cyber Threat Response Centre, CRC), створений 02.02.2018 р. як центральний компонент національної системи кіберзахисту України. CRC побудовано на базі

найновітніших досягнень у сфері кібербезпеки як вітчизняних, так і провідних ІТ-компаній світу. Розроблені на рівні кращих світових аналогів сучасні технологічна та аналітична системи CRC закономірно претендують на звання найпотужніших в європейському співтоваристві [21].

Інша важлива функція ДССЗЗІ пов'язана з контролем за дотриманням вимог законодавства у сфері електронних довірчих послуг, наглядом за кваліфікованими постачальниками електронних довірчих послуг, у галузі криптографічного захисту інформації [198].

Адже саме гарантування конфіденційності й цілісності інформації, захист інформації від несанкціонованого доступу є вимогою успішної реалізації електронного документообігу між державними установами, громадянами та суб'єктами приватного сектора.

Оскільки сьогодні персональні дані громадян потребують захисту так само, як і конфіденційні дані компаній, в Україні був створений відповідний незалежний державний наглядовий орган, як того вимагає Конвенція Ради Європи про захист осіб у зв'язку з автоматизованим обробленням персональних даних. Контроль за дотриманням законодавства про захист персональних даних було покладено на Уповноваженого Верховної Ради України з прав людини [102].

Також, було організовано роботу Департаменту кіберполіції Національної поліції України, який спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних мереж і систем.

Створено компетентний орган у сфері інформаційної безпеки – Державне агентство з електронного врядування України [6], яке має повноваження контролювати операторів основних послуг щодо вимог кібербезпеки. Постачальників цифрових послуг та операторів основних служб відповідно до ст. 5 Закону України про кібербезпеку зобов'язали

керувати кіберризиками, реалізовувати у межах своєї компетенції заходи для забезпечення кібербезпеки і повідомляти відповідні державні органи про випадки кіберінцидентів.

Станом на 2022 рік сформовано законодавчу базу у сфері кібербезпеки держави [16]: затверджено Доктрину інформаційної безпеки України (введена в дію 25.02.2017 р.), закони України «Про основні засади забезпечення кібербезпеки України» 2163-VIII (набрав чинності 09.05.2018 р.), [113] «Про національну безпеку України» 2469-VIII (набрав чинності 08.07.2018 р.), [110] «Про інформацію» 2657-XII (редакція від 01.01.2017 р.), [105] «Про захист інформації в інформаційно-телекомунікаційних системах» 80/94-ВР (редакція від 19.04.2014 р.), [101] «Про електронні довірчі послуги» 2155-VIII (набрав чинності 07.11.2018 р.), [97] «Про захист персональних даних» 2297-VI (редакція від 30.01.2018 р.) [102] тощо. Низка відповідних положень щодо кібербезпеки закріплена в Указах Президента, зокрема: «Про Концепцію розвитку сектора безпеки і оборони України» (№ 92/2016 від 14.03.2016 р.) [106], «Про стратегічний оборонний бюлетень України» (№ 240/2016 від 06.06.2016 р.) [116], «Про Національний координаційний центр кібербезпеки» (№ 242/2016 від 07.06.2016 р.) [109] Указ Президента України «Про рішення Ради Національної безпеки і оборони» «Про стартегію інформаційної безпеки» України [117] тощо.

Саме Закон «Про основні засади забезпечення кібербезпеки України» визначає основні об’єкти кіберзахисту, які створюють критичну інфраструктуру країни, нормативно закріплює понятійний апарат у сфері кібербезпеки на найвищому рівні, регламентує принципи забезпечення кібербезпеки та національну систему кібербезпеки, окреслює державно-приватну взаємодію у сфері кібербезпеки та встановлює відповідальність за порушення законодавства у цій сфері і контроль за законністю заходів щодо забезпечення кібербезпеки» [198].

У вересні 2018 року Міністерством оборони США було оприлюднено Стратегію з кібербезпеки. Ця стратегія було покликана оновити процеси

кібербезпекових питань у державі. «У стратегічних положеннях задекларовано, що американці стають більш залежними від сучасних цифрових технологій, більш вразливими до таких загроз, як: корпоративні порушення безпеки, фішинг та шахрайство в соціальних мережах, кібератаки тощо». Також за словами С.М. Стежко «У Стратегії кібербезпеки США викладені нові інструкції щодо дотримання безпеки в кіберпросторі для усіх федеральних відомств» [90, с.141].

Були також викладені та задекларовані пріоритетні напрямки щодо стримання таких держав, як РФ, Іран, КНР та КНДР та визнано РФ та КНР головними загрозниками безпеці кіберпростору США. Згідно з прийнятим положенням Стратегії кібербезпеки США розуміння поняття «кібербезпека» – наступне :

«це комплекс заходів, спрямованих на захист комп'ютерних систем (включаючи апаратні засоби, програмне забезпечення та дані) від несанкціонованого доступу або атак через мережу Інтернет» [90, с.142].

Вбачаючи різні варіанти протистояння, а також ймовірної безпосередньої війни, «Стратегія також передбачає регулювання ринку систем і засобів захисту інформації, зокрема уніфікацію устаткування та відбір дистриб'юторів. Документ закріплює право вимагати фінансового відшкодування від виконавців та організаторів проведення кібератак» [90, с.142].

Також, не можемо не приділити увагу стану розвитку кібербезпеки в Японії. Країна знаходиться серед ідеологічних конкурентів, тому задля безпеки власної держави та громадян і суспільства в цілому, має забезпечувати високий рівень кібербезпеки. Стратегія Кібербезпеки була прийнята у 2013 році. Урядом Японії також було сформовано спеціальний державний орган, який контролює та керує процесами щодо захисту кіберпростору Японії. Національний центр інформаційної безпеки приймає участь у розробці нових законів, пов'язаних з питаннями безпеки, вводить рекомендаційні запити та допрацьовує закони до відповідного стану.

«Стратегія спрямована на розвиток «провідного в світі», «сталого» і «динамічного» кіберпростору і перетворення Японії у світового лідера в області кібербезпеки. Для реалізації цих цілей в документі передбачені чотири основні принципи: забезпечення вільного обміну інформацією; забезпечення нових заходів у відповідь на те, що загрози стають більш серйозними; прийняття адекватних заходів щодо кіберзагроз на підставі оцінки ризиків; вжиття заходів і взаємодія з іншими державами на підставі їх власної соціальної відповідальності» [143].

Пліч-о-пліч з Японією, вбачаючи загрозу від сусідніх країн, забезпечуючи захист від неперервних кібератак в інформаційному просторі, довели Південній Кореї (РК) розробити та адаптувати власну стратегію кібербезпеки. «Є три установи, що обладнані для вирішення питань кібербезпеки: Національний центр кібербезпеки, Корейське агентство Інтернет та безпеки (KISA), а також Центр реагування на кібертерор Національного поліцейського агентства. Ці установи несуть відповідальність за виявлення, запобігання та реагування на кібератаки та загрози безпеці. Крім того, була заснована школа, що спеціалізується на кібервійнах» [143, с.9].

Такі превентивні заходи були покликані захистити та зберегти урядовий рівень безпеки від потенційних загроз. Вважається, що «перспективами в системі захисту кіберпростору у Південній Кореї є: шифрування для доступу до мережі; системи профілактики вторгнень (IPS); розширена стійка загроза (APT); хмарні обчислення; безпека IoT (Internet of Things)» [143, с.10]

Франція, як одна з провідних країн Європейського союзу також неодноразово переглядає свою політику національної кібербезпеки. «У липні 2009 року було створено Французьке агентство мережевої та інформаційної безпеки (ANSSI, Національна агенція з питань інформаційної безпеки) для вирішення виклику кібератак, відповідно до рекомендацій

Білої книги з питань оборони та національної безпеки – це міжміністерське агентство, приєднане до кабінету прем'єр-міністра» [143, с.8].

Статус національного агентства з питань інформаційної безпеки також займає значущу роль у аспекті оборони та розвитку країни.

«У Європейському Союзі стратегія кібербезпеки була презентована у лютому 2013 року Європейською Комісією та Європейською службою зовнішньої діяльності (EEAS). Франція активно сприяє впровадженню п'яти основних напрямків:

• загальна стійкість ЄС (включаючи органи ЄС);

• боротьба з кіберзлочинністю;

• питання кіберзахисту в рамках Спільної політики безпеки і оборони;

• промислові питання;

• міжнародна політика у сфері кіберпростору» [143, с.8].

Тож Франція приділяє багато уваги, сил та коштів, щоб перейняти світовий досвід та застосувати його у себе вдома, таким чином створивши одну з найбільш вдалих систем протидії кіберзлочинності. Отож, «Франція впевнено розбудовує власний захист кіберпростору, що дозволяє їй без зайвих загроз проводити внутрішню та зовнішню політику та утримувати провідні позиції у вирішенні світових викликів» [143, с.8].

Фінляндія відома як одна з найбільш передових країн світу за рівнем доступності й швидкості інтернет-з'єднання. Ще у 2010 році , вважалось, що «96% населення вже підключено до Інтернету, і лише близько 4000 будинків потребують підключення, щоб відповідати закону» [212].

Цей результат став можливим завдяки значним державним інвестиціям у сучасну цифрову інфраструктуру та активній політиці щодо забезпечення громадян стабільним і швидким Інтернетом, що підкреслюється низкою міжнародних рейтингів і досліджень [264, с.14].

За результатами детального дослідження Фінляндія знаходиться у лідерах серед європейських країн за індексом цифрової економіки та суспільств ЄС, станом на 2020 рік [264, с.14]. Серед активних впроваджень,

які використовує Фінляндія, – впровадження хмарних обчислень, програмного забезпечення, що дозволяє вести бухгалтерський та фінансовой облік в компаніях.

Ще у 2013 році (Академія Фінляндії, Tekes, Sitra, Finnvera та Finpro), розробили спільну стратегію – SUUNTA [264, с.108] Сутність програми мала на меті трансформувати підхід до підтримки наукових досліджень та інновацій. Замість фокусування на окремих проєктах чи компаніях, стратегія спрямовувала зусилля на розвиток ширших бізнес-екосистем у ключових сферах, таких як ефективне використання ресурсів, цифровізація, добробут та охорона здоров'я.

SUUNTA визначила ефективність використання ресурсів для цифровізації суспільства, розвиток добробуту, питання охорони здоров'я як сфер, що мають потенціал для утворення нових бізнес-екосистем, для підключення в систему глобальних центрів та залучення фінансування до держави.

Таким чином, комплексна стратегія Фінляндії щодо розвитку швидкісного доступу до глобальної мережі повністю виправдала себе. Інвестиції в цифрову інфраструктуру забезпечили країні місце серед світових лідерів за рівнем доступності й швидкості Інтернету, і з огляду на активні плани уряду щодо подальших інвестицій ця тенденція, імовірно, збережеться найближчими роками.

Крім того, у Tekes «фінському агентстві фінансування інновацій, стратегія SUUNTA впроваджується у програми щодо: цифрових рішень у галузі охорони здоров'я (Bits of Health), телекомунікаційних стандартів наступного покоління (5th Gear), технології IoT та інклюзивних інновацій у співпраці з країнами, що розвиваються (Business with Impact)» [264, с.108]

Зокрема, великі фінські інтернет-провайдери, такі як Elisa [170] та DNA [169], активно застосовують методи шифрування інтернет-трафіку, завдяки чому інформація, яка передається між пристроями користувачів і серверами операторів, є надійно захищеною від потенційних загроз,

включаючи хакерські атаки. Це суттєво ускладнює можливість стороннього втручання або перехоплення персональних даних. Додатково провайдери пропонують користувачам послуги віртуальних приватних мереж (VPN), що дозволяють зберігати анонімність і забезпечують додатковий рівень захисту при користуванні Інтернетом

Провайдери також активно займаються інформуванням клієнтів щодо онлайн-безпеки. Elisa та DNA регулярно оновлюють спеціалізовані сторінки на своїх сайтах із рекомендаціями з безпечного використання мережі, зокрема щодо створення складних паролів, активації двофакторної автентифікації та розпізнавання небезпечних посилань чи повідомлень.

Ще одним ефективним інструментом забезпечення безпеки є постійний моніторинг провайдерських мереж для виявлення та оперативного блокування загроз, таких як віруси, шпигунські програми чи фішингові атаки. Використовуючи сучасні аналітичні технології, провайдери можуть оперативно реагувати на потенційні небезпеки й ефективно захищати персональні дані своїх клієнтів.

Таким чином, фінські провайдери активно й системно підходять до забезпечення безпеки й конфіденційності користувачів, надаючи їм сучасні рішення, такі як шифрування, VPN-технології та ефективний моніторинг мережевого трафіку.

Швейцарія швидкими темпами стає одним з ключових гравців у сучасній глобальній цифровій економіці. Так, за світовим рейтингом цифврової конкурентоспроможності (WDCR) 2024, Швейцарія посіла друге місце [280].

Цей місце значною мірою пов'язано із привабливістю країні для іноземного висококваліфікованого персоналу, а також ефективним забезпеченням дотримання прав інтелектуальної власності. [255, с.40] Уряд активно підтримує цифрове підприємництво й інновації, запроваджуючи стартап ініціативи, що надає фінансування та необхідні ресурси новим компаніям.

Швейцарія приваблює цифрових підприємців та інвесторів завдяки розвиненій законодавчій базі, яка гарантує стабільність, захист інвестицій і сприяє інноваціям. Додаткові стимули, такі як податкові пільги та доступ до висококваліфікованої робочої сили, ще більше посилюють інвестиційну привабливість країни.

Важливими центрами цифрових інновацій є Цюріх та Женева. Ці міста відомі наявністю великої кількості акселераторів, інкубаторів, науково-дослідних установ і штаб-квартир великих технологічних компаній, що формують потужні інноваційні екосистеми, завдяки чому посідають перше та 4 місце серед усіх цифрових-міст світу [280, с.35]

Хоча Швейцарія широко відома якістю свого високошвидкісного Інтернету, все ж існують значні регіональні відмінності. Останніми роками держава суттєво інвестувала в покращення широкосмугової інфраструктури, завдяки чому середня швидкість Інтернету вже сягає приблизно 30 Мбіт/с і постійно зростає. Проте міста мають значно кращу цифрову інфраструктуру, включаючи доступ до сучасних волоконно-оптичних мереж, порівняно із сільськими районами, які здебільшого покладаються на менш сучасні технології, такі як DSL або супутниковий Інтернет.

Швейцарія вирізняється суворим і комплексним законодавством щодо цифрової конфіденційності й безпеки, діяльність у цій сфері контролюється законом (FDPA) [210], аналогом європейського (GDPR).

Основою цієї політики є Федеральний закон про захист даних (DPA), який зобов'язує компанії забезпечувати високий рівень захисту персональної інформації. FDPIC має повноваження штрафувати підприємства, які порушують норми FDPA, або навіть обмежувати їхню діяльність [210].

Додатковим важливим документом є Федеральний закон, що регулює збирання, зберігання й обробку персональних даних, зобов'язуючи компанії захищати цю інформацію від несанкціонованого доступу і зловживань.

Федеральна рада Швейцарії також ухвалила Стандарт інформаційної безпеки (ISMS), який передбачає жорсткі вимоги щодо захисту інформаційних систем і даних.

Швейцарія активно інтегрує Інтернет речей (IoT) у свою економіку, впроваджуючи інноваційні проекти в галузях транспорту, охорони здоров'я та енергетики. Наприклад, проект «Smart Valais» оптимізує транспортні потоки через сенсорні технології, покращуючи екологію та безпеку руху.

У сфері охорони здоров’я IoT-технології використовуються для дистанційного моніторингу стану пацієнтів, особливо літніх людей та жителів віддалених регіонів, що значно покращує доступність медичних послуг.

Крім того, IoT застосовується для підвищення енергоефективності, зменшення споживання енергії та активнішого використання відновлюваних джерел енергії у повсякденному житті громадян та діяльності підприємств.

Інноваційні технології блокчейн активно розвиваються у сфері платіжних рішень завдяки таким компаніям, як Swisscom, UBS та EY, які забезпечують надійні, безпечні та прозорі транзакції. Ці ж компанії також створюють віртуальні ринки, надаючи нові можливості для бізнесу і якісно покращуючи взаємодію з клієнтами.

Швейцарські компанії активно впроваджують штучний інтелект (ШІ), за показником кількості опублікованих статей про ШІ на душу населення – посідає третє місце у світі [280, с.40 .], активно розвивається машинне навчання для автоматизації процесів і створення персоналізованих послуг, що покращує клієнтський досвід і підвищує конкурентоздатність на ринку.

Таким чином, завдяки широкому спектру інновацій, цифровій інфраструктурі та прогресивному законодавству, Швейцарія продовжує зміцнювати свої позиції як один із провідних центрів глобальної цифрової економіки й інновацій.

Китайська Народна Республіка в свою чергу, вбачаючи необхідність в доробці та розвитку власної кіберзахисної стратегії, сконцентровує власні сили на розробці наступних завдань :

«1. Захист суверенітету кіберпростору;

2. Захист критичної інформаційної інфраструктури (ICI);

3. Створення здорової онлайн-культури;

4. Боротьба з кіберзлочинністю, шпигунством і тероризмом;

5. Поліпшення кібер-управління;

6. Підвищення базової кібербезпеки;

7. Підвищення можливості захисту кіберпростору;

8. Зміцнення міжнародного співробітництва» [143, с.9].

У найближчі декілька років КНР продовжить здійснювати контроль за інформацією та технологіями відповідно до CSL та пов'язаних з ним нормативних положень.

Для всіх компаній, що працюють на території Китаю, буде обов’язковою локалізація даних, особливо тих, які мають статус «важливих». Регулюючі органи також вимагатимуть впровадження технологій, що відповідають визначеним стандартам «безпеки і керованості», наприклад, систем шифрування.

Правозастосовні заходи здебільшого будуть спрямовані на інформаційні системи та ресурси, що перебувають у володінні китайських державних установ, а також державних і приватних підприємств, які серйозно ставляться до загроз у сфері кібербезпеки. Це підтверджують ухвалені ними нормативні акти, спрямовані на захист власного кіберпростору та протидію діяльності ворожих сил.

Ключовими принципами інформаційної безпеки є забезпечення цілісності інформації, конфіденційності та доступності для авторизованих користувачів. Основні порушення інформаційної безпеки включають несанкціонований доступ, витік, втрату, підробку, блокування інформації та збої в роботі інформаційних систем.

Безумовно, стратегія інформаційної безпеки повинна передбачати не лише захист існуючих об'єктів інтелектуальної власності з комерційною цінністю, але й профілактику можливих втрат таких об'єктів у майбутньому. Уніфіковані вимоги до захисту інформації неможливі через різноманітність інформаційних систем і видів інформації. Конкретні заходи визначаються виробничими, фінансовими та іншими можливостями підприємства, а також обсягом і значущістю конфіденційної інформації.

Систему захисту необхідно будувати з огляду на те, що основну загрозу становлять співробітники підприємства чи організації. При цьому система має бути достатньою, надійною, ефективною та керованою. Ефективність захисту інформації визначається не обсягом витрат на її організацію, а здатністю адекватно реагувати на всі потенційні загрози. Заходи захисту інформації мають комплексний характер, включаючи різні методи та засоби. В основі комплексу заходів має лежати стратегія, яка визначає мету, критерії, принципи та процедури, необхідні для створення надійної системи захисту. На основі концепції інформаційної безпеки формуються стратегія та архітектура системи захисту інформації, а далі — політика інформаційної безпеки.

Серед заходів, що безпосередньо забезпечують інформаційну безпеку, виділяють правові (наприклад, захист авторських прав), організаційно-адміністративні (наприклад, охорона комп'ютерних систем) та інженерно-технічні (програмні та криптографічні засоби). Програмні засоби захисту дозволяють здійснювати ідентифікацію та аутентифікацію користувачів, розмежовувати доступ відповідно до повноважень, реєструвати події в інформаційній системі, забезпечувати криптографічний захист і захист від комп'ютерних вірусів.

Таким чином, інформація, яка є сукупністю знань про факти та взаємозв’язки між ними, перетворилася на стратегічний ресурс і основу для прийняття управлінських рішень. В інформаційних системах державних і комерційних структур циркулює інформація, що містить секретні й

конфіденційні відомості про економічний, оборонний, науковий і технічний потенціал, а також управлінську, господарську та фінансову діяльність.

Отже, захист інформації є складною, наукоємною та багатовимірною задачею, особливо гострою в умовах застосування сучасних інформаційних технологій, створення розподілених обчислювальних мереж та систем зв'язку.

3.2. Порівняльний аналіз практик цифрового регулювання в демократичних та авторитарних державах

Останніми роками світови лідери активно рухаються шляхом формування інформаційного суспільства, впроваджуючи сучасні цифрові технології та посилюючи заходи для гарантування національної кібербезпеки. В умовах зростаючих кіберзагроз держави докладають значних зусиль для протидії кібертероризму, зміцнюючи власний інформаційний простір і розвиваючи стійкість до викликів сучасного цифрового середовища.

Так, на загальноевропейському рівні у 2016 році була прийнята постанова 2016/679 або «Загальний регламент захисту персональних даних»/ GDPR. У преамбулі було зазначено : «Цей Регламент спрямовано на сприяння формуванню простору свободи, безпеки і правосуддя, економічного союзу, соціально-економічному прогресові, зміцненню та конвергенції економік у межах внутрішнього ринку, підтриманню добробуту фізичних осіб» [40].

Цей регламент, вважається історичним кроком у розвитку цифрового регулювання в демократичних державах, особливо в контексті порівняння авторитарним підходам до контроля інформації.

Було значно розширені права на доступ до даних (стаття 15); про внесення виправлень (стаття 16) про видалення даних (стаття 17), про

обмеження обробки (стаття 18) про отримання інформації (стаття 19); про перенесення даних (стаття 20);про заперечення (стаття 21); та право не ставати об'єктом рішення, що ґрунтується виключно на автоматизованій обробці (стаття 22) [40].

GDPR охоплює дві основні групи суб'єктів:

1) Рекламні фірми, які використовують інформацію для рекламних кампаній. Медичні установи, які займаються обробкою медичних досьє пацієнтів. Освітні інститути, які акумулюють відомості про студентів для освітніх потреб. Оператори даних. Це зовнішні організації чи внутрішні відділи, які маніпулюють інформацією від імені регулятора.

2) IT-проєкти, які пропонують послуги хмарних ресурсів чи технічну підтримку серверів. Аутсорсингові послуги підтримки, які займаються обробкою звернень клієнтів. Фірми, які спеціалізуються на аналізі даних, здійснюють дослідження поведінкових особливостей користувачів [168].

Впилв GDPR виявився значним по відношенню до підприємств та їнього діловодства з одного боку зміцнюючи довіру, з іншого боку уніфікуючи та втягуючи інформаційні суспільства до чіткого підпорядкування новому закону.

Окрім GDPR, у 2022 також були прийняті нові Акти : Про цифрові послуги / DSA № 2022/2065 [253] та Про цифрові ринки / DMA № 2022/1925 [252], зарахунок яких, була поставлена мета адаптації та регуляції інформаційного простору по відношенюю до нових цифрових змін в суспільстві та структурах роботи ЄС.

23 квітня 2023 року Європейська комісія опублікувала перший список із 19 веб-компаній та сайтів, які повинні були відповідати стандартам DSA. В цей список увійшли крупні компанії, такі як Google, Meta, Amazon, Apple, Alibaba, TikTok, Youtube, X (Twitter) та інші [207].

Висунуті вимоги точились навколо публікування додаткової інформації користувачам, а саме : про те, чому їм рекомендується та чи інша інформація, … право відмовитися від систем рекомендацій, що ґрунтуються

на профілюванні… право на повідомлення про протизаконний контент [207].

В свою чергу, платформи повинні ретельно обробляти такі повідомлення, маркувати всі оголошення та інформувати користувачів про те, хто їх просуває та надавати простий виклад своїх положень, умов усіма мовами держав-членів ЄС, в яких вони працюють. Сенатори США Уайден та Крапо критично поставились до актів, стверджуючи, що DMA та DSA нерівномірно направлені щодо компаній, які знаходяться у ЄС, КНР та Росії, а також звернулись до 46-го Президента США Джозефа Байдена вирішити це питання [211].

Депутат Європарламенту від Швеції Джесіка Стегруд також критичино коментувала характер та сутність нових регламентів, вважаючи їх ще більш цензурними та недемократичними. «Технологічні компанії і так природно пригнічують контент і блокують облікові записи користувачів, а тепер вони робитимуть це ще більше через великі та швидкі штрафи, передбачені DSA. Довільні законодавчі категорії, такі як «шкідливий» чи «небажаний», відкриють усі шлюзи, як навчає історія» [268].

З боку урядів ЄС, такі регламенти не зустрічали маштабного опіру через бажання регулювати технологічні корпорації в сферах цифровізації послуг, то почались вводитись та копіюватись і в таких державах, як США, Японія, Бразилія, Великобританія тощо [209].

В порівнянні із загальноєвропейським рівнем, Німеччина ще у 2017 році вела закон «Захист прав у мережі»/ NetzDG [224] завдяки якому, регулюється національний ринок постачальників та їхніх цифрових послуг, які керують платформами в Інтернеті з метою отримання прибутку. Також цей закон стосується регламентації дії у соціальних мережах. Закон спіткала неабияка критика з різних сторін, як з боку правозахисних груп, як Human Rights [223], так спецдоповідачем ООН по питанням захисту свободи слова та вільного її використання Девідом Кейєм. [243]. Технологічні компанії

рівню Google розуміючи силу цього закону подали позив щодо перегляду таких норм та потенційних штрафів [226].

Проте закон залишився актуальним для німецького уряду, який активно продовжує притягувати до відповідальності веб-платформи за незаконний контент.

КНР в рамках нормативно-правової бази регламентує цифровізаційні щонайменш трьома основними законами. Закон про кібербезпеку / Cibersecurity Law (CSL) [284]. Був прийнятий у 2017 році, як реакція на заяви Едварада Сноудена про роботу амереканської системи PRISM щодо відслідковування дій громадськості у Інтернеті з боку АНБ США.

Закон про кібербезпеку також містить докладні положення та визначення юридичної відповідальності. Для різних видів незаконного провадження Закон встановлює різні накази, такі як штрафи, відкликання на виправлення, відгук дозволів і ліцензій на ведення бізнесу та інші. Відповідно, Закон забезпечує органам кібербезпеки та адміністрування права та керівні принципи для здійснення правозастосування у відносинах протизаконних дій [192]

Закон про безпеку персональних даних / Data Security Law (DSL) [286]. Був прийнятий у 2021 році, також, як реакція на нову систему США CLOUD ACT [194], який направлений на дозвіл законним чином збирати персональні дані користувачів мережі Інтернет через компанії, які працюють в сфері обробки даних. Цей Закон використовує обґрунтування національної безпеки для затвердження широких повноважень за всіма методами збору даних, включаючи процес огляду національної безпеки. Однак DSL не описує, що є інтересом безпеки. Це створює невизначеність щодо технологічних корпорацій,яким чином можуть проводитися огляди національної безпеки, що має значні довгострокові наслідки для роботи. В результаті регіональні та місцеві органи влади мають повноваження на розробку власних законів, що стосуються безпеки даних [193].

Закон КНР про захист особистої інформації / Personal information protection law (PIPL) був також прийнятий у 2021 році, як доповнення до минулих, а також орієнтований на GDPR ЄС. [285] PIPL – всеоб'ємний закон про конфіденційність даних у Китаї, який спрямований на захист персональних даних осіб, що знаходяться в Китаї, незалежно від місця розташування процесора. Закон застосовується до організацій та осіб, які збирають, використовують, зберігають, передають або розкривають персональні дані осіб, що знаходяться в Китаї.

Адміністрація кіберпростору Китаю (CAC) може накладати адміністративні стягнення на організації, які порушують PIPL. Ці стягнення можуть включати штрафи до 50 мільйонів юанів (приблизно 7,7 мільйона доларів США) або 5% від річного доходу організації, залежно від того, що більше. CAC також може зобов'язати організації виправити свої порушення та призупинити свою діяльність. Особи, які несуть пряму відповідальність за порушення PIPL, можуть бути засуджені до 7 років позбавлення волі. На додаток до цих наслідків, організації, які не дотримуються PIPL, також можуть бути об'єктом приватних позовів від осіб, чия персональна інформація була використана неналежним чином.

Державні нормативно-правові акти, з урахуванням сучасного процесу цифровізації постають як фронтальними, що формують певні тренди щодо цифрової трансформації країн світу та активно формують правові механізми для регуляції інформаційного простору, захисту персональних даних і забезпечення національної кібербезпеки.

Це дозволяє розглядати питання цифрового регулювання, як направлений шлях щодо забезпечення з боку держав та урядів інформаційної безпеки як складової процесу регуляції з урахуванням особливостей регуляторної політики, кіберзагроз, технологічного суверенітету та впливу приватного сектора – особливо транснаціональних IT-корпорацій — на державну політику у сфері безпеки.

За цитатою І. Сопілко «Згідно Дж. Фрулінгеру, інформаційна безпека (також infosec, від англ. Information security) – це сукупність різних методів, за допомогою яких здійснюється захист даних від несанкціонованого доступу або змін під час їх зберігання або передачі з одного пристрою на інший» [137, с.106]

Однак у контексті протидії цифровому тоталітаризму поняття інформаційної безпеки набуває значно глибшого значення. Захист інформації у цьому випадку передбачає не тільки збереження конфіденційності, цілісності й доступності даних, але й захист особистості, суспільства та демократичних цінностей від авторитарних маніпуляцій через цифровий простір.

В умовах цифрового тоталітаризму, коли інформація перетворюється на інструмент контролю та пригнічення свобод громадян, виникає необхідність використовувати сучасні технології саме з позицій захисту прав людини, прозорості управлінських процесів та створення бар'єрів на шляху зловживань цифровими інструментами влади. Тому дисертантом було прийнято використовувати більш широке визначення, «надане Інститутом SANS: infosec – це процеси і методи, розроблені й реалізовані з метою захистити друковану, електронну, а також інформацію, представлену в іншій формі від несанкціонованого доступу, використання тощо» [137, с.106].

На погляд доктора юридичних наук І.М. Сопілко «найбільш повне визначення містить підхід В. Мороза, згідно з яким інформаційна безпека, з одного боку, являє собою стан, коли, з урахуванням реальних і потенційних загроз, інформаційна сфера зберігає свій сталий розвиток, а з іншого боку – це безперервний процес діяльності компетентних осіб із метою запобігти або протидіяти загрозам в інформаційній сфері, пов’язаний із використанням активних заходів інформаційного впливу» [137, с.106].

Таким чином, протидія цифровому тоталітаризму передбачає застосування не тільки захисних механізмів, але й створення умов для

проактивного реагування на інформаційні маніпуляції, зокрема шляхом розвитку сучасних цифрових інструментів моніторингу, аналізу, прогнозування і нейтралізації загроз інформаційному суверенітету та особистим свободам громадян.

Так, з метою поглиблення міжнародного співробітництва, підвищення ефективності боротьби з кіберзагрозами та гармонізації національного законодавства у сфері кібербезпеки з нормативно-правовими актами Європейського Союзу, НАТО та іншими міжнародними стандартами, Україна здійснила низку вагомих кроків. Зокрема, було ратифіковано Конвенцію Ради Європи про кіберзлочинність, яка передбачає комплексну взаємодію держав у протидії злочинам у сфері інформаційних технологій, а також інші важливі міжнародні договори та документи.

У рамках реалізації цих ініціатив, а також за сприяння і безпосередньої підтримки Трастового фонду НАТО, в Україні створено спеціалізовані Ситуаційні центри при Службі безпеки України (СБУ) та Державній службі спеціального зв'язку та захисту інформації (ДССЗЗІ). Дані центри відіграють ключову роль у моніторингу кіберпростору, оперативному виявленні загроз, оцінці ризиків та негайному реагуванні на інциденти, спрямовані проти національних інформаційних систем України.

Виконуючи покладені на них завдання, ситуаційні центри здійснюють постійний аналіз та координацію заходів із запобігання і нейтралізації кібернетичних атак, а також надають оперативну допомогу іншим органам державної влади, що беруть участь у забезпеченні національної кібербезпеки.

Водночас завдяки створенню цих інституційних механізмів та інтеграції з міжнародними мережами співпраці, у структурі Національної поліції України ефективно функціонує Національний контактний пункт цілодобового формату 24/7. Його завданням є оперативне реагування на комп'ютерні злочини, координація зусиль національних правоохоронних структур, а також забезпечення обміну актуальною інформацією та

передовим досвідом з міжнародними партнерами щодо протидії кіберзлочинності.

«Кіберборотьба й кіберзахист стали одними із ключових елементів гібридної війни. Наші фахівці та хакери-волонтери не лише успішно протистоять нападам, а й завдають дошкульних ударів у відповідь. Торік зафіксовано понад 1,25 мільйона DDoS-атак на російську інфраструктуру (це 8,4% від усіх кібератак у світі). За оцінками керівника служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО Наталії Ткачук, Україна – єдина держава, яка змогла здобути перевагу у протистоянні кібератакам та інформаційній агресії РФ» [49].

Вважається, що Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку) відповідає за формування та реалізацію державної політики в галузі кіберзахисту, зокрема щодо забезпечення безпеки об'єктів критичної інфраструктури та державних інформаційних ресурсів у кіберпросторі.

Крім того, до компетенції цієї установи належить підготовка кваліфікованих фахівців у сфері кібербезпеки, що передбачає використання гнучких освітніх підходів, здатних оперативно адаптуватися до постійно змінюваних умов і викликів сучасності. За думкою низки дослідників, а саме О. Азюковського, А. Павличенко, О. Пащенко, Т. Медведовської існує лише два шляхи підготовки спеціалістів на державному рівні :

«перший – впровадження змін у систему вищої освіти. Зараз абітурієнтам, яких цікавить робота, пов'язана із захистом інформації, доступна лише одна опція – спеціальність «Кібербезпека» у галузі знань «Інформаційні технології». Однак її стандарти не забезпечують майбутнім фахівцям увесь спектр знань та навичок, необхідних на сучасному ринку праці. Вихід – розширення переліку освітніх можливостей у співпраці з МОН. Однак кооперація з іншою державною структурою ускладнює процес і розтягує його в часі;

другий шлях – імплементувати міжнародні стандарти та кращі світові практики і розробити кваліфікаційну рамку професій у галузі кібербезпеки. Тобто – розширити перелік можливих посад для кіберспеціалістів в українському Класифікаторі професій, а також створити для них відповідну систему оцінювання фаху. Саме у цьому напрямі Держспецзв'язку наполегливо працює останні роки. У результаті кількість професій галузі кіберзахисту та захисту інформації збільшилася із 2 до 27» [146].

Запропоновані дії є важливими кроками на шляху до формування стійкої системи протидії цифровому тоталітаризму. Розширення освітніх можливостей у сфері кібербезпеки та впровадження нових стандартів підготовки фахівців є стратегічним чинником посилення державної спроможності виявляти й нейтралізувати сучасні цифрові загрози. Адже цифровий тоталітаризм використовує передові технології контролю, моніторингу й маніпуляції даними, що вимагає від спеціалістів не лише базових знань, але й комплексного розуміння сучасних тенденцій і технологічних викликів.

У контексті сучасних викликів цифрової безпеки надзвичайно актуальним є питання формування ефективних механізмів підбору й утримання висококваліфікованих кадрів у сфері кібербезпеки. Традиційні методи рекрутингу, які передбачають відкритий доступ до особистої інформації кандидата, нерідко призводять до упередженості, суб'єктивних оцінок та дискримінації під час процесу відбору.

Водночас стрімке зростання попиту на професіоналів із захисту інформації потребує впровадження більш конфіденційних, об'єктивних та орієнтованих на інтереси кандидатів підходів до рекрутингу. Відповіддю на цю потребу стало створення спеціалізованих платформ, які реалізують принцип метчингу – підбору спеціалістів на основі чіткої відповідності їхніх компетенцій запитам роботодавців, забезпечуючи при цьому високий рівень захисту персональних даних та конфіденційності користувачів.

Одним із прикладів таких інноваційних рішень стала платформа CyberPeople. «Цього року в Україні запрацювала бета-версія метчингової платформи для підбору професіоналів у галузі кібербезпеки – CyberPeople. Вона працює за принципом відповідності навичок фахівців запитам потенційних роботодавців та орієнтована у першу чергу на інтереси кандидатів. На відміну від рекрутингових платформ, таких як LinkedIn, де одразу видно всі попередні місця роботи, трудову історію та фото власника профілю, CyberPeople захищає кіберспеціалістів від оціночних суджень і неетичної поведінки з боку рекрутерів» [44].

Отже, вважається, що CyberPeople буде сприяти створенню цифрового простору, де пріоритетом є професійні якості, а не особисті дані, посилюючи опір суспільства проти проявів цифрового тоталітаризму та необґрунтованого контролю.

З огляду на постійне зростання загроз у сфері інформаційної безпеки та викликів цифрового тоталітаризму, розвиток міжнародного співробітництва у питаннях кіберзахисту набуває особливого значення.

Враховуючи важливу роль, яку відіграють сучасні технології у забезпеченні безпеки та захисту державних і громадянських свобод, міжнародні партнери України приділяють значну увагу підтримці українських ініціатив у цій галузі. Особливо важливим партнером України в цьому контексті виступають Сполучені Штати Америки, які послідовно висловлюють підтримку прагненню України зміцнювати свою систему кібербезпеки.

Зокрема, Сполучені Штати Америки підтвердили свою прихильність щодо підтримки України у створенні надійної національної системи кібербезпеки та впровадженні комплексних заходів, спрямованих на її посилення. Палата представників Конгресу США підтримала законопроєкт «Ukraine Cybersecurity Cooperation», який визначає фундаментальні засади та пріоритетні напрями двосторонньої співпраці у сфері кіберзахисту.

Ключовими напрямами такої співпраці, згідно з цим законопроєктом, планується :

- вдосконалення систем безпеки урядових систем, передусім тих, які захищають критичну інфраструктуру України;

- зменшення залежності від російських інформаційно-комунікаційних технологій;

- нарощування потенціалу, розширення обміну інформацією щодо кібербезпеки; співробітництво в кіберпросторі» [90, с.142].

Також у фокусі уваги сторін були такі питання, як: технологічне забезпечення зв'язку п'ятого покоління 5G, розбудова кіберпотенціалу, засад міжнародної політики стосовно забезпечення цифрового інформаційного простору, у тому числі перспективна участь у багатосторонніх заходах (форумах, конференціях, самітах), питання публічної відповідальності за наслідками кібератак [90, с .143]. На думку, дослідників О. Трофименко, Ю. Прокоп, Н. Логінова , О. Задерейко:

«Серед першочергових завдань, які стоять перед державними інститутами України в рамках забезпечення інформаційного та цифрового суверенітетів, є:

- здійснення автоматичного моніторингу свого інформаційного простору;

- впровадження законодавства про відповідальність за контент;

- впровадження законодавства, яке регулює фільтрацію інтернет-контенту;

- недопущення використання новітніх інформаційних технологій для поширення соціально шкідливих ідей і закликів (расизму, шовінізму, радикального націоналізму);

- правовий захист національної культури і мови від впливу домінуючих в інформаційному плані країн;

- знаходження соціально прийнятного балансу між свободою слова і поширенням інформації та невід'ємним правом держави забезпечувати незалежну політику;

- захист від культурної експансії зарубіжних інтернет-ресурсів;

- перехід державних установ на використання програмного та технічного забезпечення власної розробки і виробництва» [142].

Віртуальні приватні мережі (VPN) стали незамінним інструментом у боротьбі за цифрові права і свободу слова в сучасному світі. В умовах глобалізації, коли інтернет перетворився на основне джерело інформації, спілкування та вираження думок, авторитарні уряди дедалі активніше використовують цензуру для контролю громадян. Однак, як свідчить практика, люди знаходять способи протидіяти цифровій диктатурі, і VPN є одним із найбільш ефективних інструментів у цьому процесі.

Поширеність VPN у країнах із суворою цифровою цензурою, таких як Китай, Іран, Росія, Туреччина та Білорусь, демонструє значну стійкість громадянського суспільства. Наприклад, за оцінками Freedom House (2022), понад 90 мільйонів китайських громадян регулярно використовують VPN для отримання доступу до глобального інтернету [164].

В Ірані, за даними міжнародної правозахисної організації Article 19 (2023), близько 64% іранських користувачів регулярно використовують VPN для доступу до заблокованих державою соціальних мереж, таких як Telegram, WhatsApp та Instagram [235].

Водночас ситуація в Росії істотно погіршилася після повномасштабного вторгнення в Україну в лютому 2022 року. Російська влада активізувала цензуру, блокуючи незалежні медіа та популярні міжнародні платформи, зокрема Facebook, Twitter, Instagram і навіть Wikipedia.

Це призвело до різкого зростання попиту на VPN-сервіси серед росіян: за даними компанії Top10VPN (2023), кількість завантажень VPN-додатків після початку війни зросла у 20 разів [254].

Однак, попри величезні переваги, VPN не є абсолютним захистом. Держави, які практикують жорсткий контроль за інтернетом, активно протидіють VPN-сервісам шляхом юридичного тиску, блокування серверів, технічних атак і навіть поширення пропаганди, яка дискредитує використання VPN. Китайська влада регулярно оновлює «Великий китайський файрвол», використовуючи технології штучного інтелекту та машинного навчання, щоб ефективніше виявляти і блокувати VPN-трафік.

Також важливим аспектом є міжнародна підтримка цифрових свобод. Правозахисні організації та технологічні компанії активно працюють над розробкою нових, більш захищених і складних у виявленні технологій обходу цензури. В цьому контексті надзвичайно важливою є роль міжнародної спільноти, яка може надавати фінансову та технічну підтримку активістам і незалежним ЗМІ, що працюють у репресивних умовах.

У довгостроковій перспективі ефективність VPN залежатиме від інноваційності розробників технологій захисту конфіденційності, їх здатності швидко адаптуватися до нових методів цензури та готовності міжнародної спільноти активно підтримувати свободу інтернету. Таким чином, використання VPN символізує не лише прагнення людей до свободи інформації, але й ширшу боротьбу за фундаментальні людські права в умовах цифрової епохи.

Останнім часом Сполучені Штати Америки висловлюють занепокоєння стрімким розвитком цифрових технологій у Китаї, що, на їхню думку, створює потенційну загрозу в галузі кібербезпеки.

У відповідь на існуючі виклики та загрози, Сенат США розпочав розробку законодавчої ініціативи, спрямованої на державну підтримку виробництва напівпровідникових чипів.

Таким чином, у світлі зростаючої кількості кібератак, а також численних випадків несанкціонованого витоку та викрадення конфіденційної інформації, питання забезпечення кібербезпеки набуло особливої актуальності для країн, суспільств та урядів. Здебільшого

відповідальність за подібні кібератаки та протиправну діяльність офіційні уряди покладає один на одного або на хакерські угруповання, пов’язані з протилежними країнами-сусідами.

Цифровий тоталітаризм, що передбачає використання передових технологій для масового спостереження, цензури та обмеження інформаційної свободи, є серйозним викликом для демократичних країн. У зв’язку з цим питання протидії цифровому тоталітаризму набуває особливої актуальності та потребує розробки комплексних стратегій із використанням сучасних технологій, спрямованих на забезпечення кібербезпеки, захисту прав людини та зміцнення цифрового суверенітету демократичних суспільств.

Одним із головних викликів для демократичних країн є залежність від постачання критичних технологій із держав, що використовують цифрові інновації для встановлення авторитарного контролю та впливу на міжнародній арені. Напівпровідникова промисловість, штучний інтелект, квантові обчислення та кібербезпека є ключовими секторами, у яких необхідно розвивати національні технологічні потужності з метою зменшення ризику зовнішнього впливу.

Створення незалежної високотехнологічної екосистеми, що включає наукові дослідження, розробку мікрочипів та їх виробництво, є стратегічно важливим завданням. США, Європейський Союз та інші демократичні країни вже розробляють ініціативи, спрямовані на підтримку національного виробництва напівпровідників.

Демократичні держави мають розвивати передові технології у сферах штучного інтелекту, кібербезпеки та квантових обчислень, що дозволить зменшити технологічний розрив з авторитарними режимами та забезпечити конкурентоспроможність на світовому ринку. Захист критично важливих цифрових систем потребує створення стійких та надійних механізмів інфраструктури, які є менш вразливими до зовнішнього впливу та кібератак. Застосування штучного інтелекту є ключовим у протидії цифровому

тоталітаризму, адже такі технології можуть бути використані для ідентифікації загроз, відстеження маніпуляцій та боротьби з дезінформацією.

Використання алгоритмів машинного навчання дозволяє аналізувати великі обсяги даних у режимі реального часу та виявляти потенційні кіберзагрози.

Такі системи здатні прогнозувати кібератаки, забезпечуючи ефективний захист цифрових платформ. Технології штучного інтелекту можуть аналізувати контент у медіапросторі, виявляючи фейкові новини та маніпулятивні матеріали, що використовуються тоталітарними режимами для дестабілізації демократичних суспільств.

Однією з ключових загроз цифрового тоталітаризму є масове спостереження за громадянами та обмеження їхніх прав у цифровому просторі. Важливою складовою захисту демократичних цінностей є забезпечення приватності даних та свободи слова в інтернеті. Використання сучасних криптографічних рішень дозволяє забезпечити конфіденційність персональних даних та захистити комунікації від державного контролю.

Створення незалежних платформ, що використовують технологію блокчейн, допомагає захистити інформацію від цензури та фальсифікації. Оскільки цифровий тоталітаризм є глобальною загрозою, його ефективна протидія можлива лише шляхом міжнародної співпраці між демократичними країнами. Обмін інформацією між державами щодо кібератак, створення міжнародних механізмів реагування та запровадження спільних стандартів цифрової безпеки є критично важливими. Розвиток міжнародних програм для фінансування досліджень у галузі штучного інтелекту, квантових технологій та кіберзахисту сприятиме посиленню конкурентоспроможності демократичних держав у цифровій сфері.

Одним із найефективніших способів протидії цифровому тоталітаризму є підвищення рівня цифрової грамотності серед громадян. Впровадження курсів з кібербезпеки, інформаційної гігієни та

розпізнавання маніпуляцій є важливим для формування обізнаного суспільства.

Навчання населення способам захисту своїх даних, розпізнаванню дезінформації та методам протидії цифровому авторитаризму сприятиме зниженню впливу маніпулятивних технологій.

За рейтингами WDCI (World Digital Competitiveness Index) у 2019 році найбільш конкурентоспроможними за рівнем цифрових регулювання та перетворень, впроваджених в економіку, стали США, Сінгапур і Швеція [280].

Оцінювання рейтингу здійснювалося на основі рівня інтеграції та ефективного застосування інформаційно-комунікаційних технологій (ІКТ) у різних сферах суспільного життя та економічного розвитку. Аналіз враховував широкий спектр факторів, які визначають цифрову конкурентоспроможність держав, зокрема рівень технологічної інфраструктури, ступінь підготовленості людського капіталу до роботи в цифровому середовищі, ефективність державного управління у впровадженні цифрових рішень, а також загальний вплив ІКТ на економічний розвиток та соціальну динаміку.

За результатами оцінювання, проведеного у 2024 році, лідерські позиції за рівнем впровадження ІКТ у національні економіки посіли такі країни, як Сінгапур, Швейцарія та Данія.[280] Ці держави демонструють високий рівень цифрової трансформації завдяки комплексним стратегіям впровадження новітніх технологій, розвиненій цифровій інфраструктурі, ефективному державному регулюванню та високій цифровій грамотності населення.

Як засвідчують рейтингові показники, саме країни Європейського Союзу та розвинені азійські держави залишаються флагманами цифрової модернізації та задають напрям подальшого розвитку глобального цифрового середовища.

У сучасних економічних умовах розвинені країни приділяють значну увагу цифрового регулювання економіки. Зокрема, у 2010 році Європейський Союз ініціював «Цифровий порядок денний» (Digital Agenda for Europe), який встановив конкретні цілі для досягнення до 2020 року [160].

Ключовим елементом цієї ініціативи було створення Єдиного цифрового ринку, спрямованого на забезпечення вільного руху товарів, осіб, послуг і капіталу, а також надання фізичним та юридичним особам безперешкодного доступу до онлайн-активностей за справедливими умовами конкуренції та високим рівнем захисту даних.

У 2015 році ЄС представив Стратегію Єдиного цифрового ринку, яка базувалася на трьох основних напрямках: «*Доступ, Середовище та Економіка+Суспільство*». Ці напрями розроблені за для забезпечення кращого доступу для споживачів і підприємств до цифрових товарів і послуг по всій Європі, створення належних та рівних умов для процвітання цифрових мереж та інноваційних послуг, а також максимізація потенціалу зростання цифрової економіки [160].

Ця стратегія мала на меті сприяти економічному зростанню, збільшенню робочих місць, конкуренції, інвестиціям та інноваціям у ЄС.

У березні 2021 року Європейська комісія представила бачення цифрової трансформації Європи до 2030 року, відоме як «Цифровий компас до 2030 року». Ця політична програма спрямована на досягнення цифрової трансформації економіки та суспільства ЄС, спираючись на чотири кардинальні точки: цифрові навички, безпечна та ефективна цифрова інфраструктура, цифрова трансформація бізнесу та цифровізація державних послуг [160].

Таким чином, Європейський Союз продовжує активно працювати над поглибленням цифрової інтеграції, адаптуючи свої стратегії до нових викликів та можливостей цифрової епохи.

Розширення та розповсюджене впровадження цифрових технологій істотно впливає на економічні процеси та суспільне життя, спричиняючи масштабну трансформацію ключових аспектів виробництва, зайнятості та міжособистісних взаємовідносин.

Одним із найбільш помітних наслідків цієї трансформації є поступове відходження від традиційних моделей праці, які передбачають фізичну присутність працівників у робочих просторах, та перехід до нових, більш гнучких і адаптивних форм зайнятості, зокрема дистанційної та проектної роботи.

3.3. Інституційна спроможність міжнародних та національних систем забезпечення прав людини в умовах інформаційного суспільства

Протягом останнього десятиліття більшість цифрових прав і свобод особи отримали відповідні гарантії захисту, що закріплені чинними міжнародними правовими актами. Водночас наукова спільнота висловлює занепокоєння щодо недостатньої ефективності такого захисту, зумовленої відсутністю розвиненої правозастосовної практики. Зокрема, нестача прецедентних рішень міжнародних судів та інших правозастосовних механізмів ускладнює реалізацію та ефективне забезпечення правових гарантій у сфері цифрових прав. Міжнародні стандарти цифрових прав людини частково регулюються низкою фундаментальних міжнародно-правових документів, які встановлюють загальні принципи та механізми їхнього захисту в цифровому середовищі.

Одним із перших ключових документів, що закріплює основні права людини, є Загальна декларація прав людини, прийнята Генеральною Асамблеєю ООН у 1948 році. Вона містить положення про право на приватність та свободу вираження поглядів, які набувають особливого значення в умовах розвитку інформаційних технологій і цифрового

суспільства. Так, стаття 12 проголошує, що ніхто не може зазнавати свавільного втручання в його особисте життя, сім'ю, житло чи кореспонденцію, а стаття 19 закріплює право кожного на свободу переконань і вільне висловлення думок, включно з можливістю шукати, отримувати та поширювати інформацію будь-якими засобами та незалежно від кордонів.

Іншим важливим нормативним актом є Міжнародний пакт про громадянські та політичні права, прийнятий Генеральною Асамблеєю ООН у 1966 році (набрав чинності в 1976 році) [234].

У його статті 17 закріплено захист права на приватне життя, а стаття 19 гарантує свободу вираження поглядів, що охоплює право на отримання, передачу та розповсюдження інформації безперешкодно, що є критично важливим у цифрову епоху.

Одним із найбільш ефективних механізмів захисту прав людини у Європі є Європейська конвенція з прав людини (ECHR), прийнята Радою Європи в 1950 році (набрала чинності у 1953 році) [52].

Стаття 8 цієї Конвенції гарантує кожному право на повагу до його приватного і сімейного життя, житла та кореспонденції, що є важливим у контексті захисту персональних даних в інтернеті.

Стаття 10 визнає право на свободу вираження поглядів, включаючи право отримувати та передавати інформацію без втручання держави.

Однак, за виняткових обставин, відповідно до статті 15, уряди держав-учасниць можуть тимчасово обмежувати певні права та свободи, якщо це є необхідним у ситуаціях надзвичайного стану.

Першим міжнародним документом, що спеціально регулює питання захисту персональних даних, є Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108), ухвалена в 1981 році [197].

Вона встановлює обов'язкові стандарти для країн-учасниць щодо захисту даних, що є ключовим аспектом у цифрову епоху.

Ще одним важливим нормативним актом, що забезпечує захист персональних даних у цифровому середовищі, є Загальний регламент про захист даних Європейського Союзу (GDPR), ухвалений у 2016 році та застосовуваний з 2018 року [222].

Він встановлює високі стандарти безпеки особистої інформації, вимагаючи від компаній та державних установ забезпечувати конфіденційність і захист персональних даних користувачів.

Крім того, у сфері боротьби з кіберзлочинністю значну роль відіграє Будапештська конвенція (Кіберзлочинна конвенція), ухвалена Радою Європи у 2001 році [267].

Це перший міжнародний договір, спрямований на уніфікацію національних законодавств щодо протидії кіберзлочинам, а також на розвиток міжнародного співробітництва у цій сфері. Документ визначає юридичні механізми для переслідування осіб, які скоюють злочини в кіберпросторі, зокрема у сфері хакерства, шахрайства та поширення шкідливого програмного забезпечення.

Таким чином, міжнародні документи встановлюють важливі правові рамки для захисту цифрових прав людини, охоплюючи такі аспекти, як право на приватність, свобода вираження поглядів, захист персональних даних та боротьба з кіберзлочинністю.

Їхнє дотримання є необхідним для забезпечення прав людини в умовах глобалізації цифрових технологій.

Резолюція ООН про право на приватність у цифровому віці є важливим міжнародним документом, що закликає держави-учасниці забезпечувати дотримання прав людини в цифровому середовищі, зокрема захист права на приватність.

Вона підкреслює необхідність захисту персональних даних та конфіденційності в умовах стрімкого розвитку цифрових технологій та глобальної взаємопов’язаності.

Одним із ключових нормативних актів у цій сфері є резолюція Генеральної Асамблеї ООН від 17 грудня 2018 року (A/RES/73/179) – «Право на недоторканність приватного життя в цифрову епоху» [275].

У її положеннях, зокрема у частинах 2 і 3, наголошується на тому, що Інтернет має глобальний та відкритий характер, а також визнається, що розвиток інформаційно-комунікаційних технологій є одним із ключових рушіїв прогресу у сфері розвитку суспільства. У цьому контексті резолюція підкреслює, що права людини, які визнаються та захищаються поза межами цифрового середовища, повинні забезпечуватися і в Інтернеті, включаючи право на недоторканність приватного життя.

З огляду на зростаючу залежність сучасного суспільства від цифрових технологій, питання можливих обмежень цифрових прав людини набуває особливої актуальності. Будь-які такі обмеження мають оцінюватися з позиції верховенства права, що гарантує їхню законність, обґрунтованість і пропорційність.

Особливо це важливо в умовах нових глобальних викликів, з якими стикається міжнародна спільнота. Серед таких викликів можна виокремити:

1) Глобальна пандемія COVID-19 стала серйозним випробуванням для цифрових прав людини, оскільки багато держав у відповідь на поширення вірусу впроваджували технології стеження, що призвело до посилення контролю за цифровими комунікаціями. Наприклад, у багатьох країнах запроваджувалися мобільні додатки для відстеження контактів хворих, такі як COVIDSafe” в Австралії, TraceTogether” у Сінгапурі та Corona-Warn-App” у Німеччині. Хоча ці інструменти мали на меті боротьбу з пандемією, вони викликали серйозні дискусії щодо приватності, адже деякі з них збирали персональні дані громадян, що могло призвести до їх неналежного використання державними органами або комерційними структурами. Водночас у деяких країнах фіксувалися випадки використання пандемічних заходів для посилення цензури та контролю над інформаційним простором,

наприклад, у Китаї та Росії блокувалися незалежні джерела інформації під приводом боротьби з «фейковими новинами» про COVID-19.

2) Терористичні загрози та посилення заходів кібербезпеки призводять до дедалі активнішого використання державами механізмів цифрового контролю. Терористичні угруповання, такі як «Ісламська держава» (ISIS) та «Аль-Каїда», активно використовували соціальні мережі та месенджери для вербування нових членів і поширення своєї ідеології. У відповідь багато країн запровадили системи моніторингу інтернет-простору та масового збору даних. Наприклад, у Франції та Великій Британії ухвалювалися закони, що розширювали повноваження спецслужб щодо перехоплення комунікацій підозрюваних осіб. У США ухвалення «Патріотичного акту» та програми АНБ (Агентства національної безпеки) спричинили хвилю критики через надмірне втручання в особисте життя громадян. Аналогічно, у Китаї діє масштабна система цифрового контролю, включаючи «Великий китайський фаєрвол», який використовується не лише для протидії кіберзлочинності, а й для обмеження доступу до незалежної інформації.

3) Військова агресія Російської Федерації проти України, що триває з 2014 року та особливо загострилася після повномасштабного вторгнення у 2022 році, супроводжується широкомасштабною інформаційною війною, кіберзагрозами, масовими кібератаками та спробами цензурувати цифровий простір. Російські хакерські групи, такі як «Sandworm», «Fancy Bear» та «Cozy Bear», неодноразово здійснювали атаки на українські державні установи, енергетичну інфраструктуру та медіа. Наприклад, у 2015 та 2016 роках кібератаки на енергетичну систему України призвели до масштабних відключень електроенергії.

У 2022 році було здійснено атаки на урядові сайти та банківські системи, що стало частиною гібридної війни. Окрім кібератак, Росія активно поширює дезінформацію в соціальних мережах, використовуючи фабрики тролів та алгоритми маніпуляції громадською думкою. Водночас в самій

Росії відбувається жорстке обмеження цифрових прав – заблоковано доступ до незалежних ЗМІ, соціальних мереж (Facebook, Instagram, Twitter), а також ухвалено закони, що передбачають кримінальне переслідування за критику влади в інтернеті.Також блокуються дії незалежних медіа групп та сервісів, а також VPN-сервісів, що значно обмежують права та можливості громадян отримувати альтернативну інформацію у світі

Досліджуючи питання прав людини в онлайн-просторі, необхідно окремо розглянути проблему права особи на доступ до Інтернету, оскільки це питання відіграє ключову роль у забезпеченні реалізації інших фундаментальних прав і свобод. Хоча право на доступ до Інтернету поки що не визнане офіційним правом людини на міжнародному рівні, численні міжнародні організації та правозахисні структури постійно наголошують на його критичній важливості для розвитку демократії, громадянського суспільства та реалізації інформаційних прав людини. Наприклад, у резолюціях ООН, прийнятих у 2011, 2016 і 2021 роках, Інтернет визнається важливим засобом для здійснення права на свободу вираження поглядів та доступу до інформації [276].

Доступ до Інтернету забезпечує не лише право на інформацію, а й сприяє реалізації інших прав, таких як право на освіту, право на працю, право на участь у громадському житті. Наприклад, у 2020 році, під час глобальної пандемії COVID-19, близько 1,6 мільярда учнів та студентів по всьому світу були змушені перейти на дистанційне навчання [274]. Водночас у країнах із низьким рівнем доступу до Інтернету мільйони дітей фактично залишилися без можливості отримувати освіту, що підкреслює нерівність у цифровому просторі.

Право на доступ до Інтернету є складовою частиною сучасних цифрових прав людини та повинно бути визнане та закріплене як національним, так і міжнародним законодавством. Для його реалізації важливо забезпечити два основні аспекти:

Перший аспект – «Заборона незаконного обмеження доступу до Інтернету». Обмеження або повне відключення доступу до Інтернету є серйозним порушенням цифрових прав людини, оскільки воно може призводити до цензури, обмеження свободи слова, порушення права на доступ до інформації та ізоляції громадян від світової спільноти.

Світова практика показує, що авторитарні режими часто використовують блокування Інтернету як інструмент контролю над громадською думкою та засіб придушення протестів. Це створює небезпечний прецедент, що підриває демократичні цінності та обмежує можливості громадян для отримання достовірної інформації та комунікації з рештою світу Так, існують приклади незаконного блокування мережі Інтернет :

М’янма у 2021 році, після після військового перевороту заблокували доступ до Інтернету та соціальних мереж, щоб придушити громадські протести та обмежити комунікацію між активістами» [233].

У Ірані у 2019 році, під час протестів проти підвищення цін на паливо уряд повністю відключив Інтернет у країні на кілька днів, що призвело до ізоляції населення та неможливості отримання інформації [171].

Ефіопія також має приклад відключення Інтернету у 2020 році. В ході збройного конфлікту в регіоні Тиграй, тим самим унеможливили комунікацію серед громадян та повсталих забороняючи поширювати інформацію в соціалних мережах про гуманітарну кризу.

Міжнародна спільнота має стрімкими та рішучими діями реагувати на такі приклади заборон, розробляючи механізми захисту, прозорих підходів до регулювання цифрових прав, а також залучення експертів для підтримки альтернативних або децентралізованих джерел виходу до мережі Інтернет.

Другий аспект – Обов’язок держави сприяти розширенню доступу до Інтернету. Держави не лише повинні утримуватися від свавільного блокування Інтернету, але й активно сприяти його розвитку та забезпечувати максимально широкий доступ для своїх громадян. Це

питання особливо актуальне для країн, де значна частина населення не має якісного Інтернет-з'єднання або взагалі позбавлена можливості підключення. Саме розвиток інфраструктури забезпечить доступ до широкосмугового Інтернету в усіх населених пунктах, включно з віддаленими та сільськими районами. Підтримка ініціатив із забезпечення покриття мобільним Інтернетом 4G/5G навіть у найменш доступних регіонах.

Створення публічних точок Wi-Fi у громадських місцях (бібліотеки, навчальні заклади, лікарні, транспортні вузли тощо). Використання супутникового Інтернету (наприклад, програм SpaceX Starlink, OneWeb, Project Loon) у регіонах із низькою інфраструктурною доступністю. Надання безкоштовного або субсидованого Інтернет-доступу для малозабезпечених верств населення є важливим напрямом забезпечення цифрової рівності та соціальної справедливості. Доступ до Інтернету відіграє ключову роль у реалізації фундаментальних прав людини, таких як право на освіту, працю, доступ до інформації та медичних послуг. Багато держав та міжнародних організацій розробляють програми, спрямовані на забезпечення доступу до мережі для соціально вразливих груп, що включає введення спеціальних тарифних планів і надання безкоштовного доступу до основних інформаційних ресурсів.

У Сполучених Штатах Америки діє програма Affordable Connectivity Program (ACP), ініційована Федеральною комісією зі зв'язку США. Вона передбачає фінансову допомогу малозабезпеченим сім'ям для покриття витрат на Інтернет-послуги, що становить до 30 доларів США на місяць, а для домогосподарств на території корінних народів – до 75 доларів США.

Окрім цього, програмою передбачена можливість отримання знижки на придбання пристроїв, зокрема ноутбуків і планшетів. У країнах Європейського Союзу реалізуються подібні ініціативи зі зниження вартості Інтернет-послуг для соціально незахищених категорій громадян.

Наприклад, у Франції та Німеччині існують соціальні тарифи, що дозволяють громадянам із низьким доходом отримувати Інтернет за зниженими цінами або безкоштовно. У Великій Британії оператори зв'язку, такі як BT та Virgin Media, пропонують спеціальні тарифи для людей, які отримують соціальну допомогу, зокрема Universal Credit.

В Індії урядова ініціатива BharatNet спрямована на розвиток цифрової інфраструктури в сільських районах, а для малозабезпечених верств населення передбачені пільгові та безкоштовні тарифні плани залежно від регіону та рівня доходу. У Бразилії діє програма «Internet for All» (Internet para Todos), що передбачає надання державної підтримки у розширенні доступу до Інтернету для шкіл, лікарень і малозабезпечених громадян, включаючи субсидовані тарифи та безкоштовний мобільний Інтернет для доступу до державних сервісів [236].

Окрім програм, що забезпечують субсидований доступ до Інтернету, низка ініціатив спрямована на надання безкоштовного підключення до певних категорій цифрових послуг.

Однією з найвідоміших ініціатив є Free Basics, запущена компанією Meta (Facebook). Вона діє у понад 30 країнах, включаючи Індію, Пакистан, Нігерію, Філіппіни, Колумбію та інші держави, і передбачає надання безкоштовного доступу до обмеженого переліку веб-сайтів, що містять освітню, економічну та соціальну інформацію.

Проте ініціатива зазнала критики через порушення принципу мережевої нейтральності, оскільки користувачі можуть отримувати доступ лише до певних ресурсів, відібраних компанією. Іншим прикладом є програма Google Station, яка передбачала створення безкоштовних Wi-Fi-точок у громадських місцях у таких країнах, як Індія, Індонезія, Мексика, Нігерія та інші. Особливо успішно вона працювала в Індії, де понад 400 залізничних станцій були обладнані безкоштовним Інтернетом, поки ініціативу не було згорнуто у 2020 році [269].

Крім того, уряди та міжнародні організації впроваджують програми безкоштовного доступу до Інтернету в освітніх і медичних установах. У межах проекту Internet.org, який діє в Африці та Латинській Америці, забезпечується підключення університетів і бібліотек до глобальної мережі, що дозволяє студентам отримувати доступ до навчальних матеріалів незалежно від їхнього соціально-економічного статусу [269].

Наприклад, у Руанді, Гані та Мексиці державні установи фінансують розширення цифрової інфраструктури у вищих навчальних закладах. Також перспективним напрямом розвитку є використання супутникового Інтернету для розширення покриття у важкодоступних регіонах. Наприклад, компанія SpaceX у межах проекту Starlink у 2022 році надала безкоштовний супутниковий Інтернет для підтримки комунікацій в Україні після пошкодження традиційної інфраструктури [279].

Аналогічні ініціативи розглядаються в Африці та Південній Америці, де компанії OneWeb та інші планують розгортати супутникові мережі для надання Інтернет-доступу в регіонах із низькою цифровою доступністю [172].

Отже, сучасні держави та міжнародні організації активно працюють над розширенням доступу до Інтернету для соціально вразливих груп населення. Введення соціальних тарифів, надання безкоштовного доступу до основних інформаційних ресурсів, розвиток цифрової інфраструктури та впровадження супутникового Інтернету є ключовими механізмами для зменшення цифрового розриву та забезпечення рівноправного доступу до цифрових технологій у всьому світі.

Законодавче закріплення права на доступ до Інтернету стало важливим напрямом розвитку цифрових прав у низці країн. Деякі держави вже визнали цей доступ базовим правом своїх громадян та закріпили його на законодавчому рівні.

Фінляндія у 2010 році стала першою країною світу, яка офіційно закріпила на законодавчому рівні обов’язок інтернет-провайдерів

забезпечувати громадянам доступ до мережі зі швидкістю не менше 1 Мбіт/с. Це рішення було частиною національної стратегії цифрового розвитку, спрямованої на гарантування рівного доступу до цифрових технологій для всіх жителів країни, включаючи віддалені та малозаселені регіони [212].

Франція в 2009 році стала однією з перших країн, де доступ до Інтернету був офіційно визнаний складовою частиною фундаментальних прав людини. Конституційний суд Франції постановив, що право на доступ до Інтернету є невід'ємною частиною свободи вираження поглядів, що гарантується статтею 11 Декларації прав людини і громадянина 1789 року. Таким чином, будь-які спроби державного обмеження або відключення Інтернету без законних підстав розглядаються як порушення прав громадян [196].

В Індії у 2019 році Верховний суд країни ухвалив історичне рішення, згідно з яким доступ до Інтернету було визнано фундаментальним правом громадян. Суд постановив, що обмеження або відключення Інтернету суперечить принципам демократії та конституційним гарантіям свободи слова та інформації. Це рішення стало наслідком тривалих обмежень доступу до Інтернету в регіоні Джамму та Кашмір, де уряд Індії тимчасово заблокував цифрові комунікації, що викликало серйозну критику як усередині країни, так і на міжнародному рівні [240].

Таким чином, ці країни стали важливими прикладами того, як держави можуть на законодавчому рівні гарантувати доступ громадян до цифрових ресурсів, визнаючи його не просто технічною можливістю, а невід'ємною частиною демократичних свобод і прав людини. Глобальні ініціативи з розширення доступу до Інтернету є ключовими інструментами для зменшення цифрового розриву, особливо у віддалених та малозаселених регіонах світу. Багато урядів, міжнародних організацій та технологічних компаній реалізують проекти, спрямовані на покращення інфраструктури,

розвиток цифрових навичок та забезпечення доступу до онлайн-ресурсів для мільйонів людей.

Однією з таких ініціатив є "Internet para Todos" (Інтернет для всіх) – проект, запущений у Латинській Америці спільно компаніями Facebook (тепер Meta), Telefónica, Inter-American Development Bank (IDB) та Development Bank of Latin America (CAF). Головною метою проекту є розширення покриття Інтернету у важкодоступних регіонах, особливо в сільських районах Перу, Колумбії, Аргентини та інших країн Латинської Америки.

Проект орієнтований на співпрацю з місцевими телекомунікаційними компаніями та урядами, щоб створити стійкі та економічно ефективні моделі розгортання Інтернет-інфраструктури. У межах програми використовуються новітні технології, включаючи відкриті радіомережі (OpenRAN) та енергоефективні мобільні станції, що дозволяє забезпечити доступ до 4G-зв’язку там, де традиційні методи побудови мереж були економічно невигідними. Завдяки цій ініціативі понад 6 мільйонів людей у

Перу вже отримали доступ до швидкісного Інтернету, а подібні проекти планується розширити на інші країни регіону [236].

Ще однією масштабною ініціативою є "Digital India", започаткована урядом Індії у 2015 році для розширення цифрового доступу по всій країні. Програма передбачає розвиток широкосмугового Інтернету у сільській місцевості, створення цифрових публічних інфраструктур та покращення рівня цифрової грамотності серед населення. У межах ініціативи уряд співпрацює з приватним сектором, залучаючи інвестиції в розширення телекомунікаційних мереж, установку Wi-Fi-зон у державних установах, лікарнях та освітніх закладах [203].

Одним із ключових напрямків програми є проект BharatNet, спрямований на підключення понад 250 тисяч сільських районів до оптоволоконних мереж. Крім того, програма підтримує ініціативи з розвитку цифрових навичок, що дозволяють мільйонам громадян

користуватися онлайн-послугами, здійснювати електронні платежі та отримувати доступ до урядових сервісів в Інтернеті. На сьогодні в межах Digital India понад 500 мільйонів громадян отримали доступ до Інтернету, що значно сприяло економічному розвитку країни [203].

Ще одним значущим глобальним проектом є ініціатива Starlink від компанії SpaceX, яка передбачає розгортання супутникового Інтернету для країн та регіонів із слабко розвиненою інфраструктурою. Starlink – це мережа низькоорбітальних супутників, які забезпечують високошвидкісний Інтернет навіть у найвіддаленіших куточках світу, де традиційні оптоволоконні мережі або мобільний зв’язок недоступні.

Проект було запущено у 2019 році, і на сьогодні Starlink надає покриття у понад 60 країнах, зокрема у США, Канаді, Великій Британії, Австралії, Бразилії, Україні та інших. Особливо значущу роль ця ініціатива відіграла в Україні після повномасштабного вторгнення Росії, коли традиційна телекомунікаційна інфраструктура зазнала значних руйнувань.

Уряд України отримав десятки тисяч терміналів Starlink, що дозволило підтримувати зв’язок у критичних зонах, забезпечувати роботу лікарень, військових підрозділів та гуманітарних організацій. Окрім цього, Starlink має важливе значення для розвитку цифрової інфраструктури в Африці та Південній Америці, де традиційні методи побудови Інтернет-мереж є дорогими та малоефективними. Згідно з оцінками компанії SpaceX, у найближчі роки мережа Starlink охопить понад 10 мільйонів користувачів по всьому світу [265].

Отже, глобальні ініціативи, спрямовані на розширення доступу до Інтернету, є важливим кроком у забезпеченні цифрової рівності. Реалізація таких проектів, як Internet para Todos у Латинській Америці, Digital India та Starlink від SpaceX, дозволяє усунути цифровий розрив, забезпечити рівні можливості для всіх громадян незалежно від їхнього місця проживання та сприяти соціально-економічному розвитку країн. У майбутньому такі

ініціативи мають стати пріоритетним напрямом міжнародного співробітництва, що дозволить зробити Інтернет доступним для кожного.

Серед пріоритетних завдань, які стоять перед державними інституціями України в межах забезпечення інформаційного та цифрового суверенітету, є впровадження комплексних заходів, що відповідають світовим практикам у сфері регулювання Інтернет-простору, забезпечення безпеки цифрової інфраструктури та захисту національних інтересів. Україна, враховуючи міжнародний досвід, зокрема ініціативи Digital India, Internet para Todos та законодавчі напрацювання таких країн, як Фінляндія, Франція та Індія, має розвивати власні стандарти цифрової політики та інформаційного захисту.

Одним із ключових напрямків є здійснення автоматичного моніторингу інформаційного простору країни для виявлення загроз, дезінформації та пропагандистських впливів. Такий підхід реалізований у багатьох державах, зокрема в Європейському Союзі в рамках Законодавства про цифрові послуги [206], яке передбачає відповідальність платформ за боротьбу з дезінформацією та шкідливим контентом. Україна також має інтегрувати сучасні методи аналізу великих даних та автоматизованого моніторингу медіапростору для своєчасного реагування на інформаційні загрози.

Наступним важливим кроком є впровадження законодавства про відповідальність за контент, що регулює поширення небезпечної інформації, зокрема мови ворожнечі, екстремістських матеріалів та маніпулятивних наративів.

Франція, наприклад, ще у 2009 році визнала право на Інтернет складовою свободи слова, що водночас передбачає відповідальність за незаконний контент. Аналогічно, Україна повинна ухвалити законодавчі акти, які встановлять чіткі механізми відповідальності за розповсюдження шкідливого контенту, водночас не порушуючи основних принципів свободи вираження поглядів.

Важливим аспектом цифрового суверенітету є розробка та впровадження законодавства, що регулює фільтрацію інтернет-контенту. Досвід Фінляндії, яка у 2010 році закріпила право на доступ до Інтернету, показує, що ефективне регулювання можливе без порушення прав громадян. Україна може використовувати цей підхід для формування механізмів контролю над інформаційними потоками, включаючи блокування ворожих пропагандистських ресурсів, які загрожують державній безпеці.

Окремої уваги потребує захист національної культури та мови від інформаційного впливу домінуючих глобальних гравців. Важливим прикладом є ініціатива Digital India, яка стимулює розвиток цифрового контенту національними мовами, забезпечуючи культурну автономію країни. Україна може застосувати подібні підходи, сприяючи поширенню україномовного цифрового контенту, створенню національних інформаційних платформ та підтримці незалежних медіа.

Не менш важливим завданням є знаходження соціально прийнятного балансу між свободою слова та необхідністю інформаційного захисту держави. Приклад Європейського Союзу показує, що в умовах зростаючих загроз дезінформації та пропаганди необхідно впроваджувати регуляторні механізми, які дозволяють мінімізувати негативні впливи, не порушуючи демократичних принципів. У цьому контексті Україна може розглянути розробку відповідного законодавства, що ґрунтується на європейських практиках захисту цифрових прав.

Крім того, одним із головних викликів є захист інформаційного простору від культурної експансії зарубіжних інтернет-ресурсів. Впровадження державної політики підтримки локального цифрового контенту та інвестування у створення українських альтернатив глобальним сервісам є важливим кроком на шляху до цифрового суверенітету.

Останнім, але не менш значущим аспектом є перехід державних установ на використання програмного та технічного забезпечення власної

розробки і виробництва. Такий підхід уже реалізований у багатьох країнах, що прагнуть цифрової незалежності. Наприклад, Індія активно розвиває власні технологічні платформи в межах Digital India. В Україні подібна політика має передбачати підтримку вітчизняних ІТ-компаній, розробку національних операційних систем та перехід на використання вітчизняного програмного забезпечення у державному секторі.

Таким чином, забезпечення цифрового та інформаційного суверенітету України потребує комплексного підходу, що включає правове регулювання інформаційного простору, підтримку національного контенту, боротьбу з інформаційними загрозами та розвиток власних цифрових технологій. Враховуючи міжнародний досвід, Україна має можливість вибудувати ефективну систему захисту цифрових прав та інформаційної безпеки, що відповідатиме сучасним викликам та міжнародним стандартам.

Україна має продовжувати впровадження європейських та міжнародних стандартів у сфері кібербезпеки, що є ключовим елементом забезпечення цифрового суверенітету та інформаційної безпеки держави. У сучасних умовах кіберзагрози набувають транснаціонального характеру, що робить міжнародну співпрацю у цій сфері необхідною. Враховуючи досвід Європейського Союзу та НАТО у боротьбі з кіберзагрозами, Україна повинна не лише інтегрувати найкращі практики, а й активно співпрацювати з міжнародними партнерами, зокрема в рамках Європейської кібербезпекової стратегії (EU Cybersecurity Strategy) та НАТОвської Програми посилення кіберзахисту (Cyber Defence Pledge).

Розвиток кіберзахисту потребує ефективної роботи відповідних державних органів, здатних не лише реагувати на кіберінциденти, але й активно взаємодіяти з кіберпідрозділами ЄС та НАТО.

Зокрема, успішним прикладом міжнародного співробітництва є участь України у проєктах Європейської агенції з кібербезпеки (ENISA), яка надає експертну підтримку у сфері захисту критично важливої інфраструктури та боротьби з кібератаками. Також слід відзначити, що

Кооперативний центр кібероборони НАТО (CCDCOE) надає Україні можливість обміну досвідом та спільних навчань з кіберзахисту, що підсилює безпековий потенціал держави у сфері цифрової безпеки.

Разом з тим, досвід України у протидії сучасним кіберзагрозам дозволяє їй бути не лише реципієнтом міжнародної допомоги, але й активним учасником глобальної системи кіберзахисту. Враховуючи безпрецедентну кількість кібератак на державні установи, об'єкти критичної інфраструктури та приватний сектор, Україна накопичила унікальні знання та практичний досвід, які можуть бути корисними для країн ЄС і НАТО у формуванні ефективних механізмів протидії кіберагресії.

Сучасні кіберзагрози підкреслюють нагальну потребу у міжнародній співпраці, спрямованій на попередження атак, забезпечення ефективного розслідування, виявлення зловмисників та їхнє притягнення до відповідальності. Оскільки цифрові технології створюють глобально взаємопов'язане середовище, кібератаки можуть мати серйозні економічні, політичні та соціальні наслідки. Наприклад, кібератака на українську енергетичну систему у 2015 році, відома як BlackEnergy, продемонструвала, що подібні акти можуть мати руйнівний ефект не лише для окремих країн, а й для міжнародної спільноти загалом.

Тому критично важливою є узгоджена міжнародна політика у сфері кібербезпеки, що базується на міжнародних правових механізмах, таких як Будапештська конвенція про кіберзлочинність, яка визначає стандарти боротьби з кіберзлочинами та встановлює механізми міжнародної співпраці.

Україна має активно сприяти формуванню єдиної глобальної стратегії кібербезпеки, яка включатиме як технічні, так і нормативно-правові заходи. Важливим кроком у цьому напрямку є створення системи стратегічного кіберзахисту, що охоплює розбудову національної інфраструктури кіберзахисту, залучення до міжнародних ініціатив та впровадження стандартів безпеки для державного та приватного сектору.

Протидія цифровому тоталітаризму вимагає комплексного підходу, що поєднує захист цифрових прав громадян, розбудову незалежної цифрової інфраструктури, інтеграцію у міжнародні ініціативи з кібербезпеки та боротьбу з інформаційною експансією.

Україна, застосовуючи досвід європейських держав та ініціатив, таких як Digital India, Internet para Todos, Starlink, GDPR та Будапештська конвенція про кіберзлочинність, може побудувати ефективну систему захисту від цифрового тоталітаризму. Це дозволить не лише забезпечити цифрову безпеку держави, а й гарантувати громадянам доступ до правдивої інформації, вільний Інтернет та захист від незаконного стеження та маніпуляцій.

Таким чином, міжнародна інтеграція, зміцнення національних цифрових технологій та впровадження прозорої політики у сфері кібербезпеки дозволять Україні стати лідером у боротьбі з цифровим тоталітаризмом у регіоні та прикладом для інших держав, що прагнуть цифрової демократії та незалежності.

Висновки до третього розділу. Отже, проблема ефективного забезпечення захисту прав в умовах цифрового тоталітаризму потребує комплексного вирішення і вимагає скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади, приватного сектора і громадянського суспільства.

З огляду на сучасні суспільно-політичні та інформаційні виклики визначення політичних, науково-технічних, організаційних та просвітницьких напрямів конструювання ефективної системи кіберзахисту у рамках комплексної протидії внутрішнім та зовнішнім загрозам сприятиме формуванню ефективного механізму протидії порушенню прав у кібернетичній сфері, випереджальному реагуванні на динамічні зміни, що відбуваються на теренах інтернет-мережі, розробленню та впровадження ефективних засобів та інструментів можливої відповіді на агресію у

кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі.

Захист особистих даних є важливою задачею в цифровому суспільстві. Найпоширенішими способами, які можна використовувати для захисту особистих даних є наступні:

- використання унікальних та складних паролей для кожного облікового запису;

- увімкнення двоетапної аутентифікації;

- оновлення програмного забезпечення;

- використання шифрування для зберігання чутливих даних, таких як файли на комп'ютері чи смартфоні;

- підключення до непідтверджених відкритих мереж Wi-Fi – зокрема, віртуальних приватних мереж (VPN);

- обізнаність користувачів у шахрайських атаках, фішингу та соціально-інженерних методах.

Захист особистих даних – це постійний процес, і важливо слідкувати за новими загрозами та приймати необхідні заходи для їх запобігання.

ВИСНОВКИ

У сучасному глобалізованому світі стрімкий розвиток цифрових технологій радикально трансформував не лише соціально-економічне життя, але й механізми політичного впливу, захисту прав і свобод людини. Цифрова епоха принесла як нові можливості, так і безпрецедентні загрози. Однією з найсерйозніших серед них є поява та поширення феномену цифрового тоталітаризму, що виявляється у масовому стеженні, обмеженні свободи слова, маніпуляції інформацією та використанні технологій для контролю над громадянами.

У дисертаційній роботі представлено теоретико-методологічне розв'язання та нові шляхи вирішення наукової проблематики, які є логічним продовдженням існуючих та створення принципово нових підходів в процесі дослідження феномену цифрового тоталітаризму та загроз демократії в інформаційному суспільстві. В результаті проведених досліджень, дисертантом зроблено наступні висновки:

1. Аналіз еволюцію концепції тоталітаризму та її трансформацію в контексті цифрового розвитку засвідчує її здатність адаптуватися до нових історичних та технологічних умов. Класичні форми, які базувалися на централізованій владі, масовій пропаганді та фізичному примусі з плином часу поступово еволюціонували у гібридні моделі, які використовують цифрові інструменти як механізм контролю. Цифрові технології дозволяють не лише розширити масштаб і точність нагляду, але й здійснювати ненасильницьке, алгоритмічно кероване управління поведінкою громадян.

У цифровому вимірі тоталітаризм втрачає потребу в демонстративному насильстві, натомість набуваючи вигляду «м’якого» або прихованого примусу, де контроль здійснюється через дані, поведінкову аналітику, інформаційні потоки та автоматизоване регулювання, що доводить загрозу демократії та інформаційним суспільствам.

2. Охарактеризовано ключові ознаки інформаційного суспільства як передумови формування нових форм політичного контролю. Інформаційне суспільство характеризується зростанням ролі знань, інформації та цифрових технологій, як ключових ресурсів соціального впливу й організації влади. Домінування інформаційно-комунікаційних потоків та алгоритмічної логіки змінює традиційні уявлення про простір, час, працю й ідентичність.

У таких умовах нові форми політичного контролю не потребують прямого втручання у фізичний простір – контроль здійснюється через архітектуру інформаційного середовища, моделювання цифрових поведінкових шаблонів, соціальні рейтинги та емоційно-когнітивні інтервенції. Саме в цьому контексті інформаційне суспільство формує сприятливе підґрунтя для виникнення феномену цифрового тоталітаризму, як технологізованої практики впливу на громадянську свідомість та її дії.

3. Розглянуто методологічні підходи до вивчення цифровізації влади, контролю та управління. Дослідження цифровізації влади потребує використання міждисциплінарного арсеналу методологій, що охоплюють політичну науку, критичну теорію, соціологічні знання, кібернетичні дослідження та аналіз даних. До основних підходів належать: системний, що розглядає владу як складну мережеву структуру цифрових взаємодій; конструктивістський — який аналізує, як цифрові технології формують політичні смисли та ідентичності; та критичний – спрямований на викриття нових форм домінування, що маскуються під технологічний прогрес.

Також важливими є кіберпаноптичні та постфукоянівські концепції, які дозволяють осмислити алгоритмічне управління як форму мікровлади, що діє через тілесність, увагу, звички та цифровий слід користувача.

4. Виявлено основні технологічні інструменти, що використовуються для цифрового моніторингу, цензури та інформаційного впливу. До ключових інструментів цифрового контролю належать системи масового відеоспостереження (зокрема з розпізнаванням облич), системи соціального

рейтингу та кредитування, алгоритмічні стрічки новин, автоматизовані системи цензури контенту, трекінг мобільних пристроїв, а також програми, що збирають біометричні та поведінкові дані.

Ці інструменти використовуються як державними органами, так і технологічними корпораціями, які часто, без належного нормативного регулювання, застовують їх у власних процесах обробки даних. Особливу загрозу становить їх здатність до «невидимого управління» — коли громадяни не усвідомлюють, що їхня поведінка формується та моделюється алгоритмічними сценаріями на основі попередніх дій, вподобань та передбачуваних рішень, що є доказом процесів втручання в приватне життя представників інформаційного суспільства.

5. Аналіз процесів алгоритмічного цензурування, маніпуляцій інформацією та контроль політичного дискурсу стали одним із найнебезпечніших викликів свободі слова у цифрову епоху. На відміну від традиційних форм цензури, алгоритмічні механізми є майже невидимими для пересічного користувача, однак вони мають глибокий вплив на формування громадської думки, політичної поведінки та доступ до альтернативних точок зору.

Досвід таких країн, як Угорщина, Російська Федерація, Польща, США, КНР та інших, демонструє, що алгоритмічні інструменти, зокрема персоналізація стрічок новин, «інформаційні бульбашки», shadow banning, використання бот-мереж і таргетованої реклами, активно використовуються владою або наближеними до неї структурами для поширення пропаганди, маргіналізації опозиційних голосів та створення ілюзії суспільного консенсусу. Це супроводжується практиками адміністративного, правового чи навіть технічного тиску на незалежні ЗМІ, журналістів і цифрові платформи.

Водночас існуючи приклади свідчять, що навіть у державах із заявленим демократичним курсом існує ризик зловживання інструментами цифрового контролю під приводом захисту національної безпеки. Це

проявляється у надмірних обмеженнях доступу до інформаційних ресурсів, відсутності прозорих процедур блокування контенту та неузгодженості між національним законодавством і міжнародними стандартами у сфері прав людини.

6. Визначено роль технологічних корпорацій як суб'єктів політичного впливу, досліджено їхній вплив на трансформацію режимів інформаційного управління. Сучасні технологічні гіганти (Big Tech) – такі як Google, Meta, Amazon,Youtube, X, Alibaba чи ByteDance – дедалі частіше виступають не лише економічними агентами, а й активними учасниками політичного процесу. Вони володіють унікальними інфраструктурами для збору та аналізу даних, здатні впливати на інформаційний порядок денний, моделювати громадську думку та навіть впливати на результати виборів. Їхня діяльність призводить до ерозії традиційних інститутів політичної відповідальності, адже ці структури, формально не будучи державними, виконують функції подібні до функцій регуляторів, судових інстанцій або медіацензорів. Така приватизація управління інформацією є однією з найнебезпечніших форм феномену цифрового тоталітаризму.

7. Досліджено механізми захисту прав людини в умовах цифрових трансформацій та порівняно ефективність регуляторних практик у демократичних і авторитарних державах. Захист прав людини в цифрову епоху вимагає не лише оновлення нормативно-правових актів, а й переосмислення самих підходів до розуміння прав у контексті інформаційної взаємодії.

Демократичні держави намагаються розробляти механізми цифрової етики, впроваджувати GDPR-подібні регулювання, створювати інституції цифрового захисту громадян. Водночас, авторитарні режими використовують ті самі технології для зміцнення контролю, обмеження доступу до інформації та політичних репресій. Порівняльний аналіз свідчить, що ефективність регуляторних практик значною мірою залежить від рівня прозорості, громадянської участі, незалежності судових органів, а

також ступеню втручання державних та недержавних технологічних корпорацій у порядок денний функціонування інформаційних суспільств та демократії.

8. Оцінено використання цифрових технологій у політичних практиках, спрямованих на протидію тенденціям цифрового тоталітаризму. Цифрові технології, попри їхнє активне використання з боку авторитарних режимів для посилення контролю, водночас відкривають нові можливості для демократичного опору, мобілізації громадян та захисту прав і свобод. Одним із ключових напрямів протидії є розвиток децентралізованих технологій, зокрема блокчейн-платформ, які дозволяють зберігати дані в незмінній формі без централізованого контролю. Наприклад, платформи типу IPFS (InterPlanetary File System) забезпечують довготривале збереження інформації, що унеможливлює її цензурування.

У сфері комунікацій важливе місце посідають системи шифрування месенджерів, які гарантують конфіденційність спілкування і захист від втручання з боку держав або корпорацій. Значну роль у цифровому спротиві відіграє цифровий активізм, зокрема використання онлайн-петицій. Такі ініціативи протистоять маніпуляціям офіційних наративів та сприяють підзвітності влади. Особливе значення має розвиток цифрової освіти та медіаграмотності, як інструментів формування критичного мислення й опору дезінформації. У цьому контексті варто згадати про програми StopFake, VoxChecka, які спрямовані на боротьбу з інформаційними маніпуляціями. Водночас, незалежна журналістика дедалі частіше поєднує аналітику великих даних та цифрові інструменти розслідувань.

Формування цифрової культури опору передбачає не лише технічну обізнаність, а й розвиток етичних стандартів, цифрового громадянства та активної участі в побудові альтернативних цифрових просторів, вільних від домінування корпорацій і державного контролю. Така культура є ключовою передумовою для забезпечення демократичної стійкості та запобігання

впровадженню цифрового тоталітаризму під виглядом «ефективного управління».

9. З’ясовано політико-правову базу захисту прав людини в умовах цифрових трансформацій та виявлено перспективи їх удосконалення. Інституційна спроможність національних і міжнародних систем захисту прав людини виявляється дедалі більш уразливою перед викликами цифрової доби. Більшість правових механізмів, створених у XX столітті, не відповідають сучасним реаліям, пов’язаним з алгоритмічним управлінням, масовим збиранням даних, впливом штучного інтелекту та домінуванням приватних технологічних корпорацій над інформаційною інфраструктурою. Наприклад, такі гіганти як Meta, Google, Amazon, ByteDance фактично формують інформаційні середовища та встановлюють свої «правила гри», які нерідко суперечать конституційним гарантіям свободи слова, права на приватність або захист персональних даних. На міжнародному рівні вже вживаються кроки щодо оновлення правозахисної парадигми:

Європейський Союз ухвалив Акт про цифрові послуги (DSA) та Акт про цифрові ринки (DMA), що спрямовані на обмеження впливу цифрових монополістів, забезпечення прозорості алгоритмів та захист прав користувачів. Крім того, ухвалений і GDPR, який встановлює вимоги до компаній на рахунок збору та обробки даних, а також повідомлення користувачів про ці процеси. Окремі ініціативи також пропонуються на регіональних та національних рівнях.

Водночас у національних юрисдикціях ситуація є неоднорідною. Демократичні країни, як-от Німеччина, Швейцарія або Канада, впроваджують моделі цифрового регулювання, що поєднують захист прав людини з інноваційним розвитком. Наприклад, Німеччина ухвалила Network Enforcement Act (NetzDG) – закон, який вимагає від соцмереж швидко видаляти контент, що порушує права громадян, зберігаючи при цьому процесуальні гарантії. У той же час авторитарні режими — Китай, Іран, Росія – використовують цифровізацію для побудови систем цифрового

нагляду (наприклад, «Система соціального рейтингу» в Китаї) та легалізованої цензури, що викликає серйозні занепокоєння правозахисників.

Потреба в оновленні міжнародного правового порядку є нагальною. Серед пріоритетів – розробка глобальної Декларації цифрових прав, яка закріпила б фундаментальні свободи людини в умовах цифрового середовища (аналогічно до Загальної декларації прав людини 1948 року). Також важливим кроком має стати зобов'язання держав та корпорацій до прозорості алгоритмів і прийняття етичних стандартів розробки ШІ, як це вже частково передбачено у рекомендаціях ЮНЕСКО з етики штучного інтелекту.

Удосконалення правозахисних механізмів має передбачати не лише нові формальні регулювання, але й створення ефективних механізмів імплементації, незалежного нагляду, громадянського моніторингу та цифрової інклюзії. До прикладу, Reporters without borders (EFF), Freedom House, World Competitivness Center та інші громадянські організації відіграють все більшу роль у захисті цифрових прав, пропонуючи юридичну підтримку, технічні рішення (наприклад, шифрування, VPN, антистеження) та політичний тиск на корпорації й уряди, а також розвиток громадянських інфраструктур цифрової демократії

Таким чином, протидія феномену цифровому тоталітаризму вимагає не лише політичної волі та технологічних рішень, а й глибокої правової трансформації, нової культури цифрової відповідальності, зміцнення міжнародної співпраці, і найголовніше – інформаційно підготовленого, критично мислячого громадянського суспільства, яке здатне захищати свої права у новому інформаційному світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Арендт Х. Джерела тоталітаризма. – 2-е видання. / Пер. з англ. – К.: Дух і література, 2005. 584 с. URL: https://chtyvo.org.ua/authors/Arendt_Hanna/Dzherela_totalitaryzmu/ (дата звернення 10.09.2024)

2. Балан С. Інформаційне суспільство як основа концепції інформаційної держави. *Вісник Львівського університету. Серія філос.-політолог. студії*. 2024. Вип. 54. С. 154–161. URL: https://doi.org/10.30970/PPS.2024.54.18

3. Балаховська Ю. Діджиталізація професійної підготовки майбутніх вчителів-філологів в умовах дистанційного навчання, *Актуальні питання гуманітарних наук*. Вип. 68, том 1. 2023, С. 189-194. URL: https://www.aphn-journal.in.ua/archive/68_2023/part_1/29.pdf (дата звернення 11.12.2024)

4. Бебик В.М. Базові засади політології: історія, теорія, методологія, практика. К.: МАУП, 2010. 384 с

5. Безугла К. О. Сучасний стан сектору інформаційних технологій в Україні. *Економіко-математичне моделювання систем*: зб. наукових праць, 2018. С. 50-70. URL: http://nbuv.gov.ua/UJRN/emmses_2014_19_5 (дата звернення 15.08.2024)

6. Безуглий Д. Інформаційна безпека України: огляд останніх тенденцій, *Фізико-математична освіта*. 2018. Вип. 2(16), С. 13–17, URL: http://nbuv.gov.ua/UJRN/fmo_2018_2_4 (дата звернення 20.10.2024)

7. Белл Д. Інформація і телекомунікації в постіндустріальному суспільстві. URL: https://lib.chmnu.edu.ua/pdf/posibnuku/307/32.pdf (дата звернення 21.09.2024)

8. Бібік Н. М. Компетенції. *Енциклопедія освіти* [Акад. пед. наук України; гол. ред. В. Г. Кремень]. К. : Юрінком Інтер, 2008. С. 409–410.

9. Біленчук П. Д. Кібербезпека і засоби запобігання та протидії кіберзлочинності й кібертероризму. *Часопис Київського університету права*. 2018. № 3. С. 235-239. URL: http://nbuv.gov.ua/UJRN/Chkup_2018_3_54 (дата звернення 03.09.2024)

10. Білоус О. В. Цифрова компетентність як ключова компетентність для навчання впродовж життя. К.: НАПН. 64 с.

11. Бойко В. Кібербезпека в ЄС та країнах-членах: генезис та проблеми її підвищення URL: http://academy.ssu.gov.ua/ua/page/page_1581426437.htm

12. Брижко В.М., Пилипчук В.Г. Приватність, конфіденційність та безпека персональних даних. *Інформація і право*. 2020. № 1. С. 33-46. URL: http://nbuv.gov.ua/UJRN/Infpr_2020_1_5 (дата звернення 20.10.2024)

13. В Туркменістані користувачів інтернету змушують клястись на Корані, що вони не використовуватимуть VPN URL: https://ms.detector.media/internet/post/27966/2021-08-10-v-turkmenistani-korystuvachiv-internetu-zmushuyut-klyastys-na-korani-shcho-vony-ne-vykorystovuvatymut-vpn-zmi/ (дата звернення 21.10.2024)

14. Вдовиченко Ю. В. Цифрові технології як основа та рушійна сила розвитку сучасної глобальної економіки. *Журнал «Економіка та держава»*, 2018. №1. С. 79-82. URL: http://nbuv.gov.ua/UJRN/ecde_2018_1_17 (дата звернення 17.01.2025)

15. Великанова М.М. Ризики в цивільному праві *: монографія.* К.: *Алерка,* 2019. 378 с.

16. Вінник О.М. Правове забезпечення цифрової економіки та електронного бізнесу : *монографія.* К.*:* НДІ приватного права і підприємництва ім. акад. Ф. Г. Бурчака. 2018. 224 с. https://doi.org/10.24195/2414-9616.2022-1.21 (дата звернення 19.10.2024)

17. Вінникова Н.А. Цифрові технології у боротьбі за глобальною корупцією. *Вісник Харківського національного університету Імені*

В. Н. Каразіна, серія «Питання політології». 2022. Вип. 41. С. 30-39. URL: https://doi.org/10.26565/2220-8089-2022-41-04 (дата звернення 15.11.2024)

18. Вінникова Н.А. Штучний інтелект як чинник геополітичного впливу. *Вісник Харківського національного університету імені В.Н. Каразіна*, серія «Питання політології». 2021. Вип. 40. С. 21-28. URL: https://doi.org/10.26565/2220-8089-2021-40-03 (дата звернення 15.11.2024)

19. Войтович Р. В. Вплив глобалізації на систему державного управління (*теоретико-методологічний аналіз*): Київ, 2017. 680 с.

20. Володовська В., Дворовий М. Права людини онлайн: Порядок денний для України. URL:https://dslua.org/wp-content/uploads/2019/12/DRA_FINAL_UKR.pdf. (дата звернення 26.10.2024)

21. Впровадження європейської кібербезпеки: загальний огляд. ISACA. URL: https://www.isaca.org/Knowledge-enter/Research/Documents/European-CybersecurityImplementation-Overview_res_Ukr_1215.pdf (дата звернення 23.10.2024)

22. Габер Є. Міжнародні відносини в епоху штучного інтелекту: чи мають майбутнє дипломатичні перекладачі? *Дзеркало тижня: інформаційно-аналітичний тижневик*. Київ,2019. 12-18 жовтня (№ 38), 4

23. Головко О.М. Цифрова культура та інформаційна культура: права людини в епоху цифрових трансформацій. Інформація і право. 2019. № 4 (31). С. 37-44.

24. Горбатенко В.П. Диктатура НАН України, НТШ. Київ: Інститут енциклопедичних досліджень НАН України, 2007 URL: https://esu.com.ua/article-24278 (дата звернення 22.11.2024)

25. Гудзь О.Є. Цифрова економіка: зміна цінностей та орієнтирів управління підприємствами. *Економіка. Менеджмент. Бізнес.* № 2 (24), 2018. URL: http://www.dut.edu.ua/uploads/p_1010_10116202.pdf

26. Гуренко А. В., Гашутіна О. Е. Напрями розвитку систем управління в умовах діджиталізації бізнесу в Україні. *Розвиток продуктивних сил і регіональна економіка*. 2018. № 19. С. 739–745.

27. Данилко І., Деркач О. Особливості правового регулювання кібербезпеки в умовах цифровізації суспільства URL:https://reposit.nupp.edu.ua/bitstream/PoltNTU/12161/1/75%20%D1%82%D0%BE%D0%BC%201%20%D0%94%D0%B0%D0%BD%D0%B8%D0%BB%D0%BA%D0%BE_%D0%94%D0%B5%D1%80%D0%BA%D0%B0%D1%87.pdf (дата звернення 22.10.2024)

28. Державний стандарт України. Захист інформації. URL: https://tzi.com.ua/478.html (дата звернення 22.10.2024)

29. Добродум О. Дискурс цифрового тоталітаризму як можливого тренду дигіталізації суспільства. *Людинознавчі студії: збірник наукових праць Дрогобицького державного педагогічного університету імені Івана Франка. Серія «Філософія»*, (47), 44–56. URL: https://doi.org/10.24919/2522-4700.47.3

30. Довбуш В.І., Домашенко Д.Р Диджиталізація – важливий, необхідний та трудомісткий крок у антикризовому розвитку бізнесу в сучасних складних умовах пандемії COVID-19. 2024. С. 96-100 URL:https://er.knutd.edu.ua/bitstream/123456789/19584/1/Innovatyka2021_V2_P096-100.pdf (дата звернення 22.11.2024)

31. Доктрина інформаційної безпеки України, затверджена указом Президента України від 25.02.2017 р. №47/2017 URL: https://zakon.rada.gov.ua/laws/show/47/2017 (дата звернення 22.11.2024)

32. Доній Н. Є. Принципи конституційного дизайну в ситуації трансформації демократії. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали*

Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальноюредакцією С. В. Ківалова. – Одеса : Видавничий дім «Гельветика», 2022. – Т. 1. – С. 13-16. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/70ed48f0-6950-4e26-a72d-4f7b2030461e/content.

33. Дульська І. В. Цифрові технології як каталізатор економічного зростання. Економіка і прогнозування. 2015. № 2. С. 119–133.

34. Дунаєва Л. М. Дезінформаційні виклики під час російсько-української війни: політологічний аналіз. *Політикус : наук. журнал*. 2022. № 5. С. 73–78. URL: https://doi.org/10.24195/2414-9616.2022-5.11 (дата звернення 19.11.2024)

35. Завгородня Ю. В. Кіберконфлікти як сучасна загроза цифровізації суспільства: політичний аспект. *Актуальні проблеми філософії та соціології*. 2022. № 35. С. 88-92. URL: https://doi.org/10.32837/apfs.v0i35.1100 (дата звернення 21.11.2024)

36. Завгородня Ю. В. Кіберконфлікти, як елемент політичних технологій в інформаційному просторі. *Актуальні проблеми філософії та соціології*. 2021. Вип. 32. С. 144-148. URL:http://nbuv.gov.ua/UJRN/aprfc_2021_32_28 (дата звернення 21.11.2024)

37. Завгородня Ю.В. Специфіка розвитку політичного протиборства в кібернетичній сфері ISSN 2353-8406 *Knowledge, Education, Law, Management* 2022 № 7 (51) URL: https://kelmczasopisma.com/ua/viewpdf/9613 (дата звернення 21.11.2024)

38. Загальна Декларація прав людини URL: https://bkbnau.com/zagalna-deklaratsiya-prav-lyudyny/ (дата звернення 02.11.2024)

39. Загальна декларація прав людини від 10 грудня 1948 року. Офіційний сайт Спілки адвокатів України. URL: https://lawyersunion.org.ua/wp-content/uploads/2021/02/Deklaratsiya-prav-lyudyny.pdf (дата звернення 02.11.2024)

40. Загальний регламент про захист даних (GDPR) URL: https://gdpr-text.com/uk/read/article-1/ (дата звернення 06.11.2024)

41. Заславська О. Органи державної влади України як відкрита інформаційна система. *Науковий вісник Ужгородського університету. Серія: Політологія, Соціологія, Філософія,* 2009. С.190-194.

42. Захист систем електронних комунікацій: навч. посіб. / В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. Київ: Київ. нац. торг.-екон. ун-т, 2019. 164 с.

43. Іванов В., Мелещенко О. Комп'ютерні технології в засобах масової комунікації: сучасне та майбутнє. Київ: РВУ, 1999. 173 с.

44. Інформаційна безпека в умовах цифровізації: актуальні проблеми правового регулювання. URL: https://ippi.org.ua/sites/default/files/2023-5.pdf (дата звернення 11.11.2024)

45. Карачка А. Ф. Технології захисту інофрмації: конспект лекцій. *Тернопіль, ТНЕУ*, 2017. 86 с. URL: http://dspace.wunu.edu.ua/bitstream/316497/26564/1/lekzii.pdf (дата звернення 11.11.2024)

46. Карпенко О. В., Куйбіда В. С. Інформаційно-комунікативна діяльність органів публічної влади: монографія. Київ, 2019. 358 с.

47. Кириченко В.В. Інформаційне суспільство: еволюція явища та глобалізаційна трансформація суспільного світосприйняття. *Теорія і практика сучасної психології*. №2. 2018. С.22-26.

48. Кібербезпека в Україні: проблеми та перспективи розвитку URL:https://ippi.org.ua/sites/default/files/6_13.pdf (дата звернення 06.12.2024)

49. Кібербезпека в Україні: шляхи розвитку та можливості URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html (дата звернення 06.12.2024).

50. Кібербезпека у 2025 році: нові виклики та тренди URL: https://softline.company/ua/news/kiberbezpeka-u-2025-rotsi-novi-vyklyky-ta-trendy.html (дата звернення 01.03.2025).

51. Коляденко С. В. Цифрова економіка: передумови та етапи становлення в Україні та світі. *Економіка. Фінанси. Менеджмент: актуальні питання науки і практики*. 2016. № 6. С. 105-112. URL: http://nbuv.gov.ua/UJRN/efmapnp_2016_6_11 (дата звернення 06.12.2024)

52. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини) URL: https://zakon.rada.gov.ua/laws/main/995_004#Text (дата звернення 15.10.2024)

53. Комарова Т. Тоталітаризм як соціокультурний феномен в інформаційну епоху. *European political and law discourse.* 2020. Vol. 2. No 7. P. 107-112.

54. Конституція України: від 28.06.1996 р. URL: https://constitution.in.ua/ (дата звернення 15.10.2024)

55. Концепція розвитку цифрової економіки та суспільства України на 2018- 2020 роки : розпорядження Кабінету міністрів України від 17 січня 2018 року URL: http://zakon.rada.gov.ua/laws/show/67-2018-%D1%80 (дата звернення 15.10.2024)

56. Коренівська В. О. Цифровий банкінг: ризики фінансової дигіталізації. *Проблеми економіки*. 2017. № 3. С. 254-261.

57. Костишин Н. С. Бухгалтерський облік 2030Е – цифровий облік розвиненої країни. *Матеріали VI Міжнар. наук.-практ. конф. Тернопіль: ТНЕУ*, 2020. С. 133-134. URL: http://dspace.wunu.edu.ua/bitstream/316497/42391/1/%D0%9A%D0%BE%D1%81%D1%82%D0%B8%D1%88%D0%B8%D0%BD.pdf (дата звернення 20.10.2024)

58. Криворучко О. С., Краус Н. М. Імперативи формування та домінанти розвитку цифрової економіки у сучасному парадигмальному контексті. *Парадигмальні зрушення в економічній теорії XIX ст.: III Міжнародна науково-практична конференція,* 2–3 листопада 2017 р.: тези доповідей. Київ: КНУ ім. Т. Шевченка, 2017. С. 681–685.

59. Кримінальний кодекс України. URL: https://kodeksy.com.ua/kriminal_nij_kodeks_ukraini/statja-182.htm (дата звернення 15.10.2024)

60. Криниця С. О. державна політика цифровізації економіки України. *Фінансовий простір*. 2018. № 3 (31). С. 50-57 URL: http://nbuv.gov.ua/UJRN/Fin_pr_2018_3_8 (дата звернення 28.10.2024)

61. Кубів С. Цифрова економіка. Про нові можливості для України. URL: https://nv.ua/ukr/opinion (дата звернення 18.10.2024)

62. Кудлай В. Інформаційне суспільство: сучасні тенденції та особливості розвитку. *Галицький економічний вісник*. 2024. Том 90. № 5. С. 37-44. URL: https://doi.org/10.33108/galicianvisnyk_tntu2024.05.037 (дата зверення 21.09.2024)

63. Кушнеров О. Ю. Правові аспекти забезпечення кібербезпеки в Україні. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/85989/3/Kushnerov.pdf (дата звернення 18.10.2024)

64. Лашкіна М. Г. Нові підходи до комунікації в публічному просторі державного управління. *Публічне управління*. 2017. №1. С. 10-18. URL: http://nbuv.gov.ua/UJRN/Pubupr_2013_1_4 (дата звернення 18.10.2024)

65. Лозовицький О. Інформаційне суспільство як основа розвитку національних ціннісних орієнтацій зовнішньої політики держави в умовах сучасної доби глобалізації. URL: https://ipiend.gov.ua/wp-content/uploads/2018/07/lozovytskyi_informatsiine.pdf (дата зверення 22.10.2024)

66. Лях В.В. Свобода самореалізації у контексті інформаційно-комунікативних процесів *Мультиверсум. Філософський альманах*: Зб. наук. пр. К., 2008. Вип. 73. С. 3-27.

67. Ляшенко В. І., Вишневський О. С. Цифрова модернізація економіки України як можливість проривного розвитку: монографія. Київ, 2018. 252 с.

68. Мамонтова Е. Публічна політика URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/bc9fd726-d16b-4790-bcaf-914d53e73f33/content (дата звернення 18.12.2024)

69. Маркузе Г. Одновимірна людина. Дослідження ідеології розвинутого індустріального суспільства URL: https://shron1.chtyvo.org.ua/Marcuse_Herbert/Odnovymirna_liudyna.pdf (дата звернення 03.11.2024)

70. Масуда Й. Комп'ютопія. *Філософська і соціологічна думка*.1993. № 6. С.35-50.

71. Матвійчук О. В., Мина Ж. К., Яновська А. Розвиток електронної дипломатії в Україні: прерогативи та недоліки. *Інформація, комунікація, суспільство* 2017: *матеріали 4-ої Міжнародної наукової конференції ІКС*-2017, 20-23 травня 2017 року, Україна, Львів, Славське / Національний університет «Львівська політехніка», Кафедра соціальних комунікацій та інформаційної діяльності. Львів: Видавництво Львівської політехніки, 2017. С. 142-143. URL: https://www.researchgate.net/profile/Solomia_Fedushko/publication/331276371_Proceedings_of_the_International_Academic_Conference_ICS-2016/links/5c6fc2d5a6fdcc471591b3b5/Proceedings-of-the-International-Academic-Conference-ICS-2016.pdf (дата звернення 06.112.2024)

72. Мешко Н. П., Сазонець О. М., Джусов О. А. та ін. Стратегії високотехнологічного розвитку в умовах глобалізації: національний та корпоративний аспекти: монографія. Донецьк: Юго-Восток, 2012. 470 с.

73. Милосердна І. М. Цифровий суверенітет держави: наукова риторика та реальні зміни *Politicus*. 2024. Вип.6 С. 154-160 URL : http://politicus.od.ua/6_2024/25.pdf (дата звернення 19.12.2024)

74. Милосердна І. М., Краснопольська Т. М. Процес цифровізації в політиці: межі пізнання та особливості трансформації. *Актуальні проблеми політики*. 2022. Вип. 70. С. 106–113.

URL: http://app.nuoua.od.ua/archive/70_2022/17.pdf (дата звернення 19.12.2024)

75. Міжнародний пакт про громадянські та політичні права від 16 грудня 1966 року URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення 15.10.2024)

76. Мілова М. Тоталітарні режими: ідеологічне обґрунтування цілей, форм і методів володарюванняУкр. нац. ідея: реалії та перспективи розв. 2012. Вип. 24. С. 51-55. URL: https://onu.edu.ua/pub/bank/userfiles/files/science/totalitarizm/doslid/milova-total-rezim.pdf (дата звернення 22.02.2025)

77. Мусієнко О. 10 трендів стратегічних технологій 2023 від Gartner. URL: imena.ua/blog/10-strategic-technology-trends-2023-from-gartner/ (дата звернення 15.10.2024)

78. Наумкіна С. М. Ризики формування нових форм тиску як прояви цифрового тоталітаризму *Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів матеріали VII Всеукраїнської науково-практичної конференції* (м. Одеса, 30 квітня 2024 р.). Одеса: ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», Центр соціально-політичних досліджень «Politicus», 2024. С.150-153. URL: http://dspace.pdpu.edu.ua/bitstream/123456789/19664/1/Naumkyna.pdf (дата звернення 22.02.2025)

79. Нестеренко В. В. Тоталітаризм в інформаційному середовищі. *Радіоелектроніка та молодь у XXI столітті: матеріали 25-го Міжнар. молодіжн. форуму, м. Харків*. 20-22 квітня 2021 р. Харків, 2021. С. 84–85. URL: https://openarchive.nure.ua/server/api/core/bitstreams/3130c51f-6341-4c4e-aa11-f6b7e712b634/content (дата зверення 22.02.2025)

80. Нікітін Ю.О., Кульчицький О.І. Цифрова парадигма як основа визначень: цифровий бізнес, цифрове підприємство, цифрова

трансформація. *Маркетинг і цифрові технології*. 2019. Т. 3, № 4. С. 77-. URL : http://nbuv.gov.ua/UJRN/mardigt_2019_3_4_10 (дата звернення 03.12.2024)

81. Об'єдков О.І. Феномен цифрового тоталітаризму. Шлях від класичної концепції до сьогодення URL: https://doi.org/10.32782/apfs.v040.2023.12 (дата звернення 22.02.2025)

82. Овчарук О. В. Європейська стратегія визначення рівня компетентності у галузі цифрових технологій: рамка цифрової компетентності для громадян. *Освітній вимір*, №55(3), С. 25-36

83. Орвелл Дж. 1984. URL: https://reading.in.ua/1984-dzhordzh-orvell/ (дата звернення 11.08.2024)

84. Основи інформаційної та кібербезпеки: навчальний посібник URL: http://dspace.wunu.edu.ua/bitstream/316497/26564/1/lekzii.pdf (дата звернення 23.11.2024)

85. Податковий Кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2755-17#Text (дата звернення 15.10.2024)

86. Політанський В.С. Інформаційне суспільство в україні: від зародження до сьогодення. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/33280/1/%D0%86%D0%9D%D0%A4%D0%9E%D0%A0%D0%9C%D0%90%D0%A6%D0%86%D0%99%D0%9D%D0%95%20%D0%A1%D0%A3%D0%A1%D0%9F%D0%86%D0%9B%D0%AC%D0%A1%D0%A2%D0%92%D0%9E%20%D0%92%20%D0%A3%D0%9A%D0%A0%D0%90%D0%87%D0%9D%D0%86.pdf (дата зверення 20.02.2025).

87. Політологія: Навчальний посібник / Штанько В.І., Чорна Н.В., Авксентьєва Т.Г., Тіхонова Л.А. Видання 2е, перероблене та доповнене. – К.: Видавництво «Фірма «ІНКОС», Центр учбової літератури, 2007. 288 с.

88. Політологія: навчально-методичний комплекс / за ред. М.Ф. Юрій. К.: Дакор. 2016.

89. Правдюк А.Л. Конституціоналізація цифрових прав людини. *Наука і техніка сьогодні.* № 9. 2023, С. 44 – 54. URL: DOI: https://doi.org/10.52058/2786-6025-2023-9(23)-44-54 (дата звернення 12.11.2024)

90. Правові аспекти кібербезпеки в Україні: сучасний стан та перспективи URL: http://il.ippi.org.ua/article/view/238349 (дата звернення 10.11.2024)

91. Про біженців та осіб, які потребують додаткового або тимчасового захисту : Закон України від 08.07.2011 р. № 3671-VI (чинний) станом на 4 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/3671-17#Text (дата звернення 04.06.2025)

92. Про Всеукраїнський перепис населення : Закон України від 19.10.2000 р. № 2058-III (чинний): станом на 04. червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2058-14 (дата звернення 10.12.2024)

93. Про державний захист працівників суду і правоохоронних органів: Закон України від. 23.12.1993р. № 3781-XII (чинний) : станом на 04 чер. 2025р. URL: https://zakon.rada.gov.ua/laws/show/3781-12 (дата звернення 10.12.2024)

94. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI (чинний) : станом на 4 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення 10.12.2024)

95. Про доступ до судових рішень : Закон України від 22.12.2005 №3263-IV (чинний): станом на 4 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/3262-15 (дата звернення 10.12.2024)

96. Про друковані засоби масової інформації (пресу) в Україні : Закон України від 16.11.1992 №2782-XII (втратив чинність) : станом 31.03.2023 р. URL: https://zakon.rada.gov.ua/laws/show/2782-12#Text (дата звернення 09.12.2024)

97. Про електронні довірчі послуги : Закон України від 05.10.2017 №2155-VIII (чинний) станом на 4 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2155-19 (дата звернення 09.12.2024)

98. Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві : Закон України від 23.12.1993 №3782-XII (чинний) : станом на 4 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/3782-12 (дата звернення 09.12.2024)

99. Про загальнообов'язкове державне пенсійне страхування : Закон України від 09.07.2003 №1058-IV (чинний) : станом на 4 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/1058-15#Text (дата звернення 09.12.2024)

100. Про загальнообов'язкове державне соціальне страхування Закон України : від 23.09.1999 №1105-XIV (чинний) : станом на 4 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/1105-14#Text (дата звернення 10.12.2024)

101. Про захист інформації в інформаційно-телекомунікаційних системах : Закон Україн від 05.07.1994 №80/94-ВР станом на 04. чер. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення 10.12.2024)

102. Про захист персональних даних : Закон України від 01.06.2010 №2297-VI (чинний): станом на 4 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення 10.12.2024)

103. Про звернення громадян: Закон України від 02.10.1996 №393/96-ВР (чинний) станом: на 04 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80 (дата звернення:10.12.2024).

104. Про інформацію : Закон України від 02.10.1992 №2657-XII (чинний) станом на 4 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 09.12.2024).

105. Про інформацію Закон України №2657-XII (редакція від 01.01.2017 р.) URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення 09.12.2024)

106. Про Концепцію розвитку сектора безпеки і оборони України : Указ Президента України від 14.03.2016 р. №92/2016. URL: https://zakon.rada.gov.ua/laws/show/92/2016 (дата звернення 10.12.2024)

107. Про лікарські засоби : Закон України від 4.04.1996 №123/96-ВР станом на 04 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/123/96-%D0%B2%D1%80 (дата звернення: 09.12.2024)

108. Про медіа : Закон України від 13.12.2022 № 2849-IX (чинний) станом на 4 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення: 10.12.2024).

109. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 р. № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016 (дата звернення: 10.12.2024).

110. Про національну безпеку України : Закон України від 21.06.2018 №2469-VIII станом на 4 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 10.12.2024)

111. Про недержавне пенсійне забезпечення : Закон України від 09.07.2003 №1057-IV станом на 4 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/1057-15 (дата звернення: 10.12.2024)

112. Про оплату праці : Закон України від 24.03.1995 №108/95-ВР станом на 04 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/108/95-%D0%B2%D1%80 (дата звернення: 10.12.2024)

113. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 №2163-VIII станом на 4 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 10.12.2024)

114. Про поховання та похоронну справу : Закон України від 10.07.2003 №1102-IV станом на 4 червня 2025 р.

URL: https://zakon.rada.gov.ua/laws/show/1102-15 (дата звернення: 09.12.2024)

115. Про свободу пересування та вільний вибір місця проживання в Україні : Закон України від 11.12.2003 №1382-IV станом на 04 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/1382-15 (дата звернення: 09.12.2024)

116. Про стратегічний оборонний бюлетень України : Указ Президента України від 06.06.2016 р. № 240/2016. URL: https://zakon.rada.gov.ua/laws/show/240/2016 (дата звернення: 09.12.2024)

117. Про Стратегію інформаційної безпеки : Указ Президента України від 15.10.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 09.12.2024)

118. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Закон України від 15.05.2013 №386-VII станом на 4 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80 (дата звернення: 10.12.2024)

119. Про телебачення і радіомовлення : Закон України від 21.12.1993 №3759-XII станом на 4 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/3759-12 (дата звернення: 09.12.2024)

120. Про телекомунікації : Закон України від 18.11.2003 №1280-IV станом на 04 червня 2025 р. URL: https://zakon.rada.gov.ua/laws/show/1280-15 (дата звернення: 09.12.2024).

121. Проект Закону про електронні комунікації. URL : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68059 (дата звернення 09.12.2024)

122. Проект Закону про розвиток цифрової економіки. URL : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=63316 (дата звернення 09.12.2024)

123. Проект Закону України «Про цифровий Порядок денний України». URL : https:// www.rada.gov.ua/uploads/documents/40009.pdf (дата звернення 09.12.2024)

124. Професійна рамка цифрового навчання (Digital Teaching Professional Framework) URL: https://www.etfoundation.co.uk/supporting/supportpractitioners/edtech-support/digital skills-competency-framework (дата звернення 23.11.2024)

125. Пустоваров А. І. Механізм цифрової трансформації управління розвитком національної економіки : дис. … канд.економ.наук.07.05.2021/ Пустоваров Анатолій Іванович. Запоріжжя, 2021. 214 с. URL : http://virtuni.education.zp.ua/info_cpu/sites/default/files/Dis_Pustovarov.pdf (дата звернення 11.09.2024)

126. Ракіпов В.Р. Об'єктивні передумови розвитку цифровізації в Україні. International scientific conference Economy and Society: *The Formation of a Modern Competitiveenvironment: Integration And Globalization.* (Greenwich, May 25th, 2018). Greenwich, UK: Baltija Publishing, 2018. Part I. С. 95-98.

127. Рекомендація № CM/Rec (2014) 6 Комітету міністрів Ради Європи «Про Керівництво з прав людини для користувачів Інтернету» URL: https://search.coe.int/cm#{%22CoEIdentifier%22:[%2209000016805c6f3d%22],%22sort%22:[%22CoEValidationDate%20Descending%22]} (дата звернення 27.10.2024)

128. Рекомендація № CM/Rec (2015) 6 Комітету міністрів Ради Європи «Про вільний транскордонний рух інформації в Інтернеті» URL: https://search.coe.int/cm#{%22CoEIdentifier%22:[%2209000016805c3f20%22],%22sort%22:[%22CoEValidationDate%20Descending%22]} (дата звернення 27.10.2024)

129. Русул О. В. Свобода самореалізації в умовах інформаційного суспільства. *Вісник Дніпропетровського університету. Філософія і політологія в контексті культури*. Науковий журнал. 2014. Випуск 7.

С. 155-160. URL: https://fip.dp.ua/index.php/FIP/article/view/334/332 (дата звернення 19.11.2024)

130. Самойленко А. Особливості цифровізації країн Європейського Союзу в умовах глобалізації. *Вісник економіки.* 2021. Вип. 1. С. 46–54. DOI: https://doi.org/10.35774/visnyk2021.01.046 URL:https://visnykj.wunu.edu.ua/index.php/visnykj/article/view/1214 (дата звернення 24.10.2024)

131. Система соціального рейтингу в Китаї набула грандіозного масштабу URL: https://ivasi.news/trash/sistema-soczialnogo-rejtingu-v-kita%D1%97-nabula-nebachenogo-masshtabu/#google_vignette (дата звернення 13.12.2024)

132. Соколова Г. Б. Деякі аспекти розвитку цифрової економіки в Україні. *Економічний вісник Донбасу*. 2018. № 1 (51). С. 92–96. URL: http://nbuv.gov.ua/UJRN/ecvd_2018_1_17 (дата звернення 20.10.2024)

133. Сокоринський В. О «Сучасні інструменти захисту прав, свободи та безпеки особистості в епоху "Цифрового тоталітаризму"» с.35-39 URL: http://www.regionalstudies.uzhnu.uz.ua/archive/28/6.pdf (дата звернення 21.09.2024)

134. Сокоринський В. О. «Цифровий Паноптикум» як метод розповсюдження цифрового тоталітаризму та загроза сучасним міжнародним відносинам С. 118-122. URL: http://politicus.od.ua/2_2024/2_2024.pdf (дата звернення 21.09.2024)

135. Сокоринський В. О. Сучасні системи захисту прав людини в КНР в контексті загрози «цифрового тоталітаризму» С. 39-44 URL: http://regionalstudies.uzhnu.uz.ua/archive/33/7.pdf (дата звернення 21.09.2024)

136. Сокоринський, В. О. Цифровий тоталітаризм та системи захисту національної безпеки : дипломна робота магістра. Одеса, 2020. 125 с.

137. Сопілко І.М. Особливості протидії кіберзагрозам правовими методами та засобами URL: https://er.nau.edu.ua/server/api/core/bitstreams/7fc000b7-9e94-49e7-81cd-89537ae14cb2/content (дата звернення 20.10.2024)

138. Спенсер Г. Основи Соціології. URL: https://archive.org/details/in.ernet.dli.2015.22432/page/n7/mode/2up (дата звернення 19.08.2024)

139. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері. Київ, 2019. 28 с. URL: https:// geostrategy.org.ua/ua/analitika/item/1565-cooperation-ukraine-nato. (дата звернення 09.12.2024)

140. Стайнер К. Тотальна автоматизація. Як комп'ютерні алгоритми змінюють життя / пер. з англ. Олександр Лотоцький. Київ : *Наш формат*, 2018. 280 с.

141. Стратегічна концепція НАТО. 2022 URL:https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept-ukr.pdf (дата звернення 09.12.2024)

142. Стратегічна політика кібербезпеки України: аналіз стану та напрями вдосконалення URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/3acf4b52-6858-4bda-973c-35535be8fcfe/content (дата звернення 11.12.2024)

143. Сучасні виклики кібербезпеці в умовах цифровізації державного управління
URL: https://csecurity.kubg.edu.ua/index.php/journal/article/download/72/85/309 (дата звернення 13.12.2024)

144. Сучасні виклики та загрози кібербезпеці в Україні URL: https://archive.logos-science.com/index.php/conference-proceedings/article/download/943/966/967 (дата звернення 09.12.2024)

145. Сучасні механізми захисту прав людини: колективна монографія / С . С. Кельман, А. С. Токарська, Л. В. Ярмол, С. Б. Цебенко, А. О. Дутко. Львів : *Галицька видавнича спілка*, 2020. 220 с. URL: https://lpnu.ua/sites/default/files/2023/6/19/paragraphs/50930/monografiyakelmantokarskayarmolcebenko.pdf (дата звернення 05.12.2024)

146. Сучасні тенденції правового регулювання кібербезпеки та інтелектуальна власність URL: https://coordynata.com.ua/sucasni-tendencii-pravovogo-reguluvanna-kiberbezpeki-ta-intelektualna-vlasnist (дата звернення 11.12.2024)

147. Тероризм. Заходи спостереження URL: https://ks.echr.coe.int/documents/d/echr-ks/surveillance-measures-ukr (дата звернення 17.09.2024)

148. Ткачук Г. О. «Цифрові» трансформації: взаємозв'язок із системою економічної безпеки підприємства. *Економіка харчової промисловості*. 2019. Т. 11, Вип. 4. С. 42-50. URL: http://nbuv.gov.ua/UJRN/echp_2019_11_4_7 (дата звернення 12.11.2024)

149. Толстов І., Даніл'ян В. Інформаційне суспільство та нова глобальна етика. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Філософія. Філософські перипетії»*. 68 (Чер 2023), 39-44. URL:https://doi.org/10.26565/2226-0994-2023-68-4. (дата зверення 20.02.2025)

150. Трофименко О. «Моніторинг стану кібербезпеки в Україні», *Правове життя сучасної* України: матер. міжнар. наук.-практ. конф., 17 травня 2019 р., Т. 1, Одеса: *Видавничий дім «Гельветика»*, с. 642–646, 2019. URL: https://hdl.handle.net/11300/21309 (дата звернення 09.12.2024)

151. Трофименко О.Г. Законодавча база забезпечення кібербезпеки держави. *Кібербезпека в Україні: правові та організаційні питання*: матер. II всеукр. наук.-практ. конф., 17 листопада 2017 р., Одеса: ОДУВС, С. 55–56. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/e4395e1a-d8c8-45b6-9178-92defd98ecba/content (дата звернення 09.12.2024)

152. Ухвалення «Стратегічного компасу» Європейського союзу URL: https://niss.gov.ua/sites/default/files/2022-04/evropeyskiy_kompas.pdf (дата звернення 09.12.2024)

153. Федосенко Н.А. Використання цифрових технологій у цивільних правовідносинах. *Часопис цивілістики*. 2022. Вип. 45. С. 69-74.

154. Хартія Європейського Союзу про основоположні права URL: https://ccl.org.ua/posts/2021/11/hartiya-osnovnyh-prav-yevropejskogo-soyuzu/ (дата звернення 09.12.2024)

155. Хома Н., & Ніколаєва М. (2022). Цифровий авторитаризм: поняття, особливості, загрози. *Історико-політичні проблеми сучасного світу*, (46), 159–166. URL: https://doi.org/10.31861/mhpi2022.46.159-166 https://doi.org/10.31861/mhpi2022.46.159-166 (дата звернення 20.10.2024)

156. Хто сильний, той і правий: як Китай намагається «перевиховати» уйгурів. *Хвиля*. URL: https://hvylya.net/uk/analytics/224147-hto-silniy-toy-i-praviy-yak-kitay-namagayetsya-perevihovati-uyguriv (дата звернення 13.12.2024)

157. Цензура в Китаї та п'яти інших країнах завдає шкоди бізнесу США: звіт USITC URL: https://www.epochtimes.com.ua/novyny-svitu/cenzura-v-kytayi-ta-pyaty-inshyh-krayinah-zavdaye-shkody-biznesu-ssha-zvit-usitc-141478 (дата звернення 13.12.2024)

158. Цехановська О. У чому небезпека «інформаційної бульбашки» та як комфортно із неї вийти? URL: https://hromadske.radio/podcasts/myslennia-bazova-funktsiia/1065085 (дата звернення 20.10.2024)

159. Цивільний кодекс України. URL: https://i.factor.ua/ukr/law-54/section-300/article-6120/ (дата звернення 20.10.2024)

160. Цифрова стратегія ЄС. URL: https://eufordigital.eu/uk/discover-eu/eu-digital-strategy/ (дата звернення: 13.02.2025)

161. Чабанна М. Авторитаризм і тоталітаризм. Уявна подібність і сутнісна різниця. *Політичний менеджмент*. 2003. № 2. С. 83-92. URL : https://ipiend.gov.ua/wp-content/uploads/2018/07/chabanna_avtorytaryzm.pdf (дата звернення 03.08.2024)

162. Четверта поправка та винесення вироку в Сполучених Штатах. Юридичний факультет ЧНУ ім. Ю. Федьковича.

URL: https://law.chnu.edu.ua/chetverta-popravka-ta-vynesennia-vyroku-v-spoluchenykh-shtatah/ (дата звернення 17.12.2024)

163. Чому Київ відмовився підтримати уйгурів: ціна питання для України. URL:https://nv.ua/ukr/opinion/kitay-ukrajina-chomu-kijiv-vidmovivsya-pidtrimati-uyguriv-novini-ukrajini-50175355.html (дата звернення 13.12.2024)

164. Шемчук В. Національна стратегія кібербезпеки США: досвід для України. *Науковий вісник Національної академії внутрішніх справ*. 2020. № 4. С. 119-124.

165. Шилюк А. Правове регулювання свободи слова в мережі Інтернет в контексті глобалізаційних процесів. *Конституційно-правові академічні студії*. 2020. №1. С. 47–58. URL: https://www.constjournal.com/wp-content/uploads/issues/2020-1/pdfs/5-anna-shyliuk-pravove-rehuliuvannia-svobody-slova-merezhi-internet-kontekksti-hlobalizatsiinykh.pdf (дата звернення 20.10.2024)

166. Штанько В.І., Бордюгова Т.Г. Інформаційне суспільство: соціально-філософські проблеми становлення: Навчальний посібник. Харків: ХНУРЕ, 2012. 172 с. URL: https://openarchive.nure.ua/server/api/core/bitstreams/dccb4459-8e93-4161-9f4d-cce7eee74a13/content (дата звернення 11.08.2024)

167. Щербатенко О. Перспективи та перешкоди цифрової економіки в Україні / *Na chasi*.29.01.2018. URL: https:// nachasi.com/2018/01/29/what-makes-ukraine-digital (дата звернення 20.10.2024)

168. Що Вам потрібно знати про GDPR. URL:https://ybcase.com/ua/company-services/legal-services/cto-vam-stoit-znat-o-gdpr (дата звернення 18.11.2024)

169. A VPN connection protects your privacy https://www.dna.fi/liittymat-ja-palvelut/turvapalvelut/digiturva/vpn (дата звернення 13.12.2024)

170. A VPN connection protects your privacy online https://elisa.fi/tietoturva/vpn/ (дата звернення 13.12.2024)

171. Amnesty International: Iran authorities shut down Internet URL: https://www.amnesty.org/en/latest/news/2019/11/iran-authorities-shut-down-internet (дата звернення 18.12.2024)

172. BBC News: Starlink's global internet coverage URL: https://www.bbc.com/news/science-environment-65066669 (дата звернення 18.12.2024)

173. Bell D. The Coming of Post-Industrial Society URL : https://bgsp.edu/app/uploads/2014/12/Bell-Coming-of-Post-Industrial-Society.pdf (дата звернення 17.08.2024)

174. Break Their Lineage, Break Their Roots. China's Crimes against Humanity Targeting Uyghurs and Other Turkic Muslims.. Human Rights Watch. URL: https://www.hrw.org/report/2021/04/19/break-their-lineage-break-their-roots/chinas-crimes-against-humanity-targeting (дата звернення 13.12.2024)

175. Brennen S., Kreiss D. Digitalization, The International Encyclopedia of Communication Theory and Philosophy, John Wiley & Sons. 2016. P. 1-11. URL: https://onlinelibrary.wiley.com/doi/10.1002/9781118766804.wbiect111 (дата зверення 12.10.2024)

176. Case of Amann v. Switzerland URL: https://hudoc.echr.coe.int/fre#{%22fulltext%22:[%22Amann%20v.%20Switzerland%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58497%22]} (дата звернення 17.09.2024)

177. Case of b. V. France URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57770%22]} (дата звернення 17.09.2024)

178. Case of Copland v. the United Kingdom URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-79996%22]} (дата звернення 17.09.2024)

179. Case of Dudgeon v. the United Kingdom URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57473%22]} (дата звернення 17.09.2024)

180. Case of Gaskin v. the United Kingdom URL: https://hudoc.echr.coe.int/tur#{%22itemid%22:[%22001-57491%22]} (дата звернення 17.09.2024)

181. Case of Jankovic v. Croatia. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-5496%22]} (дата звернення 17.09.2024)

182. Case of Laskey, Jaggard and Brown v. the United Kingdom URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58021%22]} (дата звернення 17.09.2024)

183. Case of López ostra v. Spain URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57905%22]} (дата звернення 17.09.2024)

184. Case of Odièvre v. France URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-60935%22]} (дата звернення 17.09.2024)

185. Case of Rotaru v. Romania. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58586%22]} (дата звернення 17.09.2024)

186. Case of Glass v. The United Kingdom. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-61663%22]} (дата звернення 17.09.2024)

187. Case of Mikulic v. Croatia URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-60035%22]} (дата звернення 17.09.2024)

188. Case of Niemietz v. Germany. URL:https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57887%22]} (дата звернення 17.09.2024)

189. Case of Yocheva and Ganeva v. Bulgaria URL: https://hudoc.echr.coe.int/ukr#{%22itemid%22:[%22001-209866%22]} (дата звернення 17.09.2024)

190. Case *von Hannover v. Germany* URL:https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-139253%22]} (дата звернення 17.09.2024)

191. Castells M. The Information Age. URL: https://deterritorialinvestigations.wordpress.com/wp-content/uploads/2015/03/manuel_castells_the_rise_of_the_network_societybook fi-org.pdf (дата звернення 08.08.2024)

192. China’s Cybersecurity Law: An Introduction for Foreign Businesspeople URL: https://www.china-briefing.com/news/chinas-cybersecurity-law-an-introduction-for-foreign-businesspeople/ (дата звернення 13.12.2024)

193. China's 2021 Data Security Law: Grand Data Strategy with Looming Implementation Challenges URL:https://www.prcleader.org/post/china-s-2021-data-security-law-grand-data-strategy-with-looming-implementation-challenges (дата звернення 13.12.2024)

194. Cloud Act. URL: https://www.govinfo.gov/co (дата звернення 20.10.2024)ntent/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm (дата звернення 17.12.2024)

195. Comte Auguste Cours de philosophie positive URL: https://libarch.nmu.org.ua/bitstream/handle/GenofondUA/18943/e31f0c4d003196c56f1fbc14f7b8d292.pdf?sequence=1 (дата звернення 12.08.2024)

196. Conseil Constitutionnel France, Decision №2009-580 DC. URL: https://www.conseil-constitutionnel.fr/en/decision/2009/2009-580DC.htm (дата звернення 08.11.2024)

197. Convention 108: Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

URL: https://www.coe.int/en/web/data-protection/convention108 (дата звернення 19.09.2024)

198. Cybersecurity of Ukraine: Analysis of the Current Situation. URL: https://www.researchgate.net/publication/337114481_Cybersecurity_of_Ukraine_analysis_of_the_current_situation (дата звернення 17.09.2024)

199. De Clerck J.-P. Digitization, digitalization and digital transformation: the differences. Retrieved from. URL: https://www.i-scoop.eu/digitization-digitalization-digi-taltransformation-disruption/. (дата звернення 217.08.2024)

200. Debord G. The Society of the Spectacle. URL: http://library.nothingness.org/articles/SI/en/pub_contents/4 (дата звернення 16.08.2024)

201. Deleuze G. Postscript on the Societies of Control. URL: https://libcom.org/library/postscript-on-the-societies-of-control-gilles-deleuze (дата звернення 21.08.2024)

202. Digital Economy Act 2017. URL : https:// www.legislation.gov.uk/ukpga/2017/30/contents/enacted (дата звернення 25.10.2024)

203. Digital India – Official Government Initiative. URL: https://digitalindia.gov.in (дата звернення 10.02.2025)

204. Durkheim E. De la division du travail social. URL: https://monoskop.org/images/9/97/Durkheim_%C3%89mile_De_la_division_du_travail_social_1991.pdf (дата звернення 26.08.2024)

205. E-Democracy: Conceptual Foundations and Recent Trend URL: https://link.springer.com/chapter/10.1007/978-3-030-27184-8_2#Abs1 (дата звернення 12.08.2024)

206. EU Digital Services Act – Official Information Resource. URL: https://www.eu-digital-services-act.com/ (дата звернення 25.10.2024)

207. EU names 19 large tech platforms that must follow Europe's new Internet rules. URL: https://arstechnica.com/tech-policy/2023/04/google-runs-5-

of-the-19-platforms-that-must-follow-eus-new-internet-rules/ (дата звернення 25.10.2024)

208. European Convention on Human Rights URL: https://www.echr.coe.int/documents/convention_eng.pdf (дата звернення 07.11.2024)

209. Europe's DMA Goes Global. URL: https://cepa.org/article/europes-dma-goes-global/ (дата звернення 25.10.2024)

210. Federal Acton Data Protection URL: https://www.fedlex.admin.ch/eli/cc/2022/491/en (дата зверення 25.10.2024)

211. Finance Committee Leaders Wyden and Crapo: Biden Administration Must Fight Back Against Discriminatory Digital Trade Policies URL:https://www.finance.senate.gov/chairmans-news/finance-committee-leaders-wyden-and-crapo-biden-administration-must-fight-back-against-discriminatory-digital-trade-policies (дата звернення 20.10.2024)

212. Finland makes broadband a legal right. URL: https://www.bbc.com/news/10461048 (дата звернення 21.11.2024)

213. FISA and the USA PATRIOT Act: Reforms and Legal Implications. *Princeton Legal Journal.* URL: https://legaljournal.princeton.edu/fisa-and-the-usa-patriot-act-reforms-and-legal-implications/ (дата звернення 15.12.2024)

214. Foucault – Discipline and Punish URL: https://www.ethanhein.com/wp/2016/foucault-discipline-and-punish/ (дата звернення 21.08.2024)

215. Freedom House. Poland 2022. URL: https://freedomhouse.org/country/poland/nations-transit/2022 (дата звернення 15.12.2024)

216. Freedom House. Russia 2024. URL: https://freedomhouse.org/country/russia/freedom-net/2024 (дата звернення 15.12.2024)

217. Freedom on the Net 2024.Ukraine URL:https://freedomhouse.org/country/ukraine/freedom-net/2024 (дата звернення 15.12.2024)

218. Freedom on the Net 2024: United States. *Freedom House*. URL: https://freedomhouse.org/country/united-states/freedom-net/2024 (дата звернення 15.12.2024)

219. Friedrich Carl J. Totalitarian dictatorship and autocracy URL: https://archive.org/details/totalitariandict0000frie_p1x0/page/n9/mode/2up1 (дата звернення 28.98.2024)

220. Fromm Erich. The Sane Society. URL: https://historicalunderbelly.wordpress.com/wp-content/uploads/2012/12/erich-fromm-the-sane-society.pdf (дата звернення 25.08.2024)

221. Fromm Erich. Escape from freedom. URL : http://www.edarcipelago.com/classici/erichfromm/escape%20from%20freedom%20-%20erich%20fromm.pdf (дата звернення 25.08.2024)

222. General Data Protection Regulation (GDPR): URL: https://gdpr-info.eu/ (дата звернення 22.09.2024)

223. Germany: Flawed Social Media Law URL: https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law (дата звернення 23.11.2024)

224. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken. URL: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html (дата звернення 23.11.2024)

225. Global Drive to Control Big Tech. Freedom House Report. 2022. URL: https://freedomhouse.org/report/freedom-net/2022/global-drive-control-big-tech (дата звернення 22.10.2024)

226. Google takes legal action over Germany's expanded hate-speech law URL: https://www.reuters.com/technology/google-takes-legal-action-over-germanys-expanded-hate-speech-law-2021-07-27/ (дата звернення 10.10.2024)

227. Helbing D. Digital fascism rising? URL: https://www.theglobalist.com/fascism-big-data-artificial-intelligencesurveillance-democracy/ (дата звернення 20.08.2024)

228. Helsen G. Absolutism and Relativism in Philosophy and Politics American Political Science Review , Volume 42 , Issue 5 , October 1948 , pp. 906 – 914 URL: https://doi.org/10.2307/1950135 (дата звернення 23.11.2024)

229. Hendricks, V.F., Vestergaard, M. Epilogue: Digital Roads to Totalitarianism. In: Reality Lost. Springer, Cham. https://doi.org/10.1007/978-3-030-00813-0_7 (дата звернення 22.02.2025)

230. Henri Saint Simon. Selected writings on science, industry and social organisation. URL : https://api.pageplace.de/preview/DT0400.9781000112788_A40133126/preview-9781000112788_A40133126.pdf (дата звернення 07.08.2024)

231. Hikvision: не лише камери, але й зброя URL: https://drukarnia.com.ua/articles/hikvision-ne-lishe-kameri-ale-i-zbroya-nyuIi (дата звернення 13.12.2024)

232. How Web3 technology can help people in Iran during a period of internet blackout – with Matt Wisniewski. URL: https://fintech.tv/how-web3-technology-can-help-people-in-iran-during-a-period-of-internet-blackout-with-matt-wisniewski/ (дата звернення 26.10.2024)

233. Human Rights Watch – Myanmar URL: https://www.hrw.org/myanmar (дата звернення 23.11.2024)

234. International Covenant on Civil and Political Rights URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (дата звернення 21.09.2024)

235. Internet Censorship in Iran URL: https://www.article19.org/resources/iran-internet-censorship-report/ (дата звернення 21.09.2024)

236. Internet Para Todos (Internet for Everyone initiative) URL: https://www.internetparatodos.org (дата звернення 17.02.2025)

237. Jan A.G.M. van Dijk. The Network Society URL: https://forschungsnetzwerk.ams.at/dam/jcr%3A8a671e75-c945-4784-a438-15a889cf24da/The_Network_Society-Jan_van_Dijk.pdf (дата звернення 18.10.2024)

238. Klass and Others v. Germany URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]} (дата звернення 23.10.2024)

239. Landscape. Journal of Studies in Language, Culture, and Society (JSLCS)7(2), pp-pp. 182-199.

240. LiveLaw: Right to Internet Access is a Fundamental Right, Indian Supreme Court. URL: https://www.livelaw.in/top-stories/right-to-internet-access-fundamental-right-151984 (дата звернення 16.11.2024)

241. Lutkevich B. TikTok bans explained: Everything you need to know URL: https://www.techtarget.com/whatis/feature/TikTok-bans-explained-Everything-you-need-to-know(дата звернення 19.10.2024)

242. Lyon D. Surveillance. URL: https://policyreview.info/concepts/surveillance(дата звернення 28.10.2024)

243. Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. URL: https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf (дата звернення 17.11.2024)

244. Mandl C. Bridgewater sees short-term correction for tech stocks but bullish on DeepSeek impact URL: https://www.reuters.com/technology/bridgewater-sees-short-term-correction-tech-stocks-bullish-deepseek-impact-2025-01-28/ (дата звернення 22.10.2024)

245. Meta Transparency Center Reports URL: https://transparency.meta.com/reports/content-restrictions/ (дата звернення 07.11.2024)

246. Moody R. Which countries have the worst (and best) cybersecurity? URL: https://www.comparitech.com/blog/vpnprivacy/cybersecurity-by-country/ (дата звернення 16.11.2024)

247. National Cyber Strategy of the United States of America. (2018). (n.d.)URL: https://www.whitehouse.gov/wp- content/uploads/2018/09/National-Cyber-Strategy.pdf (дата звернення 16.11.2024)

248. Network Propaganda Manipulation, Disinformation, and Radicalization in American Politics. URL: https://global.oup.com/academic/product/network-propaganda-9780190923624?cc=ua&lang=en& (дата звернення 16.11.2024)

249. Ochs T., Riemann U. A. IT Strategy Follows Digitalization. Encyclopedia of Information Science and Technology 2018. Fourth Edition. Hershey, PA: IGI Global. DOI: 10.4018/978-1-5225-2255-3.ch075 (дата зверення 10.11.2024)

250. Press Information Bureau of India (2023): Digital infrastructure report. URL: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2086701 (дата звернення 17.02.2025)

251. Read Yuval Harari's blistering warning to Davos in full URL: https://www.weforum.org/stories/2020/01/yuval-hararis-warning-davos-speech-future-predications/ (дата звернення 04.09.2024)

252. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) URL: https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng (дата звернення 27.12.2024)

253. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng (дата звернення 27.12.2024)

254. Report on the State of the Digital Decade 2023 – European Commission URL: https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade (дата звернення 22.11.2024)

255. Report without borders. Hungary URL: https://rsf.org/en/country/hungary (дата звернення 22.11.2024)

256. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach URL: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (дата звернення 13.11.2024)

257. Rozumyuk, V. The Totalitarian Legacy of the Post-Soviet Countries: Theoretical Reflection of the Problems of Totalitarism", *Problems of World History*, (20), pp. 7–26. doi: 10.46869/2707-6776-2022-20-1. URL: https://journal.ivinas.gov.ua/pwh/article/view/238 (дата звернення 11.12.2024)

258. Russia to Install 'Orwell' Facial Recognition Tech in Every School. URL: https://www.themoscowtimes.com/2020/06/16/russia-to-install-orwell-facial-recognition-tech-in-every-school-vedomosti-a70585 (дата звернення 18.10.2024)

259. Russia VPN Report 2023. URL: https://www.top10vpn.com/research/russia-vpn-report-2023/ (дата звернення 18.10.2024)

260. Saliceti F. Internet Addiction Disorder. URL: https://www.sciencedirect.com/science/article/pii/S1877042815025525 (дата звернення 10.11.2024)

261. Scuotto V., Serravalle F., Murray A., Viassone M. The Shift towards a Digital Business Model: A Strategic Decision for the Female Entrepreneur. Women Entrepreneurs and Strategic Decision Making in the Global Economy. 2019. Hershey, PA: IGI Global. DOI: 10.4018/978-1-5225-7479-8.ch007 (дата звернення 11.10.2024)

262. Sedrati, Y. & Sidi Athmane, M-W. The Cookies' Quest: Towards Digital TotalitarianLandscape. Journal of Studies in Language, Culture, and

Society (JSLCS)7(2), 2024 P. 182-199. URL: https://asjp.cerist.dz/en/downArticle/681/7/2/255742 (дата звернення 20.02.2025)

263. Shoshana Zuboff on Surveillance Capitalism's Threat to Democracy. URL: https://nymag.com/intelligencer/2019/02/shoshana-zuboff-q-and-a-the-age-of-surveillance-capital.html? (дата звернення 05.11.2024)

264. Smart-інфраструктура у сталому розвитку міст : світовий досвід та перспективи України. Центр Разумкова, Видавництво «Заповіт», Київ. 400 с. URL: https://razumkov.org.ua/uploads/other/2021-SMART-%D0%A1YTI-SITE.pdf (дата звернення 14.12.2024)

265. Starlink Official Website. URL: https://www.starlink.com (дата звернення 18.12.2024)

266. The complicated truth about China's social credit system URL: https://www.wired.com/story/china-social-credit-system-explained/ (дата звернення 20.10.2024)

267. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата звернення 18.10.2024)

268. The EU's Digital Services Act is undermining free speech URL: https://www.brusselsreport.eu/2022/04/25/the-eus-digital-services-act-is-undermining-free-speech (дата звернення 13.12.2024)

269. The Index Project: Nominee – Starlink. URL: https://theindexproject.org/award/nominees/396 (дата звернення 18.12.2024)

270. Toffler E. Third Way URL: https://ia801200.us.archive.org/9/items/TheThirdWave-Toffler/The-Third-Wave_-_Toffler.pdf (дата звернення 16.09.2024)

271. Tulsi Gabbard condemns Apple's plans to scan UK iP hones for child abuse images. URL: https://www.theguardian.com/us-news/2025/feb/26/tulsi-gabbard-uk-apple (дата звернення 10.12.2024)

272. Turkle Sh. Constructions and Reconstructions of the Self in Virtual Reality *Culture of the Internet*. 1997. P. 143–155.

273. UK Digital Strategy – GOV.UK. URL : https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy (дата звернення 10.12.2024)

274. UNESCO's response to COVID-19 pandemic. URL: https://en.unesco.org/covid19 (дата звернення 09.10.2024)

275. United Nations General Assembly Resolution A/RES/73/179 on the right to privacy in the digital age. URL: https://undocs.org/en/A/RES/73/179 (дата звернення 11.12.2024)

276. United Nations Human Rights Council Resolution A/HRC/32/L.20 on the promotion, protection, and enjoyment of human rights on the Internet URL: https://undocs.org/A/HRC/32/L.20 (дата звернення 11.12.2024)

277. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) URL: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.htm (дата звернення 11.12.2024)

278. US imposes trade restrictions on two Chinese firms over human rights URL: https://www.reuters.com/world/us-imposes-trade-restrictions-two-chinese-firms-over-human-rights-2024-12-10/ (дата звернення 11.12.2024)

279. Washington Post: Starlink, Ukraine, Pentagon, Elon Musk (2023) URL: https://www.washingtonpost.com/national-security/2023/06/01/starlink-ukraine-pentagon-elon-musk/ (дата звернення 15.12.2024)

280. Why compare the digital strengths and weaknesses of economies? URL:https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/ (дата звернення 02.12.2024)

281. Zizek S. The Next Revolution – the Digital Commons? URL: https://socialecologies.wordpress.com/2018/10/31/slavoj-zizek-the-next-revolution-the-digital-commons/ (дата звернення 05.11.2024)

282. Zuboff Sh. Big other: surveillance capitalism and theprospects of an informationcivilization
URL: https://journals.sagepub.com/doi/epdf/10.1057/jit.2015.5 (дата звернення 05.11.2024)

283. 翻译：**巨蟹 、少平以太坊**（Ethereum ）:**下一代智能合**约和去中心化应用台
URL: https://wohugb.github.io/blockchain/ethereum/whitepaper/ (дата звернення 13.12.2024)

284. **中**华人民共和国网络安全法. URL: https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm (дата звернення 13.12.2024)

285. **中**华人民共和国个人信息保护法. URL: https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm (дата звернення 13.12.2024)

286. **中**华人民共和国数据安全法.
URL:https://www.gov.cn/xinwen/2021-06/11/content_5616919.htm (дата звернення 13.12.2024

ДОДАТКИ

Додаток А. Список опублікованих наукових праць автора за темою дисертації

Фахові українські видання :

1. Сокоринський В. О Сучасні інструменти захисту прав, свободи та безпеки особистості в епоху «Цифрового тоталітаризму». *Регіональні студії*. 2022. Вип. 28. С.35-39. URL: http://www.regionalstudies.uzhnu.uz.ua/archive/28/6.pdf

2. Сокоринський В. О. Сучасні системи захисту прав людини в КНР в контексті загрози «цифрового тоталітаризму» *Регіональні студії*. Вип. 33. С.39-44. URL: http://regionalstudies.uzhnu.uz.ua/archive/33/7.pdf

3. Сокоринський В. О «Цифровий Паноптикум» як метод розповсюдження цифрового тоталітаризму та загроза сучасним міжнародним відносинам. *Politicus*. 2024. № 2. С.118-122. URL: http://politicus.od.ua/2_2024/2_2024.pdf

Публікації, які засвідучують апробацію матеріалів дисертації

4. Сокоринський В.О. Цифровий тоталітаризм як виклик інтеграційним процесам у світі. У *Соціально-економічний та політичний розвиток країн в умовах глобальної нестабільності* [Електронний ресурс] : матеріали Міжнародної науково-практичної конференції (м. Одеса, 27 травня 2022 р.). Одеса: Одес. нац. ун-т ім. І. І. Мечникова, 2022. 5с.

5. Сокоринський В.О. Цифровий тоталітаризм як загроза сучасній цифровій дипломаті. У *Сучасні загрози глобальній та регіональній безпеці* : матер.Міжнар. наук.-практ. інтерн.-конф. (м. Одеса, 29 жовтня 2023 р.) уклад. А. Полухіна; ГО «ГУЕЦ». Одеса: Фенікс, 2023. 389 с.

6. Сокоринський В.О. Цифровий Паноптикум як метод розповсюдження Цифрового тоталітаризму. Сучасні системи

спостереження та контролю за суспільствами. У *Трансформація українського суспільства в цифрову еру* : матеріали III Всеукраїнської науково-практичної конференції, 22 березня 2024 р. Львів – Торунь : Liha-Pres, 2024. 108 с. URL:https://dspace.onua.edu.ua/server/api/core/bitstreams/e21276ef-218d-4e4d-905f-7c7d428df5ad/content

7. Сокоринський В.О. Сучасний стан загроз цифрового тоталітаризму у світі. VI Міжнародна науково-практична конференція У *Політичні процеси сучасності : глобальний та регіональний виміри*. 8-9 травня 2025 р. м.Івано-Франківськ. URL: https://kpn.pnu.edu.ua/2025/05/06/prohrama-konferentsii/

8. Сокоринський В.О., Мілова М.І. Цифровий тоталітаризм: трансформація влади в епоху тотального нагляду. У *Сталий розвиток регіонів, міст та спільнот в умовах глобальних перетворень: виклики, можливості, сценарії майбутнього.* Міжнародна наукова конференція. 16 травня 2025 р. м. Одеса. URL: https://onu.edu.ua/uk/fakultety/fakultet-mizhnarodnykh-vidnosyn-politolohii-ta-sotsiolohii/mizhnarodna-konferentsiia-do-iuvileiu-onu-ta-fmvps-stalyi-rozvytok-v-umovakh-hlobalnykh-zmin

Додаток Б. Акти впровадження дисертаційного дослідження

Департамент цифрового розвитку, інформаційної політики та туризму
Одеської обласної державної адміністрації

АКТ
впровадження результатів дисертаційного дослідження
Сокоринського Володимира Олеговича
на тему: «Феномен цифрового тоталітаризму: концептуалізація загроз демократії в інформаційному суспільстві»,
поданої на здобуття наукового ступеня доктора філософії за спеціальністю 052 Політологія,
в галузі знань 05 – соціальні та поведінкові науки

Дисертаційна робота Сокоринського Володимира Олеговича виконана відповідно до плану підготовки PhD аспірантів та є складовою комплексної науково-дослідної теми кафедри політології Одеського національного університету імені І.І. Мечникова «Динаміка локальних політичних процесів в умовах глобальної світ-системної трансформації». (державна реєстрація № 0123U102703 від 28.05.23)

Результати дисертаційного дослідження автора, висновки, окремі теоретико-прикладні пропозиції запропоновані для використання в роботі Департаменту за напрямом «інформаційна політика», «комунікації з громадськістю», цифрова освіта, в освітянських проектах з медіаграмотності «Фільтр» та платформа онлайн-освіти Prometheus, які мають на меті вчитися визначати маніпулятивний медіаконтент, розрізняти дезінформацію, шкідливі пропагандистські наративи тощо.

На нашу думку, результати дисертаційного дослідження є актуальними, особливо в умовах подальшої цифровізації, важливими та мають практичну значущість.

Виконуючий обов'язки
Директора **Гнатюк Ю.О.**

ЗАТВЕРДЖЕНО
Ректор Одеського національного
університету імені І.І. Мечникова

професор **ТРУБА В.І.**

_____ 2025 р.

АКТ
впровадження результатів дисертаційного дослідження
Сокоринського Володимира Олеговича
на тему: «Феномен цифрового тоталітаризму: концептуалізація загроз демократії в інформаційному суспільстві»
поданої на здобуття наукового ступеня доктора філософії за спеціальністю 052 Політологія,
в галузі знань 05 – соціальні та поведінкові науки

Дисертаційна робота *Сокоринського Володимира Олеговича* виконана відповідно до плану підготовки PhD аспірантів та є складовою комплексної науково-дослідної теми кафедри політології Одеського національного університету імені І.І. Мечникова «Динаміка локальних політичних процесів в умовах глобальної світ-системної трансформації».
(державна реєстрація № 0123U102703 від 28.05.23 р.)

Результати наукового дослідження автора, висновки, окремі теоретичні та прикладні пропозиції запропоновано для використання під час навчального процесу при викладанні дисциплін: «Політологія», «Вступ до фаху», «Загальна теорія політики», «Порівняльний аналіз політичних систем», «Сучасна зарубіжна політологія», «Політична культура та ідеологія», «Політичні комунікації», «Політична конфліктологія», «Політичне прогнозування», при написанні курсових, бакалаврських та магістерських робіт, при підготовці методичних рекомендацій з відповідних дисциплін, а також в написанні навчальних посібників.

Зважаючи на вищезазначене комісія у складі: Глєбова В.В., декана ФМВПС ОНУ ім. І.І. Мечникова, к. і. н., доцента, - голова комісії; Узун Ю.В., - заступника декана з наукової роботи ФМВПС ОНУ ім. І.І. Мечникова, д. політ. наук, професора; Коч С.І., - завідувача кафедри політології ФМВПС ОНУ ім. І.І. Мечникова, д. політ. наук, професора зазначає, що результати дисертації *Сокоринського Володимира Олеговича на тему: «Феномен цифрового тоталітаризму: концептуалізація загроз демократії в інформаційному суспільстві»,* поданої на здобуття наукового ступеня доктора філософії за спеціальністю 052 Політологія, в галузі знань 05 – соціальні та поведінкові науки, впроваджені у навчальний процес факультету міжнародних відносин, політології та соціології Одеського національного університету імені І.І. Мечникова.

Заступник декана з наукової роботи
факультету міжнародних відносин, політол та соціології
Одеського національного університету імені І.І. Мечникова, д. політ. н., професор

Юлія УЗУН
«13» Березня 2025 р.

Декан
факультету міжнародних відносин, політології та соціології
Одеського національного університету імені І.І. Мечникова, к. і. н., доцент

Віктор ГЛЄБОВ
«13» Березня 2025 р.

МП

Керівних наукової теми кафедри:
«Динаміка локальних політичних процесів в умовах глобальної світ-системної трансформації».
державна реєстрація № 0123U102703
д. філос. н., професор

Василь ПОПКОВ
«18» Березня 2025 р.

Завідувач кафедри політології
Одеського національного університету імені І.І. Мечникова
д. політ. н., професор

Світлана КОЧ
«18» Березня 2025 р.