Педагогічні науки

УДК 02:004.056]:378.147

**Цимбал Світлана Миколаївна**

*кандидат філософських наук, доцент,*

*доцент кафедри професійної підготовки,*

*документознавства та публічного управління*

*Український державний університет імені Михайла Драгоманова*

**Tsymbal Svitlana**

*PhD in Philosophy, Associate Professor,*

*Associate Professor of the Department of Professional Training,*

*Document Studies and Public Administration*

*Mykhailo Dragomanov State University of Ukraine*

*ORCID: 0000-0001-5354-6187*

DOI: https://doi.org/10.25313/2520-2057-2026-6-12081

# ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ КУЛЬТУРИ ЗДОБУВАЧІВ ОСВІТИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ
# DEVELOPING INFORMATION LITERACY OF HIGHER EDUCATION STUDENTS IN THE CONTEXT OF HYBRID THREATS

***Анотація.*** *У статті розкрито функціональне значення інформаційної культури у системі фахової підготовки майбутніх бакалаврів бібліотечної, інформаційної та архівної справи в умовах гібридних загроз. На основі структурно-функціонального та порівняльного аналізу досліджено сукупність національних стратегій та стандартів інформаційної кібербезпеки. Розкрито ефективність включення регламентуючих безпекових*

*настанов, основ кібергігієни у навчальні матеріали для формування здатності здобувачів освіти розпізнавати когнітивні маніпуляції та інформаційну експансію. Особливу увагу приділено інтерактивним методам навчання, спрямованим на формування інформаційної культури здобувачів освіти. Фахівець, здатний розпізнавати інформаційні загрози та протидіяти їм, відповідає актуальним запитам бібліотечних та архівних установ як стратегічних суб'єктів національної пам'яті.*

***Ключові слова:*** *інформаційна культура, гібридна загроза, здобувач освіти, архівні установи, освітній компонент, освітній процес, кібербезпека.*

***Summary.*** *The article reveals the functional role of information culture within the professional training system of future Bachelors in Information, Library and Archival Studies under hybrid threats. Based on structural-functional and comparative analyses, a complex of national strategies as well as information and cybersecurity standards is investigated. The study demonstrates the effectiveness of incorporating regulatory security guidelines and core elements of cyber hygiene into educational components to develop students' capacity to recognize cognitive manipulations and information expansion. Special attention is paid to interactive teaching methods aimed at shaping the information culture of higher education students. A specialist capable of identifying and counteracting information threats meets the current demands of libraries and archives as strategic entities of national memory.*

***Key words:*** *information culture, hybrid threat, higher education student, archival institutions, educational component, educational process, cybersecurity.*

**Постановка проблеми.** У сучасному суспільстві інформація посилює конкурентну боротьбу за сфери впливу між суб'єктами економічних,

політичних відносин, як на регіональному, так і міжнародному рівнях. Цифрові технології стають потужним інструментом маніпуляцій у суперництві підприємств, фінансових організацій, корпорацій, політичних партій, держав. Система освіти має оперативно реагувати на нові соціальні виклики, тому що наша країна перебуває під тиском інформаційних атак, які прагнуть підсилити воєнну інтервенцію. Важливим виміром цієї проблеми є стрімкий розвиток інформаційно-комунікаційних технологій, що підвищує рівень потенційних загроз та небезпек.

У останні роки відбулось переоцінювання проблем кібербезпеки та інформаційної грамотності державному рівні, що в подальшому вплинуло на змістовне наповнення навчального матеріалу освітніх компонентів, переорієнтувало тематику модулів на формування у здобувачів критичного мислення, здатності розпізнавати фейки під час проведення лекційних та практичних занять з інформаційної культури. Здобувачі освіти активно споживають цифровий контент, але поява принципово нових безпекових викликів та штучних тригерів вимагає від системи освіти їх ретельного аналізу для впровадження відповідних змістових блоків для викладання, щоб озброїти майбутніх фахівців інструментами захисту та протидії інформаційним викликам. Захист від дезінформації стає пріоритетним умінням за ступенем важливості, оскільки в обставинах сьогодення інформаційна культура молоді є гарантом збереження культурної спадщини, національної ідентичності.

**Аналіз останніх досліджень і публікацій.** Проблема формування інформаційної культури майбутніх бакалаврів бібліотечної, інформаційної та архівної справи в умовах гібридних загроз перебуває на стику двох наукових напрямів, фахової підготовки здобувачів освіти та державної безпеки. Теоретичні основи дослідження національної безпеки детально проаналізовано в працях О. Данільяна, О. Дзьобаня та М. Панова.

Європейський контекст та особливості реалізації національної інформаційної політики висвітлено у колективній монографії за редакцією Л. Губерського, Є. Камінського, Є. Макаренка. Водночас соціальний аспект кібербезпеки для розуміння ролі людського фактора в умовах гібридних загроз досліджено в розвідках В. Бурячка, В. Толубка, В. Хорошка, С. Толюпи. Концептуальним підґрунтям для визначення безпекових вимог до підготовки кадрів є чинна нормативна база України. Пріоритети захисту національних інтересів в інформаційній сфері та протидії маніпуляціям окреслені у Стратегії інформаційної безпеки та Стратегії кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни», в якій також висвітлено орієнтири розбудови захищеного віртуального простору. Окреме місце у формування професійних компетентностей посідають національні стандарти побудови систем керування інформаційною безпекою: ДСТУ ISO/IEC 27001:2023, ДСТУ ISO/IEC 27005:2023, ДСТУ ISO/IEC 27701:2022.

Проблемам адаптації системи освіти до викликів цифрового суспільства, трансформації професійного профілю інформаційного працівника присвячено наукові розвідки О. Матвієнко та М. Цивіна [1]. Особливості формування цифрової компетентності у здобувачів освіти бібліотечної, інформаційної та архівної справи розкрито у статті О. Мудрохи [2]. Загальні принципи та інструменти інтеграції цифрових технологій в освітній процес узагальнено О. Сахно [3]. Попри значну кількість публікацій, питання формування інформаційної культури майбутніх фахівців в умовах гібридних загроз залишається актуальним та потребує подальшого комплексного дослідження.

**Мета статті** полягає в теоретико-методологічному обґрунтуванні ключових аспектів та принципів формування інформаційної культури у здобувачів освіти як основи протидії дезінформації в умовах гібридних загроз.

Для реалізації мети в ході дослідження було застосовано метод структурно-функціонального аналізу для деталізації трансформації викладання змістових модулів з інформаційної культури; компаративний аналіз та систематизація нормативно-правових актів, стратегій кібербезпеки та останніх наукових розвідок за тематикою статті сприяли зіставленню моделей державної інформаційної політики в Україні та міжнародного досвіду. Інституційний та системний підходи стали підґрунтям розроблення методичних засад вдосконалення інформаційної грамотності здобувачів освіти.

**Виклад основного матеріалу дослідження.** В умовах розбудови цифрового суспільства інформація змінюється на визначальний чинник більшості соціальних, політичних та економічних процесів, що призводить до масштабування концепту інформаційної війни як несилового інструментарію досягнення поставлених завдань. Пришвидшений розвиток технологій суттєво збільшує аудиторію споживачів цифрового контенту, експоненційно посилює потужність ресурсів деструктивного впливу, мета якого полягає у когнітивній дезорієнтації та спрямована на маніпулювання громадською думкою, що актуалізує потребу в підготовці фахівців бібліотечної, інформаційної та архівної справи. Їх майбутня професійна діяльність буде пов'язана зі стратегічним управлянням інформаційними потоками, формуванням цифрової грамотності користувачів бібліотек та архівів, перевіркою документних джерел на валідність, пошуком фальсифікацій.

У науковому дискурсі інформаційну війну розглянуто як процес використання інформації та управління нею задля набуття переваг над конкурентом, як засіб ідеологічного та психологічного тиску, легітимізації та обґрунтуванні справедливості власних через обмеження прав опонента [4]. В широкому розумінні інформаційна війна – це протистояння з активним

залученням цифрових технологій, дослідження якого є критично важливим для здобувачів освіти, оскільки їх професійні обов'язки будуть безпосередньо пов'язані з адмініструванням, захистом та збереженням електронних документів. Оскільки віртуальний простір стає головним майданчиком розгортання маніпулятивних кампаній, навчальні матеріали курсу «Інформаційна культура» мають включати методи аналізу медіапотоків, основи кібергігієни у межах організаційних та соціальних комунікацій.

Інформація є фундаментальним атрибутом управління, її використання в межах інформаційно-комунікаційної діяльності простежується на всіх етапах історичного поступу людства. Проте, якщо в попередні епохи інформаційне протистояння редукувалося до конспірації власних даних та розвідувальної діяльності з її викриття, то сучасність вирізняється протистоянням різних технологій, «які використовуються для широкомасштабного, цілеспрямованого, швидкого і прихованого впливу на військові і цивільні інформаційні системи противника» [5, с. 90].

В умовах активної фази воєнного конфлікту в нашій країні здобувачам освіти варто пояснювати, що зіткнення в інформаційному просторі спостерігаються також в економічній сфері, для формування об'єктивного бачення глобального інформаційного суспільства. Методи виробників товарів та послуг вплинути на смаки та уподобання потенційних споживачів також належать до маніпулятивних, пошук та посилення позицій на нових ринках збуту, зміцнення національних економік за рахунок непрямих інвестицій, це також засоби протистояння на рівні корпорацій та держав. В інформаційній боротьбі держав, так само як корпорацій, інноваційним різновидом зброї вважають різноманітні комп'ютерні віруси та несанкціоновані вторгнення, що несуть пряму загрозу цілісності електронних архівів та баз даних.

Актуальною темою для вивчення та обговорення здобувачами спеціальності бібліотечна, інформаційна та архівна справа є інформаційна експансія, пролонгована в часі, цілі та методи якої передбачають варіативність та комплексність, можливість залучення зовнішніх ресурсів та союзників. Інформаційна експансія окреслюється прагненням домінувати в інформаційному просторі, на державному та локальному рівнях. Зазначена тактика передбачає активну роботу зі створення іміджу успіху, легітимності, дотримання норм моралі та гуманних цінностей. Зворотний бік такої діяльності полягає у побіжному нівелюванні опозиційної точки зору, дискредитації супротивників або конкурентів. Справжньою ареною інформаційних протистоянь є соціально-психологічна сфера, яку складно прогнозувати. Тому подання достовірної інформації на противагу фейкам та дезінформації буде недостатньо. Для протидії інформаційній експансії на рівні держави розробляються нормативно-правові документи, стратегії та стандарти інформаційної безпеки, вивченню яких необхідно приділити окремий змістовий модуль.

Система протидії гібридним загрозам та інформаційній експансії в нашій країні спирається на Закон України «Про національну безпеку України», Стратегію інформаційної безпеки та Стратегію кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни», прийняті в 2021 році. У Стратегії інформаційної безпеки пріоритетним визначено забезпечення конституційних прав і свобод кожного громадянина «на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації» [6], також констатується на відповідальності держави щодо забезпечення захисту в цифровому просторі, «існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване

поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом» [6].

У Стратегії кібербезпеки України акцентується увага на захисті критичної інформаційної інфраструктури, безпеці цифрових реєстрів та мінімізації ризиків втручання в комп'ютерні мережі [7]. Оскільки архіви та бібліотеки інтегровані у цифровий простір, захист хмарових сховищ та електронного документообігу покладається в тому числі на працівників зазначених установ, тому процес формування кібергігієни у здобувачів освіти має бути невід'ємним складником під час вивчення майже всіх дисциплін. Здобувачам освіти необхідно набути навичок розпізнавання кіберзагроз, спричинених комп'ютерними вірусами та хакерськими атаками, вміти адмініструвати бази даних, забезпечувати цілісність електронних документів.

У контексті протидії гібридним загрозам та задля реалізації Стратегії інформаційної безпеки та Стратегії кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни» до аналізу на лекційних заняттях рекомендовано три взаємопов'язані стандарти, які формують базис для інформаційних установ: ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги; ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки; ДСТУ ISO/IEC 27701:2022 (ISO/IEC 27701:2019, IDT) Методи безпеки. Розширення до ISO/IEC 27001 та ISO/IEC 27002 для керування конфіденційною інформацією. Вимоги та настанови.

Стандарт ДСТУ ISO/IEC 27001:2023 є генеральною методологічною рамкою, що забезпечує тріаду інформаційної безпеки, а саме,

конфіденційність, цілісність та доступність цифрових реєстрів, баз даних та електронного документообігу, гармонізований з міжнародними вимогами та враховує динаміку кіберзагроз [8]. ДСТУ ISO/IEC 27005:2023 обґрунтовує інструменти ідентифікації, оцінювання та мінімізації ризиків втручання в цифрові мережі та хмарні сховища, що дає змогу моделювати загрози та прогнозувати їх наслідки [9]. ДСТУ ISO/IEC 27701:2022 регулює недопущення витоків масивів даних, що є критично важливим при оцифруванні документів, містить вимоги щодо захисту персональних даних [10].

Для здобувачів освіти спеціальності бібліотечна, інформаційна та архівна справа важливим результатом вивчення проблематики інформаційного протистояння має бути розуміння того, як захистити інформаційні ресурси; яким чином дезінформація впливає на професійну сферу; як здійснюється планомірний тиск на свідомість; як відбувається зміна тактики, від раптових фейків до планомірного приховування новин. Навички протидії маніпуляціям, адекватна реакція на загрози формуються на практичних заняттях для закріплення теоретичного матеріалу. Наприклад, аналіз реальних фейків, що транслюються через новини та соціальні мережі, дослідження випадків створення штучного інформаційного хаосу, або на лабораторних заняттях здобувачі обирають роль детективів та шукають ферми ботів, перевіряють приховані дані. Під час проведення круглих столів тестуються ділові ігри-маніпуляції, що викликають сильні емоції, страх, злість, радість, а потім у групі обговорюються засоби протидії таким інформаційним атакам. Здобувачам освіти також пропонується створити власні короткі курси чи пам'ятки з інформаційної безпеки для бібліотек або архівів.

Дієвим інструментом протидії інформаційним впливам, на думку вітчизняних дослідників, визначено освіту та самоосвіту, просвітницьку діяльність та активну громадянську позицію, а саме: «захистити себе людина

може тільки шляхом використання системи внутрішньоособистісних фільтрів – зрілої організаційної свідомості, відповідної політичної культури, й, нарешті, зверненням до позитивного суспільного ідеалу особистості XXI століття, справедливої європейської держави і ефективного суспільства» [11, с. 60].

Вектором деструктивного інформаційного впливу та гібридних загроз є залучення медійних, художніх, культурних, економічних, соціальних, освітянських та наукових, політичних, кібернетичних інструментів, що дестабілізують суспільство, провокують радикальні або панічні настрої, ускладнюють роботу органів державної та місцевої влади. Для протидії гібридним загрозам необхідно «забезпечувати належний захист інформації; попереджувати введення викривленої інформації в потоці правдивих фактів і даних; протидіяти спростуванню, запереченню і знищенню інформації і вчасно та якісно реагувати на всі прояви війни» [2, с. 23]. Здобувачів освіти спеціальності бібліотечна, інформаційна та архівна справа мають усвідомлювати, що оцифровані фонди, державні реєстри та бази даних, які вони будуть адмініструвати, є об'єктами кібератак та спроб фальсифікації документів.

**Висновки та перспективи подальших досліджень.** Формування інформаційної культури – невід'ємний складник освітнього процесу, змістове наповнення методичного забезпечення фахових освітніх компонентів таких як архівознавство та документознавство, електронний документообіг та інформаційна культура. Бібліотечні та архівні установи як стратегічні суб'єкти національної пам'яті, потребують професіоналів здатних впроваджувати передові стандарти захисту інформаційних ресурсів.

Засоби розвитку та удосконалення інформаційної культури спираються на зміни в освітньому процесі фахової підготовки здобувачів спеціальності бібліотечна, інформаційна та архівна справа. Оптимізація моделі навчання має

поєднувати викладання основ кібергігієни, безпеки баз даних із дотриманням жорстких вимог відповідних стандартів. Регламентуючі акти не лише окреслюють методи захисту цифрового простору держави, але й актуалізують проблему модернізації системи освіти щодо розвитку інформаційної грамотності майбутніх фахівців, забезпечення стійкості перед гібридними загрозами інформаційно-комунікаційних технологій та цифрового суспільства. Бібліотечні та архівні установи перетворились на важливі суб'єкти захисту інформаційного суверенітету країни. В освітньому процесі переваги мають віддаватись формуванню компетентностей з верифікації документних джерел, критичного аналізу інформаційного шуму та просвітництва щодо безпеки віртуального простору.

**Література**

1. Матвієнко, О., Цивін, М. «Цифрові» професії інформаційного фахівця: освітні перспективи і вимоги ринку праці. *Український журнал з бібліотекознавства та інформаційних наук.* 2021. № 7. С. 58-70.

2. Мудроха В. О. Особливості формування цифрової компетентності здобувачів вищої освіти спеціальності 029 «Інформаційна, бібліотечна та архівна справа». *Бібліотекознавство. Документознавство. Інформологія*. 2023. № 2. С. 109-114.

3. Сахно О. В. Цифрова компетентність і технології для освіти: принципи та інструменти. *Імідж сучасного педагога.* 2023. № 6(195). С. 10-14.

4. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В.Л. Бурячок, В.Б.Толубко, В.О. Хорошко, С.В.Толюпа]; за заг. ред. д-ра техн. наук, В.Б. Толубка. Київ, 2015. 288 с.

5. Данільян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: сутність, структура та напрямки реалізації. Харків, 2002. 296 с.

6. Стратегія інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069# (дата звернення: 12.03.2026).

7. Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни»: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 13.03.2026).

8. ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги [Чинний від 2023-08-22]. Вид. офіц. Київ: ДП «УкрНДНЦ», 2023. 26 с.

9. ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки [Чинний від 2023-08-28]. Вид. офіц. Київ: ДП «УкрНДНЦ», 2023. 70 с.

10. ДСТУ ISO/IEC 27701:2022 (ISO/IEC 27701:2019, IDT) Методи безпеки. Розширення до ISO/IEC 27001 та ISO/IEC 27002 для керування конфіденційною інформацією. Вимоги та настанови. [Чинний від 2023-01-01]. Вид. офіц. Київ: ДП «УкрНДНЦ», 2022. 75 с.

11. Інформаційна політика України: європейський контекст: моногр. / Л. В. Губерський, Є. Є. Камінський, Є. А. Макаренко та ін. Київ, 2007. 360 с.

## References

1. Matviienko, O., & Tsyvin, M. (2021). «Tsyfrovi» profesii informatsiinoho fakhivtsia: osvitni perspektyvy i vymohy rynku pratsi [«Digital» professions of an information specialist: educational prospects and labor market requirements].

*Ukrainskyi zhurnal z bibliotekoznavstva ta informatsiinykh nauk – Ukrainian Journal on Library and Information Science*, 7, 58-70 [in Ukrainian].

2. Mudrokha, V.O. (2023). Osoblyvosti formuvannia tsyfrovoi kompetentnosti zdobuvachiv vyshchoi osvity spetsialnosti 029 «Informatsiina, bibliotechna ta arkhivna sprava» [Features of digital competence formation of higher education applicants in specialty 029 «Information, library and archival studies»]. *Bibliotekoznavstvo. Dokumentoznavstvo. Informolohiia – Library Science. Record Studies. Informology*, 2, 109-114 [in Ukrainian].

3. Sakhno, O.V. (2023). Tsyfrova kompetentnist i tekhnolohii dlia osvity: pryntsypy ta instrumenty [Digital competence and technologies for education: principles and tools]. *Imidzh suchasnoho pedahoha – Image of the Modern Pedagogue*, 6(195), 10-14 [in Ukrainian].

4. Buriachok, V.L., Tolubko, V.B., Khoroshko, V.O., & Toliupa, S.V. (2015). *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt* [Information and cybersecurity: socio-technical aspect]. V.B. Tolubko (Ed.). Kyiv [in Ukrainian].

5. Danilyan, O.H., Dzioban, O.P., & Panov, M.I. (2002). *Natsionalna bezpeka Ukrainy: sutnist, struktura ta napriamky realizatsii* [National security of Ukraine: essence, structure and directions of implementation]. Kharkiv [in Ukrainian].

6. *Stratehiia informatsiinoi bezpeky* [Information security strategy]. (2021). Decree of the President of Ukraine № 685/2021. Retrieved from https://www.president.gov.ua/documents/6852021-41069# [in Ukrainian].

7. *Stratehiia kiberbezpeky Ukrainy «Bezpechnyi kiberprostir – zaporuka uspishnoho rozvytku krainy»* [Cybersecurity strategy of Ukraine «Safe cyber space – the key to successful development of the country»]. (2021). Decree of the President of Ukraine № 447/2021. Retrieved from https://www.president.gov.ua/documents/4472021-40013 [in Ukrainian].

8. *Informatsiina bezpeka, kiberbezpeka ta zakhyst konfidentsiinoi informatsii. Systemy keruvannia informatsiinoiu bezpekoiu. Vymohy* [Information security, cybersecurity and privacy protection. Information security management systems. Requirements]. (2023). DSTU ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT). Kyiv: DP «UkrNDNTS» [in Ukrainian].

9. *Informatsiina bezpeka, kiberbezpeka ta zakhyst konfidentsiinoi informatsii. Nastanova keruvannia ryzykamy informatsiinoi bezpeky* [Information security, cybersecurity and privacy protection. Guidance on information security risk management]. (2023). DSTU ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT). Kyiv: DP «UkrNDNTS» [in Ukrainian].

10. *Metody bezpeky. Rozshyrennia do ISO/IEC 27001 ta ISO/IEC 27002 dlia keruvannia konfidentsiinoiu informatsiieiu. Vymohy ta nastanovy* [Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines]. (2022). DSTU ISO/IEC 27701:2022 (ISO/IEC 27701:2019, IDT). Kyiv: DP «UkrNDNTS» [in Ukrainian].

11. Huberskyi, L.V., Kaminskyi, Ye.Ye., Makarenko, Ye.A., et al. (2007). *Informatsiina polityka Ukrainy: yevropeiskyi kontekst* [Information policy of Ukraine: European context]. Kyiv [in Ukrainian].