УДК 177:316.4]:004-049.5
DOI https://doi.org/10.32782/IT/2024-4-15

Ольга КИВЛЮК
доктор філософських наук, професор, завідувачка кафедри філософії та психології, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе 210, м. Київ, Україна, 02121
***ORCID:** 0000-0002-7900-9299*
***Scopus Author ID:** 57196318811*

Бібліографічний опис статті: Кивлюк, О. (2024). Теоретико-методологічні засади інформаційної та кібернетичної безпеки в умовах цифровізації суспільних процесів. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 4, 125–131, doi: https://doi.org/10.32782/IT/2024-4-15

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬНИХ ПРОЦЕСІВ

Мета роботи. *Метою дослідження є теоретичний аналіз сутності інформаційної та кібернетичної безпеки в умовах цифровізації суспільних процесів, що передбачає концептуалізацію філософських, соціальних, політично-правових, етичних та технологічних аспектів взаємодії людини, суспільства та цифрових технологій в контексті загроз та ризиків.*

Методологія дослідження: *діалектичний метод дозволив розглянути соціальні процеси в контексті цифровізації суспільства; міждисциплінарний підхід створив можливості поєднання філософських, соціальних, технічних та політико-правових аспектів аналізу інформаційної та кібернетичної безпеки; системний підхід забезпечив розгляд інформаційної та кібернетичної безпеки як багаторівневої системи, яка охоплює технічні, організаційні та соціальні компоненти в контексті ідентифікацій взаємозв'язків між загрозами, ризиками та заходами безпеки; феноменологічний метод скорегував необхідність вивчення процесів цифровізації суспільства в контексті ризиків та потенційних загроз; прогностичний підхід змоделював можливі сценарії розвитку загроз в умовах цифровізації щодо підвищення рівня інформаційної та кібернетичної безпеки; оціночний та порівняльний методи забезпечення механізмів регулювання інформаційної та кібернетичної безпеки у відповідності до сучасних викликів цифровізації.*

Наукова новизна *полягає у інтегрованому підході дослідження впливу цифровізації на безпекові аспекти суспільних процесів, прогнозування кіберзагроз та негативних впливів інформаційних викликів, удосконалення механізмів забезпечення інформаційної та кібернетичної безпеки в цифровому вимірі, адаптації методологічних підходів щодо цифрової трансформацій, розвитку інформаційної інфраструктури, заходів захисту від цифрових маніпуляцій та дезінформації в межах соціально-філософських, політико-правових та етичних аспектів.*

Висновки. *В результаті теоретичного дослідження було здійснено концептуалізацію філософських, соціальних, політично-правових, етичних та технологічних аспектів інформаційної та кібернетичної безпеки в умовах цифровізації суспільних процесів, а також спрогнозовано механізми захисту інформаційного простору від існуючих та можливих загроз у контексті сучасних викликів техногенної цивілізації.*

Ключові слова: *інформаційна безпека, кібербезпека, цифровізація, людина, цифрові технології, суспільні процеси, техногенна цивілізація.*

Olga KYVLIUK
Doctor of Philosophical Sciences, Professor, Head of the Department of Philosophy and Psychology, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121,
o.p.kyvliuk@gmail.com
***ORCID:** 0000-0002-7900-9299*

To cite this article: Kyvliuk, O. (2024). Teoretyko-metodolohichni zasady informatsiynoyi ta kibernetychnoyi bezpeky v umovakh tsyfrovizatsiyi suspil nykh protsesiv [Theoretical and methodological foundations of information and cyber security in the context of digitalisation of social processes] *Information Technology: Computer Science, Software Engineering and Cyber Security,* 4, 125–131, doi: https://doi.org/10.32782/IT/2024-4-15

THEORETICAL AND METHODOLOGICAL FOUNDATIONS OF INFORMATION AND CYBER SECURITY IN THE CONTEXT OF DIGITALISATION OF SOCIAL PROCESSES

Aim of the study. *The purpose of the study is to theoretically analyse the essence of information and cyber security in the context of the digitalisation of social processes, which involves conceptualising the philosophical, social, political, legal, ethical and technological aspects of the interaction between man, society and digital technologies in the context of threats and risks.*

Methodology. *The dialectical method allowed us to consider social processes in the context of the digitalisation of society; the interdisciplinary approach created opportunities to combine philosophical, social, technical, political and legal aspects of the analysis of information and cyber security; the systemic approach ensured consideration of data and cyber security as a multilevel system that covers technical, organisational and social components in the context of identifying the relationships between threats, risks and security measures; the phenomenological method adjusted the need to study the processes of digitalisation of society in the context of risks and potential threats; the systemic approach ensured consideration of information and cyber security as a multilevel system that covers technical, organisational and social components in the context of identifying the relationships between threats, risks and security measures; the phenomenological method adjusted the need to study the processes of digitalisation of society in the context of risks and potential threats;*

The scientific novelty *lies in an integrated approach to studying the impact of digitalisation on the security aspects of social processes, forecasting cyber threats and the negative effects of information challenges, improving mechanisms for ensuring information and cyber security in the digital dimension, adapting methodological approaches to digital transformations, developing information infrastructure, measures to protect against digital manipulation and disinformation within the socio-philosophical, political, legal and ethical aspects.*

Conclusions. *As a result of the theoretical study, the author conceptualised the philosophical, social, political, legal, ethical and technological aspects of information and cyber security in the context of the digitalisation of social processes, and also predicted the mechanisms for protecting the information space from existing and possible threats in the context of modern challenges of technogenic civilisation.*

Key words: *information security, cybersecurity, digitalisation, human, digital technologies, social processes, and technogenic civilisation.*

Актуальність проблеми. Цифровізація суспільних процесів є не просто феноменом, а й незаперечним реальним фактом. Даний процес, як і технологізація, комп'ютеризація, чи то інформатизація – є неспинним і незворотнім, а отже, має як свої переваги так і недоліки. Зважаючи на умови протидії воєнній агресії Російської Федерації, завдання забезпечення та запобігання загрозам кіберзлочинності, інформаційного маніпулювання, протиправного розповсюдження персональних даних громадян, державних реєстрів, національних та комерційних таємниць тощо, стає вкрай складним і більш ніж актуальним. Тому важливо, щоб проблематика інформаційної та кібернетичної безпека носила не тільки технократичний характер, а й набула антропологічного, етично-ціннісного значення, не зважаючи на її цифровий, а подекуди віртуальний вимір.

Теоретико-методологічні засади інформаційної та кібернетичної безпеки як концептуальний підхід, фокусується на осмисленні принципів, цінностей, і стратегій захисту інформації та цифрових інфраструктур від реальних та можливих загроз, використовуючи як технічнологічні, так і етичні підходи.

Захист інформації від несанкціонованого доступу; гарантії точності, цілісності та незмінності (за умови необхідності) даних; забезпечення безперебійної доступності до інформаційних систем, авторизації користувача, здійснення пошукових завдань; прозорість та відповідальність оператора/організації щодо збереження, обробки, представлення та передачі даних; дотримання етичних стандартів, враховуючи права людини, приватність та інші соціальні аспекти формують основні принципи філософії інформаційної та кібернетичної безпеки.

Філософські питання, що лежать в основі концептуального підходу до цифровізації суспільних процесів, які потребують заходів безпеки в інформаційно-комунікаційному просторі можна визначити наступним чином:

- Де закінчується свобода і починається контроль?
- Як знайти баланс між правом на приватність і потребою в здійсненні заходів для забезпечення безпеки?
- Як гарантувати, що технології та штучний інтелект сприятимуть захисту людської гідності, особистої приватності та дотриманню прав людини, уникатимуть дискримінації, а також будуть використовуватися для загального блага, а не для маніпуляцій чи необґрунтованого контролю?
- Чи повинна людина обмежувати розвиток технологій та штучного інтелекту через ризики, які вони створюють у сфері безпеки?

- Як забезпечити інклюзивність та рівний доступ до цифрових технологій для всіх верств населення в контексті запобігання цифрової нерівності?
- Яке місце відводиться людині у системі кібербезпеки?
- Як гармонізувати технократичні та гуманістичні цінності у цифровому суспільстві?

Це, безумовно, лише частина питань, які вимагають детального розгляду та пошуку відповідей.

Аналіз останніх досліджень і публікацій. Акцентуючи на міждисциплінарності та багаторівневості процесу цифровізації, соціально-філософський аспект даної проблематики досліджувався в роботах як вітчизняних науковців: Воронокової В. та Нікітенко В., які в монографії «Філософія цифрової людини і цифрового суспільства: теорія і практика» аналізуються взаємодія цифрового суспільства та цифрової людини як соціального феномену; Олексенко Р. зосереджується на ціннісному вимірі цифрової освіти та цифрової людини у діджиталізованому суспільстві, Бєлов Д. розглядає доктринальні засади цифрового права; так і відомих закордонних вчених серед яких відмітимо: Андрюкайтене Р. описує цифрові суспільні трансформації, Бріньолфссон Е., Макафі Е. досліджують вплив цифрових технологій на економіку та суспільство, Скінер К., Штаб К., Даґоґо О., Пентленд А. також вивчають різні аспекти цифровізації, включаючи економічні, соціальні та технологічні зміни в сучасному суспільстві та інші.

Сутність поняття інформаційної безпеки розглядалася в роботах: Золотар О., яка досліджує права та свободу людини в умовах інформаційного суспільства його перспектив та загроз; Бикова О., який аналізує правовий та культурологічний виміри інформаційної безпеки, підкреслюючи її важливість у сучасному суспільстві; Валлерстейн І. розглядає інформаційну безпеку з урахуванням трансдисциплінарної стратегії досліджень; Петрик В. відмічає, що поняття «безпека» і «небезпека» є діалектично взаємозалежними, тобто не існують у природі окремо.

Незважаючи на дотичність і синтезованість інформаційної та кібернетичної безпеки, більшу увагу другому було сконцентровано в дослідженнях: Деннінг Д. підкреслює, що кібербезпека спрямована на захист комп'ютерних систем, мереж та цифрової інформації від несанкціонованого доступу, модифікації чи знищення; Столлінгс В. концентрується на протидії кіберзагрозам та мережевій безпеці; Бурячок В. досліджує концептуальні основи створення ефективної системи кібернетичної безпеки на державному рівні та наголошує на важливість міжнародного співробітництва у сфері кібербезпеки.

Мета дослідження полягає у теоретичному аналіз сутності інформаційної та кібернетичної безпеки в умовах цифровізації суспільних процесів, що передбачає концептуалізацію філософських, соціальних, технічних аспектів взаємодії людини, суспільства та цифрових технологій в контексті загроз та ризиків.

Цифровізація суспільних процесів. Трансформація суспільних процесів пов'язана з цифровізацією, а саме: зростання кількості цифрових даних та електронних транзакцій, розвиток технологій штучного інтелекту та Інтернету речей, трансформація соціальних комунікацій та бізнес-процесів, розмивання кордонів між цифровою та фізичною реальністю, формування нових моделей соціальної комунікації як в локальному так і глобальному форматах – створює нові виклики для суспільства в цілому та конкретної людини зокрема, концентруючи увагу на гармонійному балансі між безпекою та правами людини (Pentland, 2014).

Цифрове суспільство виникло як унікальний і багатогранний соціальний феномен, який інтегрував сучасні технології у всі сфери життя людини. Воно проходить етапи еволюції, трансформуючись із простих двовимірних взаємодій у складні тривимірні системи, де реальне і віртуальне поступово зливаються в єдине ціле. Цей процес супроводжується «розмиванням» меж між фізичною та цифровою реальністю, що надає нових можливостей для соціальної взаємодії, водночас викликаючи низку викликів та змін у людській діяльності.

Цифрова «ерозія» стала помітною на різних етапах розвитку суспільства. Вона проявляється через перехід соціальної активності людини в площину, де центральними елементами стають інформація, дані та цифрові коди. У результаті цього формується новий шар ідентичності людини – її «цифрові атрибути». Ці атрибути, включаючи онлайн-профілі, віртуальну репутацію, цифрову компетенцію та інші характеристики, стали невід'ємною частиною особистості та вплинули на те, як людина взаємодіє з суспільством. Процес розвитку цифрового суспільства можна розглядати як взаємну трансформацію: з одного боку, цифровізація змінює соціальну діяльність людини, з іншого боку – «цифрові атрибути» людей формують характер і темпи цієї трансформації. Взаємодія цих аспектів сприяє формуванню нових

механізмів управління, комунікації та інтеграції у цифровому просторі (Кивлюк, Воронкова, Нікітенко, 2023).

Цифровізація реалізує накопичення інформаційних ресурсів і даних, їхню циркуляцію та обробку. Водночас інтелектуалізація додає цьому процесу зміст, інтегруючи дані в системи прийняття рішень та оптимізації діяльності. Такий симбіоз дозволяє суспільству адаптуватися до викликів цифрової епохи та максимально використовувати потенціал технологій.

Проте цифровізація соціальної діяльності людини не лише створює умови для функціонування цифрового суспільства, але й глибоко впливає на саму людину. Вона змінює її поведінку, цінності та взаємодію зі світом, формуючи нові підходи до комунікації, роботи та навіть мислення. Люди поступово набувають нових навичок, адаптуючись до швидких технологічних змін, що водночас відкриває нові горизонти та ставить перед суспільством складні моральні, етичні та соціальні питання. Цифрове суспільство можна розглядати як динамічну систему, що формується завдяки взаємодії технологій, даних і людської діяльності. Це суспільство, де цифрові інструменти не лише полегшують життя, а й створюють нові вимоги та загрози, змінюючи уявлення про реальність та соціокультурну взаємодію.

Досліджуючи права людини через призму держаної політики цифровізації суспільних процесів у сфері нацбезпеки, Д. Чижов розглядає два напрямки наукового пошуку: забезпечення інформаційної безпеки як складової національної безпеки в умовах цифровізації та упровадження цифрової трансформації Збройних сил і забезпечення інформаційної безпеки. Він вважає, що інформаційна і кібернетична системи мають розглядатися синергетично та системно з врахуванням природи технократичних, міждисциплінарних, темпоральних підходів. Обґрунтовуючи значимість інформаційної та кібернетичної безпеки особистості, звертає увагу на симбіоз безпеки «держава – суспільство – людина» та акцентує на переході держаної безпеки в оборонну, у зв'язку з воєнним станом в країні (Чижов, 2021).

Інформаційна безпека. Інформаційна безпека являє собою стан захищеності інформаційного простору і охоплює захист інформації в усіх її формах та проявах, функціонує в інтересах громадян, організацій, держави, що окрім того включає заходи захисту від негативних інформаційних маніпуляцій, пропаганди та інформаційно-психологічну безпеку. Інформаційна безпека – це не тільки засіб, чи то механізм запобігання, або подолання негативних проявів цифровізації, – це засіб для досягнення інформаційно-технічного прогресу з врахуванням гуманістичних, етичних, соціальних, політично-правових тощо аспектів.

З точки зору філософсько-антропологічного підходу варто наголосити на цінності та захищеності психічного, ментального, навіть фізичного здоров'я людини від деструктивних інформаційних впливів, що призводить до негативних наслідків.

О. Золотар у своїй монографії «Інформаційна безпека людини: теорія і практика» зазначає, що у філософському контексті важливо зосередитися на трьох ключових аспектах дослідження даної проблематики: онтологічному, де природа інформаційної безпеки є складною багатовимірною категорією, що включає аналіз сутності інформаційних загроз, їх впливу на людину, суспільство та ноосферу; гносеологічному, що аналізує пізнавальний аспект, який здійснює людина як суб'єкт пізнання, інформаційної безпеки, включаючи вивчення процесів отримання, обробки, зберігання та передачі знань, а також методів їх захисту; логічному, де досліджуються основи побудови системи аргументів, стратегій та структур інформаційної безпеки, а також розглядаються принципи логічної послідовності в процесі захисту, прийнятті рішень і розробці політик безпеки, що враховують причинно-наслідкові зв'язки між загрозами, ризиками та заходами захисту (Золотар, 2018).

Тобто, автор пропонує системний підхід до аналізу інформаційної безпеки, який охоплює не лише технічні аспекти, але й філософські, що є важливим заданням для забезпечення гармонійного функціонування інформаційного простору.

Аналіз сучасних публікацій дозволив узагальнити механізми забезпечення інформаційної безпеки особистості – це:

по-перше, загальна освіченість кожної людини, тобто рівень її теоретичної освіти та практичних компетентностей щодо інформаційних можливостей та загроз в контексті успішної життєдіяльності та гармонійного саморозвитку;

по-друге, здійснення загальнодержавних заходів задля створення безпекового рівня як в межах задоволення потреб особистості в інформаційних продуктах, так і можливих загроз;

по-третє, створення дієвого правового поля в контексті державного контролю функціонування інформаційного простору/середовища, щодо запобіганню інформаційних небезпек та відповідних процедур покарання;

по-четверте, гарантування захищеності інтересів людини від можливих гіпотетичних інформаційних загроз різного роду;

по-п'яте, забезпечення інформаційна рівності.

Тобто, з огляду на зазначене вище, людина, при всьому її бажанні та освіченості, не зможе створити свій особистий безпековий інформаційний вимір, а для цього має існувати суспільний інформаційно-безпековий рівень. От наприклад, у Філософському енциклопедичному словнику, «безпека національна – поняття політології та соціальної філософії, яке визначає певний ступінь захищеності особистості, суспільства, держави від внутрішніх та зовнішніх загроз, що дозволяє їм нормально існувати та розвиватися» (Шинкарук, 2002: с. 49). Національна безпека – це і соціальна система, це і державний пріоритет, це і національно-культурний процес, це законодавча доктрина, це політична інституція, це економічний розвиток тощо.

Отже, інформаційна безпека суспільства залежить від сукупності інтегрованих політичних, правових, економічних, соціальних, технологічних процесів, а також і окремих особистостей, дії яких спрямовані на попередження, запобігання, виявлення, подолання негативних подій, або вже їх наслідків.

Зрозуміло, що взаємозалежність високого рівня інформаційної безпеки суспільства і окремої людини в контексті інтелектуального, етичного, духовного, критичного та креативного розвитку очевидна. А провідником, так би мовити посередником, між людиною і суспільством, що гармонізує дану взаємозалежність є – держава, яка має створювати умови для розвитку та продуктивного функціонування, стабільності та захищеності інформаційної інфраструктури від негативних впливів: інформаційні війни, маніпулювання, інформаційний тероризм, незаконне оприлюднення конфіденційної інформації, кіберзлочинність і т.д., тобто все те, що загрожує та шкодить національним інтересам, суверенітету держави, економічній та політичній стабільності, міжнародному співробітництву.

Кібернетична безпека. Кібернетична безпека в епоху цифровізації сфокусована на забезпеченні конфіденційності, цілісності та доступності інформації в кіберпросторі, що охоплює захист критичної інформаційної інфраструктури та протидію кіберзагрозам.

Для ефективного захисту інформації та активів у сфері кібернетичної безпеки недостатньо застосовувати єдиного векторного підходу. Необхідно враховувати різноманітні види засобів та заходів контролю кібербезпеки та оптимально інтегрувати їх у діяльнісну сферу. Усі технологічні процеси стикаються з ризиками безпеки та конфіденційності. Хоча сучасні цифрові технології здатні ефективно протидіяти кіберзагрозам, цього замало. Важливо мати гарантії, що державні, політичні, комерційні процеси та етично-правова поведінка окремих особистостей також спрямовані на зниження або усунення цих ризиків. Оскільки забезпечення кібербезпеки є складним і багатогранним завданням, як на державному, комерційному так і особистісному рівнях, дедалі частіше впроваджують стандартизовані підходи для управління інформаційною безпекою. У цьому контексті ключову роль відіграють системи управління інформаційною безпекою, які: виявляють загрози в сфері IT-безпеки швидко і на ранніх стадіях; своєчасно впроваджують відповідні заходи для нейтралізації IT-ризиків; гарантують відповідність внутрішнім вимогам та міжнародним стандартам; зменшують навантаження на IT-персонал за допомогою автоматизації виявлення вразливостей; забезпечують надання повної доказової бази щодо інцидентів комп'ютерної безпеки. Таким чином, системний підхід до кібербезпеки дозволяє створити ефективніші механізми захисту, що враховують як технологічні, так і організаційні аспекти (Кивлюк; Воронкова, 2022).

Превентивність, комплексність, адаптованість, багаторівневість, стандартизованість, безперервність, економічна доцільність, організаційна узгодженість, правова захищеність – це основні принципи функціонування кібернетичної безпеки.

Аналіз існуючих науково-практичних розвідок дозволив узагальнити напрямки та завдання розвитку кібернетичної безпеки задля підвищення її рівня:

- освітня діяльність в контексті «кібергігієни» (підвищення обізнаності щодо основ кібербезпеки користувачів IT, створення навчальних програм, курсів та тренінгів для моделювання можливих загроз та пропедевтики їх подолання);
- розвиток культури кібербезпеки, як наслідку високого рівня кіберосвіченості;
- автоматизація процесів реагування на кіберзагрози (наприклад, SOAR-платформи дозволяють автоматизувати рутинні завдання кіберзахисту та прискорюють реагування на інциденти);
- міжнародна співпраця в контексті глобальних ініціатив та обміну інформацією задля боротьби з кіберзлочинністю та аналізу кіберзагроз;

- розробка стандартів безпеки (наприклад, GDPR або CCPA), їх моніторинг та управління;
- удосконалення механізмів для захисту конфіденційних даних, тобто вдосконалення методів біометричної автентифікації;
- використання штучного інтелекту для безперервного аналізу та алгоритму передбаченню кіберзагроз у режимі реального часу, але при умові що загроза йде не від самого ШІ;
- розвиток квантової криптографії, тобто сучасні еволюційні технології створюють нові загрози, а з їх розвитком треба бути «озброєним» новим рівнем безпеки;
- використання блокчейн-технологій для забезпечення захисту (наприклад, R3 Corda? Quorum, Dragonchain, Hyperledger Besu) та децентралізації управління даними;
- політика «нульової довіри» з елементами мікросегментація для мінімізації ризиків;

Висновки і перспективи подальших досліджень. Формування нових парадигм інформаційної та кібернетичної безпеки вимагає створення інтегрованих теоретико-методологічних підходів щодо дослідження викликів цифровізації суспільства. Етичні питання в контексті соціальної відповідальності цифровізації потребують комплексного вивчення та розробки стандартів етичного використання цифрових даних у цифровому середовищі. Серед перспективних завдань подальших наукових розвідок також відзначаємо: дослідження впливу цифровізації на соціальні інституції, освітні ініціативи щодо підвищення рівня обізнаності серед громадян та кібернетичної культури, правове регулювання та міжнародна стандартизація протистоянню кіберзагрозам, розробку інтелектуальних систем безпеки в контексті застосування штучного інтелекту. Взагалі, подальші дослідження мають бути зорієнтовані на створення інтегрованих, адаптивних і стійких систем інформаційної та кібернетичної безпеки, здатних ефективно протидіяти існуючим і гіпотетично можливим викликам цифрового світу.

Отже, в результаті теоретичного дослідження було здійснено концептуалізацію філософських, соціальних, політично-правових, етичних та технологічних аспектів інформаційної та кібернетичної безпеки в умовах цифровізації суспільних процесів, а також спрогнозовано механізми захисту інформаційного простору від існуючих та можливих загроз у контексті сучасних викликів техногенної цивілізації.

ЛІТЕРАТУРА:

1. Бріньолфссон Е., Макафі Е. Друга епоха машин: робота, прогрес та процвітання в часи надзвичайних технологій. Київ: K. FUND, 2016. 236 с.

2. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки : монографія. К. : НАУ, 2013. 431 с.

3. Даґоґо О. Нове мислення. Від Айнштейна до штучного інтелекту: наука і технології, що змінили світ / пер. з англ. І. Возняка. Харків : Віват, 2021. 368 с.

4. Золотар О. О. Інформаційна безпека людини : теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

5. Кивлюк О., Воронкова В., Нікітенко В. Цифрові права як вираження цифрових атрибутів людини: соціально-філософське обґрунтування. Освітній дискурс : збірник наукових праць. Київ : ТОВ«НІА «НТІ». 2023. Випуск 44 (4-6). С. 7–26. https://doi.org/10.33930/ed.2019.5007.44(4-6)-1.

6. Кивлюк О. П., Воронкова В. Г. Філософська рефлексія інформаційної безпеки у цифровому середовищі: проблеми, ризики, правове забезпечення. Innovative resources of modern science : collective monograph. Compiled by V. Shpak; Chairman of the Editorial Board S. Tabachnikov. Sherman Oaks, California : GS Publishing Services, 2022. С. 160–172. (186 p.) DOI: 10.51587/9798-9866-95907-2022-009-160-172.

7. Петрик В., Канарський Ю. Методи гібридної війни Росії проти України. Напрями протидії. Information Technology and Security. 2015. Vol. 3, Iss. 1 (4). P. 30–37.

8. Скінер К. Людина цифрова. Фабула. 2020. 272 с.

9. Філософський енциклопедичний словник : энциклопедия / НАН України, Ін-т філософії ім. Г. С. Сковороди ; голов. ред. В. І. Шинкарук. Київ : Абрис, 2002. 742 с.

10. Чижов Д. А., Державна політика забезпечення прав людини у сфері національної безпеки в умовах цифровізації. Науковий вісник Національної академії внутрішніх справ, 2021. № 4 (121). с. 46–52.

11. Alex Pentland, Social Physics: How Social Networks Can Make Us Smarter, Scribe Publications, 2014, p. 300.

12. Denning D., Information Warfare and Security, ACM Press, 1999, p. 522.

REFERENCES:

1. Brynjolfsson, E., & McAfee, A. (2016). Druha epokha mashyn: robota, prohres i protsvitannya v chas nadzvychaynykh tekhnolohiy [The Second Machine Age: Work, Progress, and Prosperity in a Time of Extraordinary Technology]. Kyiv. FUND. [in Ukrainian].

2. Buryachok, V. L. (2013). Osnovy formuvannya systemy kiberbezpeky derzhavy: monohrafiya [Fundamentals of the formation of a state cyber security system: monograph] Kyiv: NAU. [in Ukrainian].

3. Dagogo, O. (2021). Nove myslennya. Vid Eynshteyna do shtuchnoho intelektu: nauka i tekhnolohiyi, yaki zminyly svit [New Thinking. From Einstein to Artificial Intelligence: Science and Technologies That Changed the World] (trans. from English by I. Wozniak). Kharkiv: Vivat. [in Ukrainian].

4. Zolotar, O. O. (2018). Informatsiyna bezpeka lyudyny: teoriya i praktyka [Human Information Security: Theory and Practice: Monograph]. Kyiv: LLC “ArtEk Publishing House”. [in Ukrainian].

5. Kyvlyuk, O., Voronkova, V., & Nikitenko, V. (2023). Tsyfrovi prava yak vyrazhennya tsyfrovykh atrybutiv lyudyny: sotsial'no-filosofs'ke obgruntuvannya [Digital rights as an expression of human digital attributes: a socio-philosophical justification]. *Educational discourse: collection of scientific works*, 44(4-6), P. 7–26. [in Ukrainian]. https://doi.org/10.33930/ed.2019.5007.44(4-6)-1

6. Kyvlyuk, O. P., & Voronkova, V. G. (2022). Filosofs'ka refleksiya informatsiynoyi bezpeky v tsyfrovomu seredovyshchi: problemy, ryzyky, pravove zabezpechennya [Philosophical reflection on information security in the digital environment: problems, risks, legal support]. *Innovative resources of modern science: collective monograph* (pp. 160–172). Sherman Oaks, California: GS Publishing Services. https://doi.org/10.51587/9798-9866-95907-2022-009-160-172

7. Petryk, V., & Kanarsky, Y. (2015). Methods of Russia’s hybrid war against Ukraine [Methods of Russia’s hybrid war against Ukraine]. Directions of counteraction. *Information Technology and Security*, 3(1), 30–37. [in Ukrainian].

8. Skinner, K. (2020). Tsyfrova lyudyna [Digital Man]. Fabula. [in Ukrainian].

9. hynkaruk, V. I. (Ed.). (2002). Filosofs'kyy entsyklopedychnyy slovnyk: Entsyklopediya [Philosophical Encyclopedic Dictionary: Encyclopedia]. Kyiv: Abrys. [in Ukrainian].

10. Chyzhov, D. A. (2021). Derzhavna polityka zabezpechennya prav lyudyny u sferi natsional'noyi bezpeky v umovakh tsyfrovizatsiyi [State policy of ensuring human rights in the sphere of national security in the context of digitalization]. *Naukovyy visnyk Natsional'noyi akademiyi vnutrishnikh spravScientific* (4), 46–52. [in Ukrainian].

11. Pentland, A. (2014). *Social Physics: How Social Networks Can Make Us Smarter*. Scribe Publications.

12. Denning, D. (1999). *Information Warfare and Security*. ACM Press.