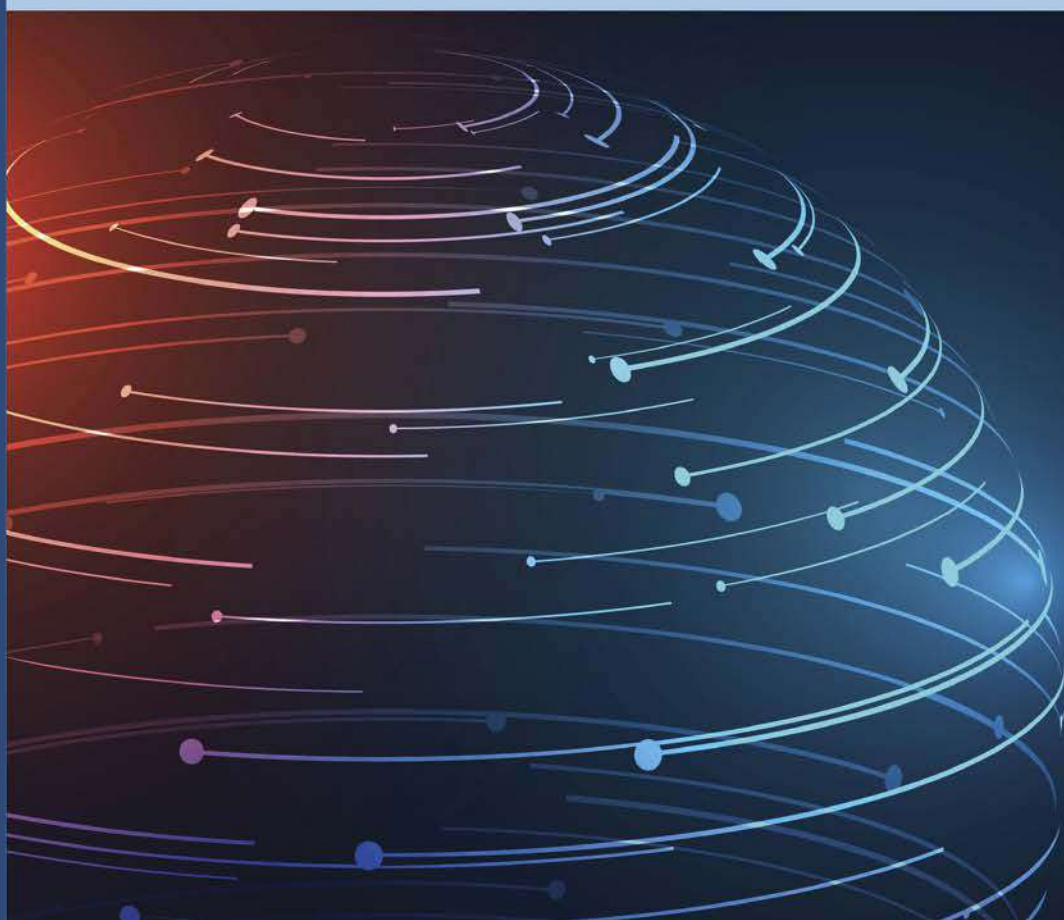


Відкрита наука та інновації

Open science
and innovation



#2 2025

Відкрита наука та інновації

Open science
and innovation

ВІДКРИТА НАУКА
ТА ІННОВАЦІЇ
№ 2, 2025

Науковий електронний
рецензований журнал
відкритого доступу

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ISSN 3041-1416 (Online)

УДК 001+001.895

Засновник: ДЕРЖАВНА
НАУКОВО-ТЕХНІЧНА
БІБЛІОТЕКА УКРАЇНИ
(ДНТБ УКРАЇНИ)

Адреса: вул.
Антоновича, 180,
м. Київ, 03150

тел. +380 (44) 521-93-50

e-mail: dntb@dntb.gov.ua

e-mail журналу:
<https://journal.dntb.gov.ua>

Мови видання:
українська, англійська.

Періодичність:
2 рази на рік

Внесено до реєстру
Національної ради України
з питань телебачення і
радіомовлення
31.08.2023 р.
Ідентифікатор медіа
R 40-01252

Підписано до друку:
05.11.2025 р.

Зображення на обкладинці:
Freepik.com



РЕДАКЦІЙНА КОЛЕГІЯ

Головний редактор:

Жарінова Алла Георгіївна

доктор економічних наук, доцент,
в. о. директора Державної науково-технічної бібліотеки України, Україна

Аврамчук Богдан Олегович

кандидат економічних наук,
заступник директора з науково-експертної діяльності Державної наукової установи «Український
інститут науково-технічної експертизи та інформації», Україна

Альперін Дж. П.

професор кафедри видавничої справи, співдиректор ScholCommLab
та науковий керівник Проєкту громадських знань (PKP)
в Університеті Саймона Фрейзера, Канада

Березко Олександр Леонідович

кандидат технічних наук, доцент,
Національний університет «Львівська політехніка», Україна

Главчева Юлія Миколаївна

доктор філософії за спеціальністю «Комп'ютерні науки»,
директор науково-технічної бібліотеки Національний технічний університет
«Харківський політехнічний інститут», Україна

Гранчак Тетяна Юріївна

доктор наук із соціальних комунікацій, Університет Сіракуз,
Університет Бінгемтона, США

Женченко Марина Іванівна

доктор наук з соціальних комунікацій,
професор, директор Наукової бібліотеки імені Максимовича,
Київський національний університет імені Тараса Шевченка, Україна

Кучма Ірина

координатор програм з відкритого доступу EIFL, Вільнюс, Литва

Лопатовська Ірена

PhD з інформаційних наук,
професор Школи інформації Інституту Пратт, США

Мар'їна Олена Юріївна

доктор наук із соціальних комунікацій, професор,
завідувачка кафедри цифрових комунікацій та інформаційних технологій,
Харківська державна академія культури, Україна

Ольшєвська Ольга Володимирівна

кандидат технічних наук, доцент,
проректор з наукової роботи та міжнародних зв'язків,
Одеський технологічний університет, Україна

Плавчан Петер

професор,
ректор Дунайського університету в Сладковичово, Словацька Республіка

Ребілас Рафал

PhD,
проректор з міжнародних зв'язків,
Університет WSB (Академія WSB), Домброва Гурнича, Польща

Сербін Олег Олегович

доктор наук з соціальних комунікацій,
директор Національної бібліотеки України імені Ярослава Мудрого, Україна

Субаверапандіян А.

Університет Беннетт, Велика Нойда, Уттар-Прадеш, Індія

Цибенко Ірина Олегівна

кандидат економічних наук,
заступник директора з науково-аналітичної роботи
Державної науково-технічної бібліотеки України, Україна

Ярошенко Тетяна Олександрівна

кандидат історичних наук, доцент,
заслужений працівник культури України, заступник директора ДНТБ України
з наукової роботи та міжнародного співробітництва, Україна

Відповідальний секретар:

Жеребчук Софія Валентинівна

завідувач відділу європейської інтеграції та міжнародного співробітництва,
Державна науково-технічна бібліотеки України, Україна

ЗМІСТ

**Дьогтева Ірина, Красовський Олексій,
Рибалко Ярослав**

Роль національної електронної науково-інформаційної системи в оцінці забезпечення національними контактними пунктами обізнаності українських суб'єктів щодо рамкової програми ЄС з досліджень та інновацій 4

Рачинська Олена

Контент-аналіз політик відкритого доступу та відкритої науки в університетах та наукових установах України 19

**Шаповалов Євгеній, Шаповалов Віктор,
Рудакова Тетяна, Рибалко Ярослав,
Василенко Андрій**

Цифровізація документообігу в науковій сфері діяльності: практичні аспекти на прикладі системи «Наука» *(англ. мова)* 33

Жорняк Андрій

Кібербезпека державних цифрових систем: пентестинг хмарних середовищ 46

Грищенко Людмила, Кипоренко Віктор

Вдосконалення державних стандартів України у сфері науково-технічної інформації: шлях до гармонізації з міжнародними та європейськими нормами 63

Баланчук Ірина, Ігнацевич Сергій

Наукометричний аналіз проблем зміни клімату: приклад України *(англ. мова)* 75

Жарінова Алла

Цифрова трансформація науки (рецензія на книгу) 90

CONTENTS

**Dohtieva Iryna, Krasovskyi Oleksii
Rybalko Yaroslav**

The role of the national electronic scientific information system in assessment of provision by national contact points information about the EU framework programme research and innovation to ukrainian entities *(Ukrainian)* 4

Rachynska Olena

Content analysis of open access and open science policies in universities and research institutions of Ukraine *(Ukrainian)* 19

**Shapovalov Yevhen, Shapovalov Viktor,
Rudakova Tetiana, Rybalko Yaroslav,
Vasylenko Andrii**

Digitization of document flow in the scientific field: practical aspects based on the example of the "Nauka" system 33

Zhorniak Andrii

Cybersecurity of government digital systems: pentesting of cloud environments *(Ukrainian)* 46

Hryshchenko Lyudmila, Kiporenko Viktor

Improvement of state standards of Ukraine in the field of scientific and technical information: the path to harmonization with international and european norms *(Ukrainian)* 63

Balanchuk Iryna, Ihnatsevych Sergiy

The potential of scientometric analysis for studying climate change issues: a case study of Ukraine 75

Zharynova Alla

Digital Transformation of Science (Review of the book) *(Ukrainian)* 90

РОЛЬ НАЦІОНАЛЬНОЇ ЕЛЕКТРОННОЇ НАУКОВО-ІНФОРМАЦІЙНОЇ СИСТЕМИ В ОЦІНЦІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНИМИ КОНТАКТНИМИ ПУНКТАМИ ОБІЗНАНОСТІ УКРАЇНСЬКИХ СУБ'ЄКТІВ ЩОДО РАМКОВОЇ ПРОГРАМИ ЄС З ДОСЛІДЖЕНЬ ТА ІННОВАЦІЙ

Ірина Дьогтева,

Державна науково-технічна бібліотека України

Олексій Красовський,

Державна науково-технічна бібліотека України

Ярослав Рибалко,

Державна науково-технічна бібліотека України

Анотація. Мета дослідження — визначити роль Національної електронної науково-інформаційної системи (Система NAUKA) в аналізі ефективності діяльності національних контактних пунктів (НКП) Рамкової програми Європейського Союзу з досліджень та інновацій «Горизонт Європа» та Програми з досліджень та навчання Європейського співтовариства з атомної енергії (2021–2025), комплементарної до неї, пов'язаних з організацією, проведенням, участю в заходах та регулярністю наповнення (оновлення) інформаційних ресурсів (ІР).

Дослідження передбачало вивчення нормативно-правових актів щодо діяльності НКП та пов'язаного фінансового забезпечення з використанням загальнонаукових (емпіричних) та загальнологічних методів. Аналіз даних щодо організації, проведення, участі в заходах представників НКП, забезпечення інформаційної підтримки їх діяльності проводився з використанням статистичних методів, доповнених візуалізацією, на основі звітних матеріалів НКП. Подання звітів забезпечувалося в тестовому режимі в Системі NAUKA в межах розробленого модуля звітності НКП, для дослідження якого застосовано інформаційний та функціональний аналіз (моделювання).

За результатами дослідження сформовано пропозиції до ключових показників ефективності (KPI) діяльності НКП, індикаторів їх виконання, модуля звітності НКП. У межах KPI пропонується уточнити формулювання, структурувати та доповнити додаткову інформацію, яка має включити узгоджену та деталізовану інформацію щодо даних, які необхідно подати, умов, за яких вони будуть зараховані. Пропозиції щодо індикаторів виконання KPI на майбутні періоди стосуються кількісних та якісних змін за результатами звітування та зібраної інформації про звітний період. У модулі звітності НКП запропоновано: збільшити обсяг даних для збору, розширити варіанти вибору з долученням відкритого варіанта, уможливити його множинність, розмежувати види завантажених матеріалів, забезпечити їх зв'язок із окремим записом щодо заходу, наповнення (оновлення) ІР, імпортувати дані з інших функціональних модулів системи NAUKA, зокрема Національного порталу міжнародного науково-технічного співробітництва, можливо, зовнішніх ІС, упровадити погодження достатності матеріалів підтвердження, провести функціональні зміни розрахунку KPI, адаптувати способи оцінки виконання KPI, включити рейтингову складову.

Ключові слова: бюджетне фінансування; Горизонт Європа; Євратом; ключовий показник ефективності; Національна електронна науково-інформаційна система; національний контактний пункт.

ВСТУП

Відповідно до умов, викладених в Угоді про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (2014, Протокол III), Україна може брати участь у програмах ЄС, які є відкритими для участі. Наймасштабнішою серед таких програм є Рамкова програма ЄС з досліджень та інновацій «Горизонт Європа» (Програма «Горизонт Європа») та комплементарна до неї програма з досліджень та навчання «Євратом» (Програма «Євратом»), у яких Україна бере участь як асоційована країна («Угода між Україною, з однієї сторони, і Європейським Союзом та Європейським співтовариством з атомної енергії, з іншої сторони, про участь України у Рамковій програмі з досліджень та інновацій “Горизонт Європа” та Програмі з досліджень та навчання Європейського співтовариства з атомної енергії (2021–2025), комплементарній до Рамкової програми з досліджень та інновацій “Горизонт Європа”», 2021, абз. 1 п. 1 ст. 1). Така участь передбачає отримання фінансування на рівних умовах з країнами-членами ЄС.

Щорічний фінансовий внесок до кожної з Програм включає суму членського внеску, який для України не є фіксованим і розраховується з урахуванням величини ВВП, та операційного — сплачується за участь у кожній із Програм «Горизонт Європа» та «Євратом» («Угода між Україною, з однієї сторони, і Європейським Союзом та Європейським співтовариством з атомної енергії, з іншої сторони, про участь України у Рамковій програмі з досліджень та інновацій “Горизонт Європа” та Програмі з досліджень та навчання Європейського співтовариства з атомної енергії (2021–2025), комплементарній до Рамкової програми з досліджень та інновацій “Горизонт Європа”», 2021, абз. 1 п. 1 ст. 3). Однак на прохання України в Угоді (у формі обміну листами) між Україною та Європейським Союзом щодо зупинення зобов'язань України щодо сплати фінансових внесків у зв'язку з

угодами про приєднання до програм Союзу (2023), яка ратифікована 05.12.2024, зупинено дію зобов'язань щодо сплати фінансового внеску за участь у всіх програмах ЄС.

За попередньою Рамковою програмою ЄС з наукових досліджень та інновацій «Горизонт 2020» ефективність виконання зобов'язань України у сфері міжнародного науково-технічного співробітництва визначалася шляхом порівняння коштів державного бюджету, використаних на реалізацію такого співробітництва, із грантами, фактично отриманими українськими суб'єктами. Нині отримані гранти є додатково залученим фінансовим забезпеченням наукової і науково-технічної, інноваційної діяльності, а визначення ефективності включає розгляд інших напрямів використання бюджетних коштів, відмінних від сплати фінансових внесків.

У затвердженому Міністерством освіти і науки України (МОН) паспорті бюджетної програми на 2025 рік за КПКВК 2201380 зазначені напрями пов'язані з фінансовою підтримкою «заходів, спрямованих на проведення інформаційно-комунікаційних компаній, забезпечення навчання та підвищення обізнаності українських учасників щодо міжнародного науково-технічного співробітництва, зокрема інструментів ЄС з питань підтримки досліджень та інновацій» зі спеціальним фондом 16 027,5 тис. гривень та участю «представників України та українських експертів у заходах, організованих в рамках інструментів ЄС з питань досліджень та інновацій» зі спеціальним фондом 7 608,7 тис. гривень («Про затвердження паспорта бюджетної програми на 2025 рік за КПКВК 2201380», 2025). Крім фінансової підтримки заходів перший напрям включає фінансування національних контактних пунктів (НКП) Програм «Горизонт Європа» та «Євратом», створених на базі закладів вищої освіти (ЗВО), наукових установ (НУ) та державних установ (ДУ) («Про затвердження плану заходів з реалізації міжнародних наукових та науково-технічних програм і проєктів відповідно до міжнародних договорів України на 2025 рік за бюджетною програмою за КПКВК

2201380 «Виконання зобов'язань України у сфері міжнародного науково-технічного та освітнього співробітництва, участь у рамковій програмі Європейського Союзу з досліджень та інновацій»», 2025). Розподіл коштів у 2025 році передбачений для фінансування 22 НКП за 17 напрямками діяльності, які створені на базі 15 ЗВО, 2 НУ, 2 ДУ та заповідника («Про фінансування у 2025 році національних контактних пунктів Рамкової програми Європейського Союзу з досліджень та інновацій “Горизонт Європа” та Програми з досліджень та навчання Європейського співтовариства з атомної енергії (2021–2025), комплементарної до програми “Горизонт Європа”», 2025).

Мета та завдання дослідження. Мета дослідження полягає у визначенні ролі Національної електронної науково-інформаційної системи в аналізі ефективності діяльності національних контактних пунктів Рамкової програми Європейського Союзу з досліджень та інновацій «Горизонт Європа» та Програми з досліджень та навчання Європейського співтовариства з атомної енергії (2021–2025), комплементарної до неї, пов'язаних з організацією, проведенням та участю в заходах, регулярністю наповнення (оновлення) інформаційних ресурсів.

Перелік завдань включає:

- аналіз нормативно-правових актів щодо діяльності НКП та пов'язаного фінансового забезпечення;
- аналіз даних щодо організації, проведення та участі у заходах представників НКП, забезпечення інформаційної підтримки з використанням інформаційних ресурсів (ІР), отриманих з модуля звітності НКП, за результатами звітування керівників НКП в тестовому режимі в Національній електронній науково-інформаційній системі (Система НАУКА);
- формування пропозицій до ключових показників ефективності (KPI), збору даних, пов'язаних із заходами, наповненням (оновленням) ІР, розрахунку відповідних KPI в Системі НАУКА, встановлення індикаторів виконання KPI.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

Вивчення та аналіз нормативно-правових актів проводилися з використанням загальнонаукових (емпіричних) та загальнологічних методів. Для дослідження модуля звітності НКП в частині заповнення даних, пов'язаних із заходами, наповненням (оновленням) ІР, та формування відповідних KPI застосовано інформаційний та функціональний аналіз (моделювання). Під час аналізу даних щодо організації, проведення та участі в заходах представників НКП, регулярності наповнення (оновлення) ІР за результатами звітування керівників НКП використовувалися статистичні методи, доповнені візуалізацією даних.

РЕЗУЛЬТАТИ ТА ЇХ ОБГОВОРЕННЯ

Відповідно до Положення про НКП та Координаційний центр Програм «Горизонт Європа» та «Євратом» («Про затвердження Положення про національні контактні пункти та Координаційний центр Рамкової програми Європейського Союзу з досліджень та інновацій “Горизонт Європа” та Програми з досліджень та навчання Європейського співтовариства з атомної енергії (2021–2025), комплементарної до програми “Горизонт Європа”», 2024) функціонування НКП реалізується шляхом покладення функцій щодо підтримки та супроводження відповідних програм на окрему посадову особу ЗВО, НУ, іншої юридичної особи незалежно від форми власності або громадської наукової організації, яка має статус юридичної особи. Перелік формується за результатами конкурсного відбору за напрямом діяльності та у сфері наукової, науково-технічної та інноваційної діяльності й затверджується наказом МОН, наприклад, оновлений перелік 2025 року («Про внесення змін до переліку національних контактних пунктів Рамкової програми Європейського Союзу з досліджень та інновацій “Горизонт Європа” та Програми з досліджень та навчання Європейського співтовариства з атомної енергії (2021–2025), комплементарної до програми “Горизонт Європа”», 2025).

Серед основних завдань НКП, які стосуються зазначених вище напрямів використання бюджетних коштів, у паспорті бюджетної програми на 2025 рік за КПКВК 2201380, виділяють («Про затвердження Положення про національні контактні пункти та Координаційний центр Рамкової програми Європейського Союзу з досліджень та інновацій “Горизонт Європа” та Програми з досліджень та навчання Європейського співтовариства з атомної енергії (2021–2025), комплементарної до програми “Горизонт Європа”», 2024, п. 5):

- інформування суб'єктів наукової, науково-технічної та інноваційної діяльності щодо програм ЄС, конкурсів, умов участі та подання проєктних пропозицій;
- підвищення рівня обізнаності громадськості, малих та середніх підприємств (МСП) про можливості Програми «Горизонт Європа» та Програми «Євратом»;
- організацію та проведення інформаційних днів, навчальних семінарів для відповідних цільових груп за актуальними тематичними напрямками Програми «Горизонт Європа» та комплементарних до неї програм;
- забезпечення інформаційної підтримки діяльності НКП;
- поширення інформаційно-аналітичних матеріалів (інформації про умови участі, подання проєктних пропозицій, формування бюджету проєкту, звітування).

До функцій включені («Про затвердження Положення про національні контактні пункти та Координаційний центр Рамкової програми Європейського Союзу з досліджень та інновацій «Горизонт Європа» та Програми з досліджень та навчання Європейського співтовариства з атомної енергії (2021–2025), комплементарної до програми “Горизонт Європа”», 2024, п. 6):

- проведення інформаційних, навчальних або тематичних заходів для цільових груп щодо правових аспектів, умов участі, фінансування тощо;
- участь у заходах та проєктах Європейської комісії (ЕК);
- популяризація результатів наукової, науково-технічної діяльності, інноваційної

продукції з метою пошуку співвиконавців для підготовки спільних проєктів.

Критеріями оцінки діяльності НКП, які стосуються зазначених завдань та функцій, згідно з Положенням («Про затвердження Положення про національні контактні пункти та Координаційний центр Рамкової програми Європейського Союзу з досліджень та інновацій “Горизонт Європа” та Програми з досліджень та навчання Європейського співтовариства з атомної енергії (2021–2025), комплементарної до програми “Горизонт Європа”», 2024, п. 13) є кількість проведених заходів, підготовлених для проведення матеріалів, загальна кількість їх учасників та кількість спільних заходів, проведених разом з іншими НКП та/або іноземними організаціями, регулярність наповнення (оновлення) ІР (кількість підготовлених матеріалів для наповнення Національного порталу міжнародного науково-технічного співробітництва, кількість публікацій у соціальних мережах).

Показники діяльності НКП підтверджуються звітами («Про затвердження Положення про національні контактні пункти та Координаційний центр Рамкової програми Європейського Союзу з досліджень та інновацій «Горизонт Європа» та Програми з досліджень та навчання Європейського співтовариства з атомної енергії (2021–2025), комплементарної до програми “Горизонт Європа”», 2024, п. 15). Частина звітних документів не безпосередньо фінансового характеру стосується визначення рівня досягнення KPI. До KPI, які відповідають зазначеним критеріям та вказані в додатку до договору на виконання функцій НКП Програми «Горизонт Європа» та Програми «Євратом» («Про затвердження примірної форми договору на виконання функцій національного контактного пункту Рамкової програми Європейського Союзу з досліджень та інновацій «Горизонт Європа» та Програми з досліджень та навчання Європейського співтовариства з атомної енергії (2021–2025), комплементарної до програми “Горизонт Європа”», 2024, дод. 1), відносять:

- KPI 9. Кількість проведених заходів (інформаційні дні, тренінги), у т. ч. спільних;

- KPI 10. Загальна кількість учасників заходів;
- KPI 11. Кількість підготовлених матеріалів для проведення заходів, зокрема презентацій, опитувань тощо;
- KPI 12. Регулярність наповнення (оновлення) інформаційних ресурсів, зокрема кількість підготовлених матеріалів для наповнення Національного порталу міжнародного науково-технічного співробітництва, кількість публікацій у соціальних мережах;
- KPI 13. Охоплення цільової аудиторії різними засобами поширення інформації;
- KPI 14. Участь у навчальних заходах для НКП;
- KPI 15. Участь в інформаційних та брокерських заходах (за наявності фінансування).

Для забезпечення електронного звітування керівників НКП в Системі НАУКА (НАУКА: Національна електронна науково-інформаційна система, б. д.) розроблено модуль звітності НКП. У 2025 році вперше в тестовому режимі було забезпечено заповнення електронної форми звіту про діяльність НКП відповідно до критеріїв оцінки діяльності НКП за

I етап 2025 року. Керівники НКП мали можливість заповнити інформацію щодо діяльності НКП, а система на основі заповнених даних розраховувала KPI та формувала пакет документів звітності.

Форма звіту для заповнення даних про заходи включала блок «Заходи» для внесення даних KPI 9 — 11, 14, 15 та «Матеріали заходів» для долучення підготовлених матеріалів та матеріалів підтвердження KPI (рис. 1).

Блок «Заходи» містив мінімальний набір полів для заповнення, достатній для збору даних відповідних KPI. Варіація заходів KPI 9, 14 та 15 забезпечувалася за рахунок значень типу заходу. Вибір організації, проведення заходу чи участі реалізовувався з використанням типу участі. Також додатково долучено вибір організаторів (для виокремлення заходів ЄК та розмежування організаторів щодо навчальних заходів) і формат заходу.

Для звітності щодо регулярності наповнення (оновлення) ІР розроблено блоки «Наповнення (оновлення) інформаційних ресурсів та охоплення цільової аудиторії» та «Файли-підтвердження» (рис. 2).

Внесення даних KPI 12 передбачає вибір виду ІР (серед варіантів Національний пор-

Заходи

Переглянути записи

Тип заходу	Назва			
Організатор	Тип участі	Формат	К-ть учасників	К-ть матеріалів
			0	0
Посилання на захід	Посилання на матеріали	Дата	x	
		дд.мм.гггг		

Додати поле

Матеріали заходів

Переглянути записи

Виберіть файл Файл не вибран

Видалити поле

Додати поле

Рис. 1. Блоки «Заходи» та «Матеріали заходів» форми звіту НКП в Системі НАУКА (НАУКА: Національна електронна науково-інформаційна система, б. д.)

тал міжнародного науково-технічного співробітництва, власний Інтернет-ресурс, власна сторінка в соціальних медіа, партнерська сторінка в соціальних медіа, ЗМІ, інше), заповнення інформації про публікацію, а також охоплення цільової аудиторії, яка в додатковій інформації до KPI 13 визначається як статистика охоплення публікацій.

Із метою підтвердження заповнених даних KPI 12 та 13 керівникам НКП запропоновано варіанти долучення файлів матеріалів підтвердження, зокрема підготовлених матеріалів, фото підтвердження, або внесення інформації щодо таких матеріалів, наприклад їх розміщення в хмарних сховищах (Google Диск, Dropbox тощо).

За результатами електронного звітування керівників НКП за I етап 2025 року (січень-червень) проаналізовано ефективність діяльності НКП, пов'язаною із заходами, використанням ІР з метою забезпечення інформаційної підтримки діяльності НКП. До аналітичних розрахунків включені дані індикаторів виконання KPI, визначені Додатковими угодами, та дані звітних матеріалів у Системі NAUKA

зі статусом «Подано до МОН». Аналіз проводився в розрізі напрямів діяльності, а не персоніфіковано за кожним керівником НКП.

На рис. 3 представлено результати виконання завдань згідно з KPI 9 за напрямками діяльності.

Для всіх НКП встановлене мінімальне значення індикатора виконання KPI, визначене в Додаткових угодах (рис. 3). Фіксуються перевиконання або повне виконання річного значення індикатора, а також індикатора виконання KPI 9 за пів року. Третину річного значення індикатора розраховано лише для 2 НКП, що становить майже 11% від загальної кількості поданих до МОН звітів. Рівень результативності KPI 9 дозволяє збільшити величину індикатора для майбутніх періодів.

Варто зауважити, що формулювання назви KPI не враховує інформацію, зазначену в примітці до KPI щодо включення виступів на заходах, що проводяться іншими організаціями, у т.ч. іноземними. З метою їх включення в процесі тестування значення типу участі «Учасник / Спікер» розділено на окремі скла-

Наповнення (оновлення) інформаційних ресурсів та охоплення цільової аудиторії

Переглянути записи

Вид	Назва публікації	Охоплення цільової аудиторії
Посилання на публікацію	Підтвердження	0

Додати поле

Файли-підтвердження

Переглянути записи

Виберіть файл	Файл не вибран
Видалити поле	Додати поле

Рис. 2. Блоки «Наповнення (оновлення) інформаційних ресурсів та охоплення цільової аудиторії» та «Файли-підтвердження» форми звіту НКП в Системі NAUKA (NAUKA: Національна електронна науково-інформаційна система, б. д.)

дові та долучено імпорт даних до KPI 9 для заходів НКП, у яких зазначено тип участі «Спікер». Однак такі зміни не стосувалися звітів, які на момент внесення змін були подані до МОН, зокрема, за запитом керівника НКП «Правові та фінансові аспекти і Європейська дослідницька рада» зафіксований один такий випадок, хоча передбачений бізнес-процес включав можливість доопрацювання матеріалів звіту. Відкритими залишаються питання формулювання «проводяться іншими організаціями, у т.ч. іноземними», яке дозволяє долучати дані з типом участі «Спікер» інших типів заходів, відмінних від «Захід НКП», а також контроль за кількістю учасників тре-

нінгів, адже в інформації до KPI уточнено «не більше 15–20 осіб на тренінг на 1 НКП». В останньому випадку автори пропонують долучити для заповнення форму проведення, наприклад із значеннями інформаційний день, тренінг, семінар, конференція тощо.

Загальна кількість учасників заходів за даними результатів виконання KPI 10 (рис. 4) становить 5330.

Аналогічно встановлене єдине мінімальне значення індикатора виконання KPI 10. Лише для 4 НКП відсоток виконання близький до половини, тобто майже всі НКП виконали відповідний показник. Варто відмітити результат НКП за напрямом діяльності «Нова

KPI 9. Кількість проведених заходів (інформаційні дні, тренінги), у т. ч. спільних

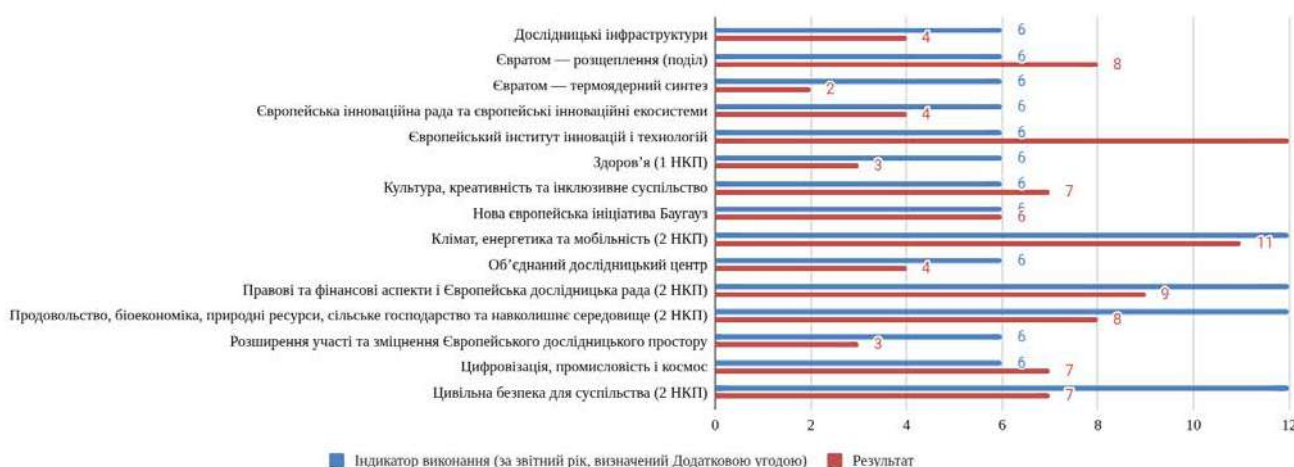


Рис. 3. Порівняльна горизонтальна гістограма значень індикаторів та результатів виконання KPI 9

KPI 10. Загальна кількість учасників заходів



Рис. 4. Порівняльна горизонтальна гістограма значень індикаторів та результатів виконання KPI 10

європейська ініціатива Баугауз», величина якого більше ніж утричі перевищує індикатор виконання за звітний рік.

Оскільки спостерігається розширення учасників за рахунок спільних заходів з іншими НКП, автори пропонують уточнити формулювання KPI, яке частково включити учасників заходу за типом участі «співорганізатор», а також виключити за умови участі в якості спікера.

За інформацією від керівників НКП учасники надають перевагу онлайн-формату проведення, спостерігається залучення невідповідної цільової аудиторії.

Загальна кількість підготовлених матеріалів (KPI 11) більш ніж удвічі перевищує суму значень індикаторів для кожного НКП з розрахунку щонайменше 4 позиції у звітному році, що допустимо, оскільки встановлений лише мінімальний поріг. При цьому система сумує дані заповнені в «К-сть матеріалів», тобто враховуються всі типи участі. Хоча у формулюванні KPI 11 зазначаються підготовлені матеріали лише для проведення заходів, але не уточнюється щодо включення матеріалів, які готуються для виступів на заходах, щоб покрити весь спектр заходів KPI 9, оскільки множина підготовлених матеріалів за KPI 11 $\subseteq$ підготовлені матеріали KPI 9. Також не допускає ймовірність підготовки матеріалів в якості учасника (KPI 14, 15), наприклад за умови участі в обговореннях,

панелях «Запитання та відповіді», що часто практикується в програмах заходів ЄК (наприклад інформаційних днях).

Крім того, на думку авторів, варто розмежувати підготовлені матеріали, які можуть одночасно виступати і способом підтвердження (наприклад для KPI 9), та матеріали, які належать виключно до способів підтвердження (KPI 11, 14, 15). Із метою реалізації такого розмежування пропонується долучити інформаційну частину до завантаження файлів чи розміщення посилання на матеріали, наприклад види підготовлених матеріалів (довідка, презентація, опитування, анкетування, інформаційна брошура, аналітична довідка, публікація), види підтверджень (оголошення / запрошення, звіт (про проведений захід, про участь, звіт та пропозиції), фотозвіт / фотопідтвердження, учасники / список учасників (забезпечити не лише кількісну інформацію, а, можливо, додатково інформацію щодо представництво ЗВО, НУ, МСП, громадські організації тощо)). За таких умов важливою є прив'язка матеріалів (підготовлених, підтвердження) до конкретних заходів.

Статистичні дані результатів виконання KPI 14 керівниками НКП представлені на рис. 5. За напрямом діяльності «Здоров'я» керівник НКП у формі звіту не вказав дані, які могли б імпортуватися в KPI 14.

Для KPI 14 не встановлено кількісну величину індикатора, однак у Додаткових уго-

KPI 14. Участь у навчальних заходах для НКП



Рис. 5. Горизонтальна гістограма результатів виконання KPI 14

дах визначено умову участі в усіх запропонованих навчальних заходах. Тому для аналізу виконання такого KPI пропонується отримати інформацію за звітний період від організаторів таких заходів, наприклад МОН, Координаційний центр (відділ «Офіс Горизонт Європа в Україні» Національного фонду досліджень України) («Про покладення функцій Координаційного центру програми “Горизонт Європа” та програми “Євратом” на відділ “Офіс Горизонт Європа в Україні” Національного фонду досліджень України», 2024), Національний портал міжнародного науково-технічного співробітництва, НКП. Щоб забезпечити вибір повного переліку співорганізаторів, пропонується його зробити множинним, а також залучити відкритий варіант для заповнення значення, якого немає в переліку.

Майже всі НКП, які подали звіти до МОН, повністю виконали значення індикатора KPI 15 за півріччя або перевищили його (рис. 6). Для всіх НКП встановлений єдиний мінімальний індикатор. Окремо керівниками НКП порушується питання наявності фінансування для забезпечення виконання такого KPI, тому в електронному звіті варто забезпечити можливість зазначити наявність фінансування, можливо, розмір. Також у формулюванні KPI не враховані випадки включення окремих панелей щодо партнерства та брокерських питань до складових, наприклад інформаційних заходів ЄК.

Щодо аналізу даних регулярності наповнення (оновлення) IP KPI 12, то встановлений індикатор виконання відповідно до результатів із матеріалів звітів аналогічно має дещо занижене мінімальне значення, єдине для всіх НКП (рис. 7).

Менше ніж 10% виконання розраховано для НКП напряму діяльності «Здоров'я», однак під час аналізу поданих звітних матеріалів з'ясовано, що зазначено інформацію лише про публікацію в партнерській організації, при цьому наявні опубліковані матеріали на Національному порталі міжнародного науково-технічного співробітництва (Національний портал міжнародного науково-технічного співробітництва, б. д.). Третину річного виконання зафіксовано за одним з НКП напряму діяльності «Продовольство, біоeкономіка, природні ресурси, сільське господарство та навколишнє середовище».

У випадку одного НКП «Клімат, енергетика та мобільність» з невисоким відсотком виконання в єдиному записі проінформовано про більш ніж 300 публікацій за звітний період в соцмережах, а також внесено пропозицію синхронізувати дані з Google-таблицею, посилання на яку розміщено в матеріалах звіту. Оскільки з метою синхронізації даних необхідно буде забезпечити сумісність структур таблиці Excel та бази даних, то необхідно попередньо напрацювати вимоги до таких файлів, можливо, розробити його шаблон.

KPI 15. Участь в інформаційних та брокерських заходах (за наявності фінансування)

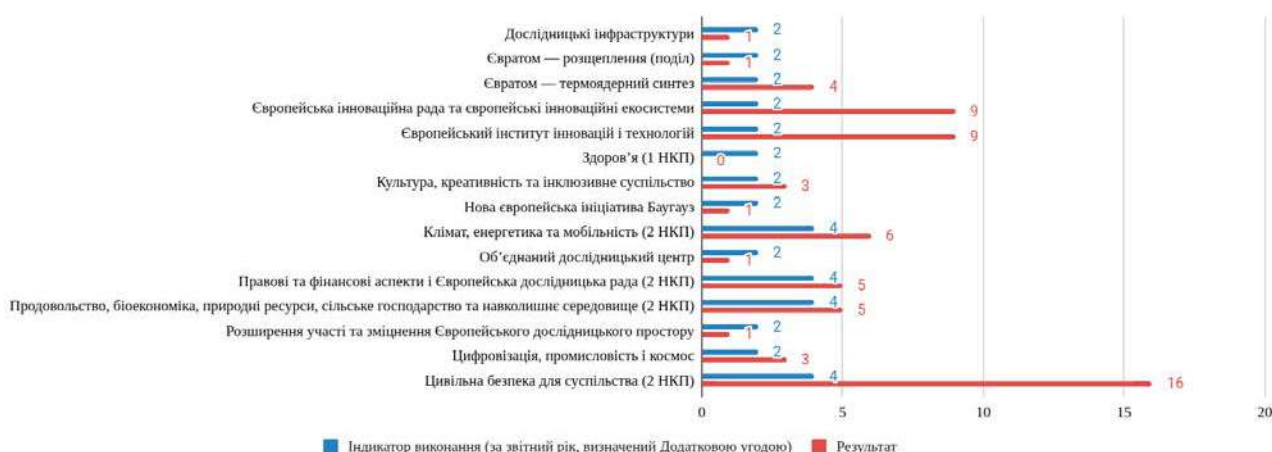


Рис. 6. Порівняльна горизонтальна гістограма значень індикаторів та результатів виконання KPI 15

КРІ 12. Регулярність наповнення (оновлення) інформаційних ресурсів, зокрема кількість підготовлених матеріалів для наповнення Національного порталу міжнародного науково-технічного співробітництва, кількість публікацій у соцмережах



Рис. 7. Порівняльна горизонтальна гістограма значень індикаторів та результатів виконання КРІ 12

Питання синхронізації особливо актуальне для кількості матеріалів, які стосуються наповнення Національного порталу міжнародного науково-технічного співробітництва. Адже у 2025 році з метою поінформованості та залучення ширшого кола наукової спільноти України до участі в Програмах «Горизонт Європа», «Євратом» на відповідному порталі для кожного НКП створено особистий кабінет. Використання такого кабінету надало можливість керівникам НКП:

- редагувати сторінку НКП, яка містить інформацію про представників НКП, включаючи контактну, інформаційну структуру якої можна розгорнути з використанням інформаційних блоків, наприклад для опису діяльності НКП, а також форму звернення до НКП для заповнення потенційними представниками цільової аудиторії;
- редагувати сторінку програми, а саме її структурного елементу, який відповідає напрямку діяльності НКП, хоча за зверненням НКП відкрита можливість забезпечення доступу до ієрархічно вищих сторінок програми;
- додавати, редагувати, публікувати інформацію про організацію та проведення заходів, зокрема оголошення, включаючи програми;
- використовувати календар заходів із метою розміщення анонсів та основної інформації про заплановані заходи мережі

НКП (автоматичне заповнення даних за умови публікації заходів);

- додавати, редагувати, публікувати новини про результати діяльності НКП.

Згодом із метою забезпечення єдиної точки доступу до Модуля звітування НКП та персонального кабінету НКП на Національному порталі міжнародного науково-технічного співробітництва до початку звітної кампанії НКП технічним адміністратором забезпечено єдину авторизацію з використанням Інтегрованої системи електронної ідентифікації ID.GOV.UA.

Загалом імпорт даних з Національного порталу міжнародного науково-технічного співробітництва в модуль звітності НКП забезпечить централізоване автоматичне заповнення інформації, рекомендовано в режимі вибору для підтвердження, для кожного НКП не лише про опубліковані чи підготовлені (наприклад у статусі чернетки) матеріали КРІ 12, а й частково інформації про організовані та проведені заходи КРІ 9 (наприклад, у разі використання імпорту даних з адміністративної панелі: назви за умови типу заходу «Захід НКП» з типом дії «Опублікувати»), а також деякої інформації КРІ 14 та 15 (наприклад, заходи порталу частково містять інформацію про інформаційні дні ЄК, навчальні заходи для НКП).

Враховуючи вище описане, додатково пропонується, по-перше, внести зміни у фор-

мулювання KPI 12 та інформацію до показника з метою включення не лише підготовлених, а й опублікованих матеріалів, по-друге, розширити набір даних, зокрема долучити тип (наприклад новина НКП, анонс заходу НКП, сторінка НКП, сторінка програми / структурного елемента), тип дії (наприклад створено, відредаговано, опубліковано, оброблено (форма звернення)), дату, по-третє, аналогічно доповнити варіанти виборів та розширити їх відкритими варіантами, наприклад для виду, та уже запропонованими.

Щодо долучення файлів підтвердження (рис. 2), то за умови реалізації пропозиції щодо відокремлення виключно способів підтвердження шляхом доповнення інформаційної складової до завантажених файлів, включаючи прив'язку, як раніше було описано до конкретних заходів (KPI 9, 10, 14, 15), а у випадку KPI 12, 13 — IP, блоки «Матеріали заходів» (рис. 1) та «Файли-підтвердження» (рис. 2) можна об'єднати в спільний для всіх KPI.

Результати даних KPI 13 порівнюються з нижньою границею, тобто індикатором виконання в 1000 осіб у звітному році для кожного НКП (рис. 8).

У переважній більшості випадків спостерігається перевищення річного показника та показника за півріччя, тобто звітний період. Нульове значення результату пояснюється браком даних у звітних матеріалах, невисо-

ке — браком чітких пояснень до KPI щодо видів цільової аудиторії, які зараховуються. Наприклад, у доповненні до числового значення НПК за напрямом діяльності «Розширення участі та зміцнення Європейського дослідницького простору» окремо вказана кількість підписників, переглядів та реакцій, сума яких перевищує вказану у звітних матеріалах кількість.

Тому пропонується:

- розмежувати види цільової аудиторії, де допускається їх кількісний перетин, наприклад відкрита (аудиторія, яка заповнює форми (респонденти), надсилає звернення / запитання, залишає відгуки через різні канали (дискусії, коментарі, реакції тощо)), закрыта (фактично підписники, а точніше — пасивні підписники), зацікавлена (можна віднести перегляди), налаштована на співпрацю (наприклад учасники заходів (врахування можна забезпечити автоматично шляхом долучення кількості учасників заходів, включених у KPI 10)), а також ті, хто консультується під час підготовки проєктних пропозицій, реєстрації організації в системах подачі);
- деталізувати канали комунікації, до яких включити електронну пошту (створення розсилок, персоналізовані листи, відповіді на звернення / запитання, наприклад через форму на сторінці НКП Національного порталу міжнародного науково-тех-

KPI 13. Охоплення цільової аудиторії різними засобами поширення інформації



Рис. 8. Порівняльна горизонтальна гістограма значень індикаторів та результатів виконання KPI 13

нічного співробітництва), форми для заповнення з метою збору інформації (наприклад анкетування).

Висновки та пропозиції щодо подальших досліджень. НКП у своїй діяльності керується Положенням про НКП («Про затвердження Положення про національні контактні пункти та Координаційний центр Рамкової програми Європейського Союзу з досліджень та інновацій “Горизонт Європа” та Програми з досліджень та навчання Європейського співтовариства з атомної енергії (2021–2025), комплементарної до програми “Горизонт Європа”», 2024), у якому визначені завдання та функції, критерії та показники діяльності. Перелік НКП Програм «Горизонт Європа», комплементарної до неї Програми «Євратом» та фінансування затверджується наказами МОН. Перелік містить інформацію про окрему посадову особу ЗВО, НУ, іншої юридичної особи незалежно від форми власності або громадської наукової організації, яка має статус юридичної особи, за кожним напрямом діяльності. Фінансування розподілене за установами, на базі яких створено НКП. Нині сума загального фінансування НКП в паспорті бюджетної програми на 2025 рік за КПКВК 2201380 («Про затвердження паспорта бюджетної програми на 2025 рік за КПКВК 2201380», 2025), затвердженому МОН, включена в фінансову підтримку заходів, спрямованих на проведення інформаційно-комунікаційних компаній, забезпечення навчання та підвищення обізнаності українських учасників, зокрема щодо інструментів ЄС з питань підтримки досліджень та інновацій, та безпосередньо визначена в плані заходів з реалізації міжнародних наукових та науково-технічних програм і проєктів відповідно до міжнародних договорів України на 2025 рік.

Показники діяльності НКП підтверджуються звітами, зокрема визначається рівень досягнення KPI, майже половина яких пов'язана з організацією, проведенням, участю в заходах та забезпеченням інформаційної підтримки з використанням інформаційних ресурсів (ІР). Для забезпечення електронного

звітування керівників НКП в Системі НАУКА розроблено модуль звітності НКП, у якому у 2025 році вперше в тестовому режимі було забезпечено заповнення електронної форми звіту про діяльність НКП відповідно до критеріїв оцінки діяльності НКП за I етап 2025 року. Для відповідних KPI у формі звіту розроблені два окремих універсальних, оптимізованих блоки з виокремленою можливістю завантаження матеріалів.

За результатами тестового звітування керівників НКП було встановлено обмежену повноту назв деяких KPI, їх неузгодженість з додатковою інформацією, яка має несистемний та недеталізований характер, невизначеність умов зарахування наданих даних, нечітке розмежування матеріалів заходів та способів підтвердження, теоретичний характер даних, які збираються, порівняно з практичною діяльністю НКП. Відкритим залишається питання роботи з матеріалами підтверджень.

Із метою покращення якості звітних матеріалів пропонується: уточнити формулювання KPI, погодити формулювання з додатковою інформацією, деталізувати її в контексті умов для підрахунку показників, зокрема, чітко визначити спектр заходів, можливо, їх складових, зафіксували тип участі за кожним KPI щодо заходів, розширити набір даних щодо наповнення (оновлення) ІР, зокрема, долучити тип матеріалів, тип дії з такими матеріалами, дату підготовки чи публікації, розмежувати види цільової аудиторії та деталізувати канали комунікації, розмежувати інформативну частину та способи підтвердження, підготовлені матеріали від матеріалів підтвердження. Також внести зміни у формування індикаторів виконання деяких KPI, провести кількісні зміни за результатами звітування та зібраної інформації про звітній період на майбутні періоди. Розширити способи оцінки виконання KPI та включити рейтингову складову. Включити в бізнес-процес погодження достатності матеріалів підтвердження для визначеної ролі.

У процесі тестового режиму на запити керівників НКП проводилися зміни у формі

звіту модуля звітності НКП у Системі НАУКА. За умови внесення змін у KPI, адже форма звіту початково розробляється на їх основі, пропонується збільшити обсяг даних для збору, для деяких даних розширити перелік запропонованих варіантів, долучити до них відкриті для внесення значень, відмінних від наявних, забезпечити множинність вибору, імпорт даних з інших функціональних модулів системи НАУКА, можливо, із зовнішніх інформаційних систем, провести функціональні зміни щодо зарахування даних до деяких KPI, адаптувати визначення виконання

відповідно до формату індикатора виконання, реалізувати прив'язку завантажених матеріалів до конкретних заходів та IP, зокрема для KPI 9–15, загалом долучити інформативну частину про завантажені матеріали, як мінімум, щодо їх статусу, зокрема підготовлені матеріали та спосіб підтвердження або їх одночасність, для використання єдиного блоку для завантажених матеріалів повного переліку KPI, долучити функціонал для забезпечення погодження достатності матеріалів підтвердження з метою зарахування даних до KPI.

REFERENCES

1. On Amendments to the List of National Contact Points of the European Union Framework Programme for Research and Innovation “Horizon Europe” and the European Atomic Energy Community Research and Training Programme (2021-2025), Supplementary to the Horizon Europe Programme, Order of the Ministry of Education and Science of Ukraine No. 405. (2025) (Ukraine). <https://mon.gov.ua/static-objects/mon/uploads/public/67d/a6b/09d/67da6b09de5f8200120522.pdf>
2. On approval of the passport of the budget program for 2025 under the KPKVK 2201380, Order of the Ministry of Education and Science of Ukraine No. 335 (2025) (Ukraine). <https://mon.gov.ua/static-objects/mon/uploads/public/67d/041/d36/67d041d36c87b523691533.pdf>
3. On approval of the action plan for the implementation of international scientific and scientific-technical programs and projects in accordance with international treaties of Ukraine for 2025 under the budget program under the CPKVK 2201380 “Implementation of Ukraine’s obligations in the international sphere”. scientific-technical and educational cooperation, participation in the European Union Framework Program for Research and Innovation, Order of the Ministry of Education and Science of Ukraine No. 655 (2025) (Ukraine). <https://mon.gov.ua/static-objects/mon/uploads/public/684/83d/919/68483d9196b3a633514058.pdf>
4. On Approval of the Primary Form of the Agreement for the Performance of the Functions of the National Contact Point of the European Union Framework Programme for Research and Innovation “Horizon Europe” and the European Atomic Energy Community Research and Training Programme. (2021-2025), complementary to the Horizon Europe program, Order of the Ministry of Education and Science of Ukraine No. 1003 (2024) (Ukraine). <https://mon.gov.ua/static-objects/mon/uploads/public/66a/23f/872/66a23f8721c56357459757.pdf>
5. On the placement of the functions of the Coordination Center of the Horizon Europe program and the Euratom program to the department «Horizon Europe Office in Ukraine» of the National Research Foundation of Ukraine, Order of the Ministry of Education and Science of Ukraine No. 410 (2024) (Ukraine). <https://mon.gov.ua/static-objects/mon/uploads/public/664/32f/1c9/66432f1c9b749029576698.pdf>
6. On financing in 2025 the national contact points of the European Union Framework Programme for Research and Innovation “Horizon Europe” and the European Atomic Energy Community Research and Training Programme (2021-2025), complementary to the Horizon Europe programme, Order of the Ministry of Education and Science of Ukraine No. 61 (2025) (Ukraine). <https://mon.gov.ua/static-objects/mon/uploads/public/678/e12/b18/678e12b182ce6096207731.pdf>
7. National Portal of International Scientific and Technical Cooperation. <https://ms.nauka.gov.ua/>

8. On approval of the Regulations on the National Contact Points and the Coordination Centre of the European Union Framework Programme for Research and Innovation “Horizon Europe” and the Research and Training Programme of the European Atomic Energy Community (2021-2025), complementary to the Horizon Europe programme, Resolution of the Cabinet of Ministers of Ukraine No. 214 (2024) (Ukraine). <https://zakon.rada.gov.ua/go/214-2024-%D0%BF>
9. Agreement (in the form of an exchange of letters) between Ukraine and the European Union on the termination of Ukraine’s obligations to pay financial contributions in connection with the agreements on accession to the Union program, Agreement (2023) (Ukraine, European Union). https://zakon.rada.gov.ua/go/984_011-23
10. Agreement between Ukraine, of the one part, and the European Union and the European Atomic Energy Community, of the other part, on the participation of Ukraine in the Horizon Europe Framework Programme for Research and Innovation and the Research and Training Programme of the European Atomic Energy Community (2021-2025), supplementing the Horizon Europe Framework Programme for Research and Innovation, Agreement (2021) (Ukraine, European Union). https://zakon.rada.gov.ua/go/984_005-21
11. Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part (Annexes), Agreement (2014) (Ukraine, European Union). https://zakon.rada.gov.ua/go/984_a11
12. NAUKA: National Electronic Scientific and Information System. <https://nauka.gov.ua/>

THE ROLE OF THE NATIONAL ELECTRONIC SCIENTIFIC INFORMATION SYSTEM IN ASSESSMENT OF PROVISION BY NATIONAL CONTACT POINTS INFORMATION ABOUT THE EU FRAMEWORK PROGRAMME RESEARCH AND INNOVATION TO UKRAINIAN ENTITIES

Abstract. *The aim was to determine the role of the National Electronic Scientific Information System (NAUKA System) in analyzing the effectiveness of the activities of the National Contact Points (NCPs) of the European Union Framework Programme for Research and Innovation “Horizon Europe” and the Research and Training Programme of the European Atomic Energy Community (2021–2025), complementary to the Horizon Europe programme, related to the organization, conduct, participation in events and regularity of filling (updating) of information resources (IR).*

The research involved the study of regulatory legal acts on the activities of NCPs and related financial support using general scientific (empirical) and general logical methods. Data analysis on the organization, conduct and participation in events by NCP representatives, provision of information support using IS was carried out using statistical methods, supplemented by visualization, based on NCP reporting materials. Reporting was provided in a test mode in the NAUKA System within the framework of the developed NCP reporting module, for the study of which information and functional analysis (modeling) was applied.

According to the results of the research, proposals were formed for key performance indicators (KPIs) of NCP activities, indicators of their implementation, and the NCP reporting module. Within the framework of the KPIs, it is proposed to clarify the wording, structure and supplement additional information, which should include consistent and detailed information on the data that must be submitted, the conditions under which they will be counted. Proposals for KPI performance indicators for future periods relate to quantitative and qualitative changes based on the results of reporting and the information collected about the reporting period. In the NCP reporting module, it is proposed to: increase the volume of data to be collected, the options for choosing with the inclusion of open data, its multiplicity, distinguish the types of uploaded ma-

terials, ensure their connection with a separate record regarding the event, filling (updating) the IR, import data from other functional modules of the NAUKA system, in particular, the National Portal of International Scientific and Technical Cooperation, external information systems, implement approval of the sufficiency of confirmation materials, make functional changes to the calculation of KPIs, adapt the methods of assessing the implementation of KPIs, and include a rating component.

Keywords: budget financing; Horizon Europe; Euratom; key performance indicator; National Electronic Scientific and Information System; national contact point.

ІНФОРМАЦІЯ ПРО АВТОРІВ

Дьогтєва Ірина — науковий співробітник сектору адміністрування відділу супроводження та розвитку Національної електронної науково-інформаційної системи, Державна науково-технічна бібліотека України, вул. Антоновича, 180, Київ, 03150, Україна, +380 44 521 9350, e-mail: i.djogtjeva@dntb.gov.ua, ORCID: 0000-0002-8567-6952

Красовський Олексій — науковий співробітник, Державна науково-технічна бібліотека України, м. Київ, вул. Антоновича, 180, Київ, 03150, Україна, тел. +380 44 521 93 50, e-mail: aleksey_ks@ukr.net, ORCID: 0000-0003-1622-2655

Рибалко Ярослав — науковий співробітник, Державна науково-технічна бібліотека України, м. Київ, вул. Антоновича, 180, Київ, 03150, Україна, тел. +380 44 521 93 50, e-mail: r@nervin.net, ORCID: 0009-0001-9564-7653

INFORMATION ABOUT THE AUTHORS

Dohtieva Iryna — Research Fellow, Administration Sector, Department for Support and Development of the National Electronic Research Information System, State Scientific and Technical Library of Ukraine, 180 Antonovycha Street, Kyiv, 03150, Ukraine, +380 44 521 9350, e-mail: i.djogtjeva@dntb.gov.ua, ORCID: 0000-0002-8567-6952

Krasovskyi Oleksii — Research Fellow, State Scientific and Technical Library of Ukraine, Ukraine, Kyiv, 180 Antonovycha Street, Kyiv, 03150, Ukraine, +380 44 521 9350, e-mail: aleksey_ks@ukr.net, ORCID: 0000-0003-1622-2655

Rybalko Yaroslav — Research Fellow, State Scientific and Technical Library of Ukraine, Ukraine, Kyiv, 180 Antonovycha Street, Kyiv, 03150, Ukraine, +380 44 521 9350, e-mail: r@nervin.net, ORCID: 0009-0001-9564-7653

КОНТЕНТ-АНАЛІЗ ПОЛІТИК ВІДКРИТОГО ДОСТУПУ ТА ВІДКРИТОЇ НАУКИ В УНІВЕРСИТЕТАХ ТА НАУКОВИХ УСТАНОВАХ УКРАЇНИ

Олена Рачинська,

Державна науково-технічна бібліотека України

Анотація. Дослідження присвячене аналізу стану впровадження принципів відкритої науки в українських закладах вищої освіти та наукових установах. Методологічною основою став контент-аналіз офіційних вебсайтів університетів та науково-дослідних інститутів України, що дало змогу оцінити рівень інституційної підтримки відкритого доступу та відкритої науки, наявність відповідних політик, планів щодо впровадження, сервісів тощо, а також відкритості наукових комунікацій та доступності дослідницьких результатів. Метою роботи є визначення ступеня інтеграції концепцій відкритого доступу, управління дослідницькими даними та принципів FAIR (Findable, Accessible, Interoperable, Reusable) у діяльності вітчизняних університетів і наукових установ. У фокусі дослідження – ключові терміни, критерії та індикатори, які дають змогу оцінити прогрес у реалізації відкритої науки на інституційному рівні та співставити українські практики з міжнародними стандартами.

Отримані результати висвітлюють нерівномірність процесу впровадження відкритої науки: провідні університети та установи, залучені до міжнародних проєктів, демонструють вищий рівень адаптації, тоді як більшість організацій перебувають на початковому етапі формування політик відкритого доступу й управління даними. Водночас виявлені як позитивні практики (створення інституційних репозитаріїв, поява авторських договорів, проведення семінарів і тренінгів), так і бар'єри — технічні, організаційні та нормативні. Таким чином, дослідження має прикладне значення для вироблення рекомендацій щодо гармонізації національної наукової політики з європейськими вимогами, а також для визначення пріоритетів подальшого розвитку інституційної інфраструктури відкритої науки в Україні.

Дослідження виконано в межах проєкту НТР «Розробка методології та інструментарію моніторингу ефективності впровадження принципів відкритого доступу, належного управління дослідницькими даними та їхній відповідності принципам FAIR» (2025–2026).

Ключові слова: відкрита наука, відкритий доступ, репозитарій, FAIR, дослідницькі дані, наукова політика, законодавство, Україна, євроінтеграція.

ВСТУП

Сучасний етап розвитку наукової комунікації характеризується переходом до нової парадигми — відкритої науки (Open Science), яка передбачає прозорість усіх етапів дослідницького процесу, вільний доступ до наукових публікацій, дослідницьких даних, програмного забезпечення, методології та інших результатів наукової діяльності (Yaroshenko, 2021; Suber, 2020). Це не лише технологічна чи інформаційна зміна, а глибинна трансформація академічної культури, що змінює

уявлення про роль науки в суспільстві та посилює її суспільну значущість (Burgelman, 2019; OECD, 2021).

Реалізація принципів відкритої науки визначена пріоритетом у Європейському дослідницькому просторі (ERA) та закріплена в кількох стратегічних документах, зокрема Амстердамській декларації про відкриту науку (2016), ініціативі *Plan S*, рамковій програмі *Horizon Europe*, а також у концепції Європейського хмарного середовища відкритої науки (EOSC) (Burgelman, 2019; Björk, 2021).

В основі цих стратегій лежать чотири ключові складові:

- відкритий доступ до публікацій;
- управління дослідницькими даними на основі FAIR-принципів (*Findable, Accessible, Interoperable, Reusable*);
- розвиток відкритих інфраструктур (репозитарії, платформи, цифрові сервіси);
- стимулювання відкритої співпраці між науковцями, установами та суспільством (*Kersloot, 2025; Mohammed Benhamed, 2023; Pence, 2023*).

Для України впровадження цих підходів набуває особливої актуальності в умовах євроінтеграції та необхідності підвищення міжнародної конкурентоспроможності національної науки (*Berezko, 2022; Prykhodkina, 2024*). Важливим кроком стало ухвалення у 2022 році Національного плану відкритої науки (*Kabinet Ministriv Ukrainy, 2022*), а також винесення Міністерством освіти і науки України в березні 2025 року на громадське обговорення законопроекту, спрямованого на гармонізацію національного законодавства з європейськими стандартами (*European Commission, 2020*).

Законопроект передбачає:

- обов'язкове впровадження політик відкритого доступу в закладах вищої освіти та наукових установах;
- розбудову інституційних репозитаріїв;
- забезпечення збереження, довготривалого доступу та повторного використання дослідницьких даних відповідно до FAIR-принципів;
- інтеграцію українських наукових інфраструктур до EOSC.

Запропоновані норми узгоджуються з вимогами програми *Horizon Europe*, яка визначає відкритий доступ обов'язковим елементом для фінансованих досліджень, а також з ініціативою *Plan S*, що встановлює стандарти для наукових публікацій (*Burgelman, 2019; Suber, 2022*). Таким чином, їх ухвалення має стратегічне значення для інтеграції України у європейський науковий простір і забезпечення відповідності міжнародним вимогам.

Водночас, попри нормативне закріплення, рівень реалізації принципів відкритої науки в українських наукових установах залишається нерівномірним. Лише окремі університети розробляють власні політики відкритого доступу та активно використовують системи репозитаріїв (*Drach, 2020; Chmyr, 2017*), тоді як інші обмежуються формальними деклараціями. Аналіз наявності елементів відкритої науки на вебсайтах установ дозволяє оцінити їхню готовність до участі в глобальних ініціативах та виявити ключові прогалини (*Kopanieva, 2023; Shyshkina, 2021*).

Зарубіжні дослідження акцентують на тому, що успіх відкритої науки залежить не лише від наявності законодавчих норм, а й від культурної зміни серед науковців та запровадження системи мотивацій (*Burgelman, 2019; Pence, 2023*). Це робить український контекст особливо цікавим: формування власної політики відкритої науки тут іде паралельно з адаптацією до європейських вимог, що як відкриває нові можливості, так і створює додаткові виклики (*Berezko, 2022; Prykhodkina, 2024*).

ОСНОВНІ ПОНЯТТЯ

Відкрита наука (Open Science, OS) — сучасна концепція організації наукової діяльності, що передбачає відкритість усіх етапів дослідження — від доступу до публікацій і даних до прозорості методології, — використання відкритих інфраструктур та забезпечення можливості повторного використання результатів (*Burgelman, 2019; OECD, 2021*). Основними принципами відкритої науки є відкритий доступ до наукових публікацій, відкриті дані, відкрите рецензування, застосування принципів FAIR (*Findable, Accessible, Interoperable, Reusable*), а також залучення суспільства до наукових процесів через громадянську науку (*Yaroshenko, 2021; Mohammed Benhamed, 2023*).

Дослідницькі дані (Research Data) — цифрові чи фізичні дані, отримані в процесі наукового дослідження, що є підґрунтям для формування висновків і підтвердження результатів (*Shyshkina, 2021*).

Відкриті дані (Open Data) — це дослідницькі дані, що оприлюднені у відкритому доступі та можуть бути вільно використані, повторно застосовані чи поширені з дотриманням умов ліцензування та авторських прав (OECD, 2021; Open Journal Systems, 2025).

Управління дослідницькими даними (Research Data Management, RDM) — комплекс заходів і процедур, що забезпечують організоване збирання, опис, зберігання, поширення та повторне використання дослідницьких даних протягом усього життєвого циклу дослідження. RDM базується на принципах FAIR і передбачає наявність політик, стандартів метаданих, використання унікальних ідентифікаторів (DOI), а також дотримання етичних і правових норм (Kersloot, 2025; Mohammed Benhamed, 2023).

Відкриті репозитарії — електронні системи для зберігання, накопичення та поширення наукових публікацій, дослідницьких даних і навчальних матеріалів у відкритому доступі. Вони можуть бути інституційними (створеними університетом або науковою уста-

новою) чи тематичними (за галузями знань). Якість репозитарію визначається його відповідністю міжнародним стандартам, зокрема DIN 31644:2012-04 (сертифікація надійності) та ISO 16363 (оцінка довготривалого збереження цифрових об'єктів) (OpenDOAR, 2025; BASE, 2025).

АНАЛІЗ ПУБЛІКАЦІЙ

Концепція відкритої науки та вільного доступу до знань дедалі більше утверджується в сучасному науковому дискурсі. Вона спрямована на забезпечення прозорості досліджень, підвищення їх доступності, відтворюваності та соціальної значущості (OECD, 2021). Відкрита наука передбачає не лише вільний доступ до результатів, а й можливість їх повторного використання, спільного аналізу, критичного переосмислення та моніторингу, що набуває особливої ваги в умовах глобалізації науки та цифровізації наукової комунікації (Burgelman, 2019).

Теоретичні засади Open Science були закладені в роботах таких дослідників, як

Таблиця 1

Типи та формати наукових даних: приклади застосування

Поняття	Визначення	Основна функція / призначення	Ключові характеристики
Відкрита наука (OS)	Концепція відкритості всіх етапів наукової діяльності	Забезпечення прозорості, вільного доступу та повторного використання результатів досліджень	Відкритий доступ, FAIR, громадянська наука, відкриті інфраструктури
Дослідницькі / відкриті дані (RD / OD)	Дані, отримані під час дослідження; відкриті дані — доступні для вільного використання	Основний інформаційний ресурс для підтвердження і розвитку досліджень	Цифрові, структуровані, ліцензовані, FAIR
Управління дослідницькими даними (RDM)	Комплекс процедур організації збирання, зберігання, опису, поширення і використання даних	Забезпечення якісного і ефективного життєвого циклу даних	Політики, стандарти метаданих, DOI, дотримання етики і законів
Відкриті репозитарії	Електронні системи зберігання і поширення наукових результатів	Забезпечення відкритого доступу до публікацій і даних	Інституційні, тематичні, стандарти DIN 31644, ISO 16363
Національний репозитарій	Загальнодержавна розподілена електронна база даних академічних текстів	Максимальний доступ до наукової інформації України і світу, сприяння академічній доброчесності	Розподілена структура, систематизація, національний масштаб

П. Субер (*Suber, 2022*). Саме ці праці стали підґрунтям для розвитку сучасних концепцій, що інтегрують етичний, правовий і технологічний виміри відкритої науки.

Подальші емпіричні дослідження підтвердили багатогранність цього феномену. Зокрема Н. Левін та ін. показали, що сприйняття відкритості серед дослідників значною мірою залежить від культурного та дисциплінарного контексту, що зумовлює відмінності між формальними положеннями політик і реальною дослідницькою практикою (*Levin, 2016*). У свою чергу, А. Манко наголошує на необхідності стимулювання відкритості на всіх етапах дослідження, включно з механізмами винагороди для науковців, адже саме система стимулів визначає сталість практик відкритого доступу (*Manco, 2022*).

У європейському контексті важливою є праця Бугельмен Дж. та ін. (2019), де відкритість розглядається як інструмент підвищення ефективності, надійності та соціальної релевантності науки (*Burgelman, 2019*). Значну увагу приділено також відкритим даним, які забезпечують відтворюваність результатів та сприяють розвитку нових міждисциплінарних напрямів. Мохаммед Бенхамед О. пропонує технологічні рішення для впровадження FAIR-принципів, зокрема через *FAIR Data Point*, що стає ключовим інструментом у розвитку цифрових дослідницьких екосистем (*Mohammed Benhamed, 2023*).

С. Мораді та С. Абді класифікують політики відкритої науки за трьома вимірами: *open input*, *open process* та *open output*. Вони доводять, що, хоча більшість країн орієнтуються передусім на відкритий результат, практична реалізація принципів варіює залежно від ресурсів і політичних умов (*Moradi, 2023*).

Вагомий внесок у поширення ідей відкритої науки здійснюють міжнародні ініціативи та інфраструктури: **SPARC Europe**, **OpenAIRE**, **OpenDOAR**, **ROAR** та **BASE**, — які забезпечують функціонування інституційних репозитаріїв, підтримку відкритих журналів і доступність метаданих (*ROAR, 2025; OpenAIRE, 2025; OpenDOAR, 2025; BASE, 2025*). Важливим інструментом для видавців і універ-

ситетів залишається система **Open Journal Systems (OJS)**, яка активно застосовується і в Україні (*Open Journal Systems, 2025*).

У вітчизняному науковому середовищі ідеї відкритої науки почали активно поширюватися після ухвалення ключових міжнародних декларацій, насамперед Будапештської ініціативи відкритого доступу (2002), яка стала відправною точкою для формування глобальних стратегій (*Budapest Open Access Initiative, 2025*). Значний внесок у розвиток тематики зробили українські дослідники: Т. Ярошенко у своїх працях аналізує історичні аспекти впровадження відкритого доступу та роль університетів і бібліотек у цьому процесі (*Yaroshenko, 2021; Yaroshenko, 2011; Yaroshenko, 2022*).

Дослідження В. Копанєвої (2023) розкривають виклики цифровізації наукової комунікації, тоді як Н. Приходькіна (2024) підкреслює значення відкритої науки як умови модернізації дослідницького простору (*Kopanieva, 2023*). Водночас праці М. Шишкіної та О. Спірина (2021) демонструють брак цілісної державної стратегії та недостатню інституційну підтримку, що гальмує процес адаптації України до європейських вимог (*Shyshkina, 2021*).

Попри зростання інтересу до проблематики відкритої науки, в українському контексті бракує системних досліджень, які б оцінювали ефективність упроваджених практик і демонстрували їхні реальні переваги. Такий аналіз необхідний для розкриття потенціалу відкритої науки, здатного забезпечити українським науковцям нові можливості для міжнародної співпраці, підвищити професійну мобільність та конкурентоспроможність у глобальному науковому просторі (*Berezko, 2022*).

Мета дослідження

Метою цієї статті є аналіз сучасного стану розроблення та впровадження політик відкритого доступу та відкритої науки в українських університетах і наукових установах шляхом контент-аналізу офіційних документів та вебресурсів (*Kabinet Ministriv Ukrainy, 2022; Yaroshenko, 2011*).

Завдання дослідження

У межах досягнення поставленої мети визначено такі завдання:

1. Ідентифікувати та систематизувати офіційні документи щодо політик відкритого доступу в українських закладах вищої освіти (ЗВО) та наукових установах (НУ) через аналіз їхніх вебсайтів (*Koranieva, 2023; Yaroshenko, 2022*).

2. Розробити категоріальну схему для контент-аналізу нормативних документів і політик.

3. Проаналізувати змістові характеристики політик відкритого доступу та відкритої науки, у т.ч. аспекти управління даними, надання відкритого доступу до публікацій та підтримку репозитаріїв (*Shyshkina, 2021*).

4. Виявити спільні тенденції та відмінності в підходах різних установ.

5. Оцінити рівень відповідності українських політик міжнародним стандартам, зокрема ініціативам Plan S, EOSC, рекомендаціям UNESCO та OECD (*Burgelman, 2019; OECD, 2021*).

6. Сформулювати рекомендації щодо вдосконалення політик відкритого доступу та відкритої науки з урахуванням європейського та світового досвіду (*Berezko, 2022*).

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

Методологічною основою дослідження є моніторинг офіційних вебсайтів закладів вищої освіти та наукових установ України. Аналіз здійснювався з метою виявлення таких елементів:

- наявність політик відкритого доступу та відкритої науки;
- функціонування інституційних репозитаріїв, що відповідають міжнародним стандартам довготривалого збереження та сертифікації (DIN 31644:2012-04, ISO 16363 або аналогічні);
- нормативні документи, які регламентують зберігання, управління та повторне використання дослідницьких даних;
- використання метаданих із унікальними ідентифікаторами (DOI) для публікацій та дослідницьких даних;
- згадки про впровадження принципів FAIR у внутрішніх нормативних документах

(*Kersloot, 2025; Mohammed Benhamed, 2023*).

Застосування цих критеріїв дозволяє оцінити рівень відповідності українських наукових установ сучасним вимогам відкритої науки та визначити пріоритетні напрями подальшого розвитку. Такий підхід відповідає міжнародній практиці оцінювання, яку використовують, зокрема, OpenAIRE та SPARC Europe (*ROAR, 2025; Open Journal Systems, 2025*).

Вибірка дослідження

Для контент-аналізу було відібрано:

- **137 провідних університетів України** (включно з усіма закладами, що входять до топ-рейтингів національного та міжнародного рівня);
- **203 науково-дослідні інститути НАН України;**
- **11 галузевих наукових установ** (підпорядкованих окремим міністерствам та відомствам) (рис. 1).

Ця вибірка дозволила охопити як найбільші освітньо-наукові центри країни, так і профільні інститути з вузькою спеціалізацією, що забезпечує репрезентативність результатів дослідження.

Критерії оцінювання

Для аналізу стану реалізації принципів відкритої науки у ЗВО та НУ було застосовано такі критерії:

- наявність на сайтах установ (або на сайтах їхніх бібліотек) нормативних документів, що регламентують політику відкритого доступу, управління дослідницькими даними, а також внутрішні положення щодо дотримання принципів FAIR (*Mohammed Benhamed, 2023; Shyshkina, 2021*);
- розміщення інституційних планів розвитку, що передбачають впровадження механізмів відкритої науки, створення або підтримку репозитаріїв, відкритих платформ та інформаційних систем;
- публікація інформації про заходи, події та проекти, які підтверджують практичні кроки з боку адміністрації установ (семінари, тренінги, курси з відкритої науки, створення політик відкритого доступу);

Найменування органу, до сфери управління якого належить заклад освіти

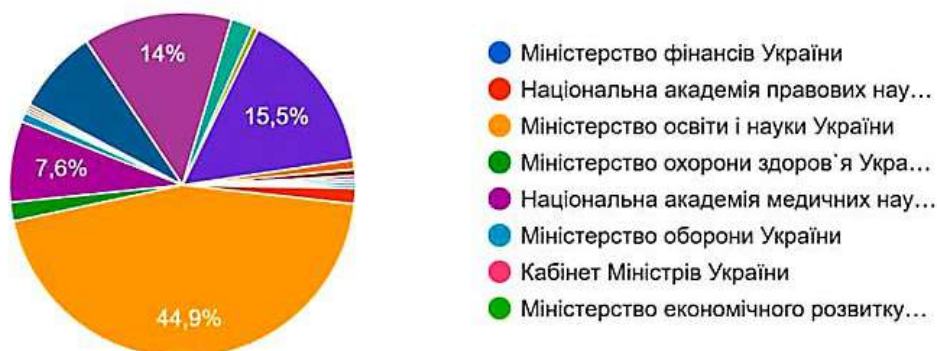


Рис. 1. Розподіл установ за сферою управління (%). Джерело: побудовано автором на основі власних даних дослідження

- наявність інституційних репозитаріїв, що відповідають міжнародним стандартам надійності та довготривалого збереження цифрових об'єктів (DIN 31644:2012-04, ISO 16363 або аналогічні) (*OpenDOAR, 2025; BASE, 2025*);
- використання систем ідентифікації публікацій та даних (наприклад DOI), а також згадування принципів FAIR у внутрішніх документах (*Kersloot, 2025; Mohammed Benhamed, 2023*).

Кожен із цих критеріїв розглядався як показник готовності наукової установи до впровадження політик відкритої науки та інтеграції до європейського наукового простору (*Burgelman, 2019; OECD, 2021*).

Процедура збору та аналізу даних

Збір інформації здійснювався шляхом систематичного моніторингу офіційних вебсайтів університетів, науково-дослідних інститутів НАН України та галузевих наукових установ. Аналіз охоплював матеріали, опубліковані у відкритому доступі за період з 2020 року до 01 липня 2025 року. Основними об'єктами дослідження були:

- **нормативні документи** (положення чи політики про відкритий доступ, відкриту науку, управління дослідницькими даними, внутрішні регламенти щодо FAIR-принципів);
- **стратегічні документи установ** (програми розвитку, плани цифрової трансформації,

мації, дорожні карти з упровадження відкритої науки);

- **інформаційні повідомлення про заходи та події**, що свідчать про практичні дії з реалізації відкритої науки (семінари, вебінари, освітні проекти).

Перегляд здійснювався в таких розділах сайтів: «Про університет / установу», «Наука» або «Наукова діяльність», «Бібліотека», «Політика відкритого доступу», «Репозитарій» чи «Електронні ресурси».

Для фіксації результатів використовувалася спеціально розроблена матриця оцінювання, де робилася відмітка про наявність або брак кожного з визначених критеріїв. На основі зібраної інформації був сформований узагальнений аналітичний огляд, що дозволив визначити рівень готовності установ до впровадження принципів відкритої науки.

Критерії формувалися так, щоб оцінювати не лише формальну наявність документів, а й фактичну активність установи. Наприклад, розміщення положення про відкритий доступ на сайті підтверджує прийняття політики, тоді як анонси заходів чи тренінгів свідчать про практичну реалізацію відповідних принципів (*Yaroshenko, 2022; Pence, 2023*).

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Аналіз офіційних вебсайтів 351 закладу вищої освіти та наукових установ України

показав, що рівень упровадження принципів відкритої науки є **нерівномірним** та значною мірою залежить від типу установи, її розміру, наявності міжнародних проєктів і доступу до фінансування (*Kabinet Ministriv Ukrainy, 2022; Prykhodkina, 2024*).

Для оцінювання було застосовано такі критерії:

- наявність політики відкритого доступу (ПВД);
- функціонування інституційного репозитарію (Реп);
- наявність документів з управління дослідницькими даними (RDM);
- згадування принципів FAIR у внутрішніх документах (FAIR);
- використання унікальних ідентифікаторів (DOI) для публікацій;
- інформаційна активність (новини, семінари, події, навчальні заходи).

Політики відкритого доступу

Лише **12 % установ** (з 351) оприлюднили окремі документи або положення про відкритий доступ. Зазвичай такі документи розміщуються в розділах «Наукова діяльність» або «Бібліотека». У стратегічних планах розвитку лише окремих провідних ЗВО (Національний технічний університет «Київський політехнічний інститут» імені Ігоря Сікорського» (КПІ ім. Ігоря Сікорського), Київський національний університет імені Т. Шевченка (КНУ імені Т. Шевченка), Сумський державний університет (СумДУ)) простежуються згадки про *Open Science* та цифровізацію (*Yaroshenko, 2021; Kopaniieva, 2023*).

Репозитарії

У **17,3 % досліджених установ** (61 із 351) функціонують інституційні репозитарії (разом в Україні їх 137 станом на 10 серпня 2025 за даними НРАТ¹) та є посилання на них. Водночас лише **32 %** із цих 61 установ мають на сайтах положення про репозитарій чи аналогічні регламентуючі документи.

87,9 % репозитаріїв побудовані на базі відкритої платформи DSpace. Водночас немає підтвердження відповідності репозита-

ріїв міжнародним стандартам DIN 31644 або ISO 16363 (*OpenDOAR, 2025; BASE, 2025*).

Виявлено значну кількість неактивних репозитаріїв, де оновлення не здійснювалося протягом тривалого часу.

Документи з управління дослідницькими даними (RDM)

Жодна з проаналізованих установ не оприлюднила окремої політики з управління дослідницькими даними. У кількох випадках є лише загальні згадки про «публікацію результатів» у планах цифрової трансформації без конкретних вимог щодо зберігання чи повторного використання даних (*Mohammed Benhamed, 2023; Shyshkina, 2021*).

Метадані та унікальні ідентифікатори (DOI)

DOI для публікацій застосовують переважно університети, що мають власні наукові журнали, переважно через співпрацю з CrossRef. Водночас у більшості репозитаріїв DOI або *Handle System* не використовуються, що суттєво обмежує інтероперабельність та міжнародну видимість досліджень (*Kabinet Ministriv Ukrainy, 2022; Kersloot, 2025*).

Згадки про FAIR-принципи

Жодна з установ не оприлюднила документів, які б прямо регламентували дотримання FAIR-принципів (*Findable, Accessible, Interoperable, Reusable*). Це підтверджує, що перехід від декларацій до реального впровадження стандартів управління даними ще не відбувся (*Mohammed Benhamed, 2023; OECD, 2021*).

Окремий фрагмент результатів моніторингу ЗВО та НУ України представлено в табл. 1, повні дані будуть представлені у Звіті за результатами проєкту до кінця 2026 року.

Позитивні практики

Найбільш системну та послідовну роботу щодо впровадження принципів відкритої науки презентують НТТУ КПІ імені Ігоря Сікорського (перша в Україні політика відкритої науки на інституційному рівні, схвалена ще у 2022 році²), Бердянський державний

¹ НРАТ – <https://nrat.ukrintei.ua/korysni-resursy/>

² НТТУ КПІ – https://kpi.ua/2022_НОН-337

Таблиця 1

Результати моніторингу (фрагмент)

№	Назва установи	ПВВ	Реп	RDM	FAIR	Активність
1	КНУ ім. Т. Шевченка	+	+	±	±	+
2	НТУ «Харківський політехнічний інститут»	+	+	–	–	+
3	ЛНУ ім. І. Франка	+	+	±	–	±
4	Інститут математики НАН України	–	±	–	–	–
5	Інститут кібернетики ім. В. Глушкова НАН України	–	±	–	–	–

Умовні позначення: + — наявне в повному обсязі; ± — частково реалізовано; – — немає.

педагогічний університет (схвалена не лише Стратегія розвитку відкритої науки, але й Дорожня карта її реалізації та перспективний план)³, Ужгородський національний університет⁴ та деякі інші.

Окремі університети демонструють прогрес також у впровадженні принципів відкритої науки, зокрема:

- КНУ ім. Т. Шевченка, НТТУ КПІ ім. Ігоря Сікорського, Львівський національний університет ім. І. Франка (ЛНУ ім. І. Франка), Одеський національний університет ім. І. Мечникова (ОДУ ім. І. Мечникова) та Державний торговельно-економічний університет впровадили **авторські договори про передачу невиключних прав**, що сприяє забезпеченню відкритого доступу. Зокрема, ДТЕУ в договорі передбачає безоплатну передачу невиключних прав на розміщення твору в інституційному репозитарії; гарантує авторам збереження майнових прав та можливість вільного розміщення творів у відкритому доступі; містить чіткі умови щодо відповідальності сторін та правового захисту;
- СумДУ, КПІ ім. Ігоря Сікорського, НаУКМА, Ужгородський національний університет (УжНУ) регулярно організовують вебінари та семінари з відкритої науки, демонструючи практичну активність у цьому напрямі (Berezko, 2022; Koranićeva, 2023).

Результати аналізу показали, що політики відкритого доступу у відкритому доступі опубліковані лише в 17 установах (4,8 % від вибірки), переважно в університетах та установах НАН України. Найбільш активними у впровадженні елементів відкритої науки залишаються заклади, що беруть участь у міжнародних проєктах і співпраці з європейськими партнерами (*Kabinet Ministriv Ukrainy, 2022; Burgelman, 2019*). Це підтверджує загальну тенденцію: інтеграція до міжнародних ініціатив сприяє більш системному впровадженню політик Open Science (*Open Journal Systems, 2025; OpenAIRE, 2025*).

Важливим кроком у цьому напрямі стало створення порталу «Відкрита наука НАН України» (<https://openscience.nas.gov.ua/>), що об'єднує інформаційні ресурси академічних установ. Крім того, у 2024 році було ухвалено Концепцію реалізації європейських принципів відкритої науки в НАН України на 2024–2030 роки, яка визначає стратегічну політику академії щодо впровадження відкритої науки: мету, принципи, пріоритетні завдання та основні напрями діяльності (*Приходькіна, 2024; Шишкіна, 2021*).

Суттєве значення мають і нормативні документи, ухвалені у 2025 році:

- Розпорядження Президії НАН України «Прозатвердження цільового науково-технічного проєкту НАН України «Впровадження і підтримка відкритої науки в установах НАН України (OPENS²)» на 2025–2026 роки» №104 від 26.02.2025;

³ БДПУ – <https://bdpu.org.ua/polityka-vidkrytoyi-nauky-bdpu/>

⁴ УжНУ – <https://www.uzhnu.edu.ua/uk/infocentre/get/60042>

- Розпорядження Президії НАН України «Про затвердження переліку науково-технічних робіт цільового науково-технічного проекту НАН України «Впровадження і підтримка відкритої науки в установах НАН України (OPENS²)» на 2025 рік» №139 від 13.03.2025.

Ці документи засвідчують наміри НАН України інтегруватися в європейський науковий простір, проте їх реалізація перебуває на початковому етапі. Водночас слід відзначити, що більшість установ, підпорядкованих НАН України, нині не мають власних локальних політик відкритого доступу чи RDM-документів, що свідчить про нерівномірність процесу впровадження та брак єдиної координації (Yaroshenko, 2021; Kopanieva, 2023).

Таким чином, можна зробити висновок, що реформування системи відкритої науки в Україні відбувається «зверху вниз»: нормативна база формується на рівні міністерств і НАН України, але на рівні окремих установ цей процес здебільшого залишається декларативним і нерідко обмежується формальним розміщенням документів на сайтах.

Документи з управління дослідницькими даними (RDM) виявлені лише в 13 установах (3,7 % від загальної вибірки). Це свідчить про те, що практика формалізації правил управління даними в Україні залишається на початковому етапі. Навіть там, де такі документи є, вони здебільшого носять фрагментарний характер і не містять чітких положень щодо збереження, повторного використання чи інтеграції з міжнародними інфраструктурами.

Згадки про FAIR-принципи в нормативних документах поодинокі, що ще раз підтверджує недостатню інтеграцію України в європейські дослідницькі практики, де дотримання FAIR вважається базовою вимогою.

Інформаційна активність (семінари, тренінги, новини про Open Science) властива лише для частини провідних університетів — Київського національного університету імені Т. Шевченка, Національний технічний університет «Київський політехнічний інститут» імені Ігоря Сікорського», Львівського національного університету ім. І. Франка, Сумсь-

кого державного університету. Саме ці заклади найчастіше виступають організаторами вебінарів, курсів та наукових шкіл із питань відкритої науки, що узгоджується з міжнародними тенденціями.

Інституційні репозитарії в Україні функціонують переважно у великих університетах, проте більшість із них не сертифіковані за стандартами DIN 31644 чи ISO 16363. Це знижує їхню надійність та довготривалу стійкість, ускладнюючи інтеграцію в європейську екосистему EOSC (*OpenDOAR, 2025; BASE, 2025*).

Аналіз глобальної бази Registry of Open Access Repositories (ROAR) свідчить про активне зростання кількості відкритих репозитаріїв у світі. Станом на 2025 рік зареєстровано понад 4973 репозитарії, з яких 1789 — у Європі [21]. Лідерами залишаються: США — 870, Німеччина — 252, Велика Британія — 244, Іспанія — 195. Для порівняння, у країнах Центральної та Східної Європи кількість репозитаріїв є суттєво меншою: Польща — 90, Чехія — 50, Литва — менше ніж 20 (рис. 2).

Україна посідає 4-те місце серед європейських країн за кількістю зареєстрованих відкритих репозитаріїв наукових публікацій — 137 (станом на 2025 рік), що становить близько 7,5 % від загальноєвропейського показника. Це свідчить про відносно високий рівень розвитку інфраструктури відкритого доступу в Україні порівняно з іншими країнами Центральної та Східної Європи, де кількість репозитаріїв суттєво менша (*ROAR, 2025*).

Такий результат можна вважати позитивним індикатором інтеграції України в глобальний рух відкритого доступу. Він свідчить, що навіть за умов фінансових та організаційних обмежень українські університети та наукові установи активно розбудовують репозитарії — як інституційні, так і галузеві. Це, у свою чергу, сприяє збільшенню видимості українських досліджень у світі, зростанню цитованості та залученню до міжнародних наукових мереж (*OpenAIRE, 2025; ROAR, 2025*).

Водночас слід зазначити, що кількісні показники не завжди корелюють із якістю функ-

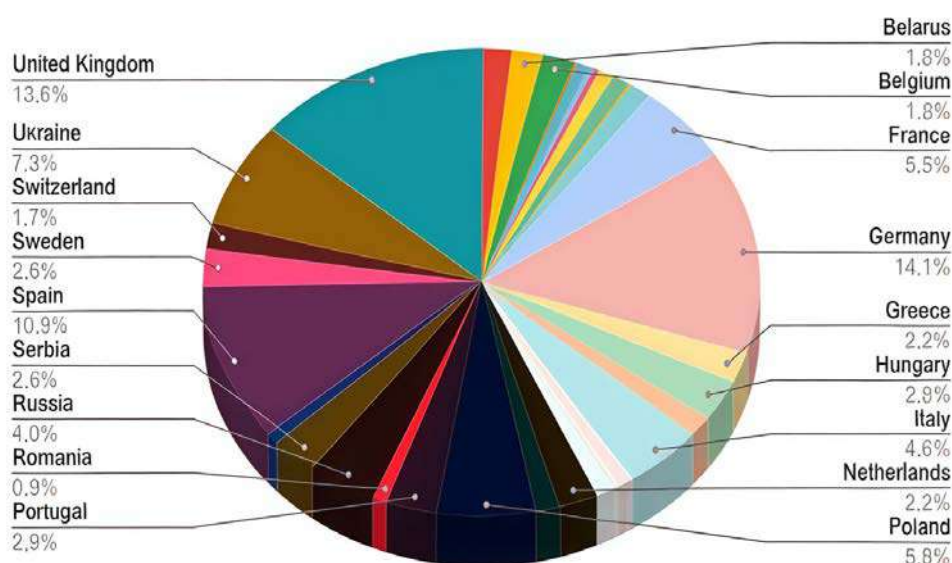


Рис. 2. Відсоткове співвідношення кількості відкритих репозитаріїв у світі за країнами відповідно до даних Registry of Open Access Repositories (ROAR) станом на 2025 рік.

ціонування: значна частина репозитаріїв не сертифіковані за міжнародними стандартами DIN 31644 або ISO 16363, а їх оновлення є нерегулярним. Це обмежує можливість інтеграції з європейськими ініціативами, зокрема EOSC та OpenAIRE (OpenAIRE, 2025; ROAR, 2025).

Таким чином, Україна має помітний потенціал у сфері відкритого доступу, проте подальший розвиток інфраструктури потребує державної координації, впровадження стандартів якості та активної участі в міжнародних проєктах, що дозволить перетворити кількісне зростання в якісні зміни.

Крім того, за даними Registry of Open Access Repositories (ROAR) та результатами власного аналізу, в Україні простежуються такі закономірності:

- 87,9 % українських репозитаріїв створені на базі системи DSpace — відкритого програмного забезпечення із широкими можливостями налаштування та підтримкою міжнародних стандартів метаданих (OAI-PMH, Dublin Core). Використання саме цієї платформи пояснюється її відкритим кодом, відносно простотою інсталяції та поширеністю у світі. Однак брак національної підтримки й сертифікації відповідно до міжнародних стандар-

тів (DIN 31644, ISO 16363) часто знижує рівень надійності українських репозитаріїв (OpenAIRE, 2025; ROAR, 2025);

- найвища активність зі створення репозитаріїв в Україні та внесення контенту зафіксована у 2012 році. Цей період збігається з початком активного впровадження вимог відкритого доступу у світі та появою рекомендацій Європейської комісії для програм FP7 та Horizon 2020 (European Commission, 2020; OECD, 2021). Відповідно можна стверджувати, що міжнародні ініціативи та зобов'язання України в межах участі в європейських проєктах стали ключовим стимулом для формування локальної інфраструктури відкритого доступу (рис. 3).

Отже, репозитарії в Україні розвиваються в руслі загальноєвропейських тенденцій, але залишаються вразливими в питаннях довготривалого збереження даних, інтеграбельності та інтеграції з глобальними інфраструктурами (EOSC, 2025; OpenAIRE, 2025; BASE, 2025).

Високий формальний показник кількості українських репозитаріїв (137 у ROAR станом на 2025 рік) не завжди корелює з їхньою якістю та відповідністю міжнародним стандартам (ROAR, 2025). Більшість репозитаріїв

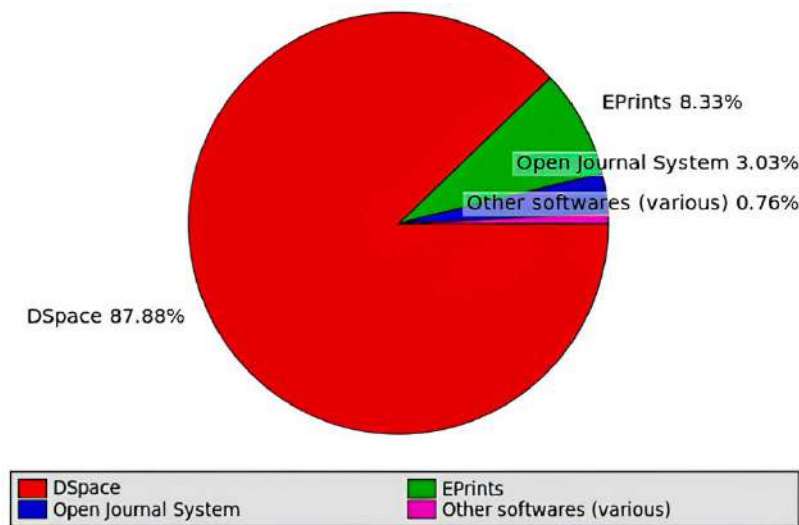


Рис. 3. Відсоткове співвідношення кількості українських репозитаріїв, створених на базі різного програмного забезпечення.

мають інституційний характер, проте лише невелика частка відповідає вимогам DIN 31644:2012-04, ISO 16363 чи отримала статус сертифікованого *Trusted Digital Repository* (OpenDOAR, 2025; BASE, 2025). Також не всі з них підтримують метадані з використанням DOI або інших постійних ідентифікаторів, що обмежує їх інтеграцію в міжнародні інформаційні системи.

Особливу увагу було приділено аналізу українських репозитаріїв, зареєстрованих у глобальній системі Registry of Open Access Repositories (ROAR). Станом на 2025 рік в ROAR зафіксовано 137 українських репозитаріїв, серед яких 15 належать науковим установам, 120 — бібліотекам закладів вищої освіти.

Однак під час перевірки виявлено значну кількість неактивних сторінок, які не оновлюються або є недоступними, що свідчить про недостатню увагу до сталого адміністрування частини таких ресурсів.

Додаткову інформацію надає система BASE (Bielefeld Academic Search Engine), у якій Україна представлена 1 763 951 публікацією відкритого доступу від 378 провайдерів контенту (передусім інституційні репозитарії) (BASE, 2025). Найбільшими за обсягами постачання публікацій до цього гарвестера стали: DSpace Національної бібліотеки України

імені В. І. Вернадського (НБУВ) — 187 528 публікацій, LibNAS (НАН України) — 113 905, ESSUIR (СумДУ) — 94 990, ELAKPI (КПІ ім. І. Сікорського) — 56 528, eNTUKhPIIR (НТУ «Харківський політехнічний інститут») — 56 090.

Моніторинг офіційних сайтів українських ЗВО та НУ підтвердив, що формування інституційної інфраструктури відкритого доступу перебуває на різних стадіях розвитку. Серед досліджених 61 установи:

- усі 61 мають посилання на інституційний репозитарій, що забезпечує базову доступність ресурсів;
- лише 32 % установ (близько 20) розмістили на сайтах Положення про репозитарій чи інші нормативні документи, що регламентують його функціонування;
- окремі ресурси мають інноваційні ознаки — наприклад, репозитарій Одеського національного університету імені І. І. Мечникова отримав ISSN, що відповідає міжнародним практикам і підвищує статус цього ресурсу.

Водночас виявлено суттєві відмінності між формальним і фактичним доступом до результатів досліджень. Часто розділи з назвами «Електронний каталог», «Електронний архів», «База даних публікацій нау-

ковців», «Бібліографічний перелік робіт» не забезпечують повнотекстового доступу, а містять лише бібліографічні описи. Це суперечить міжнародним критеріям відкритого доступу.

Виявлені проблеми та бар'єри

Системні проблеми: брак централізованої координації; нестача фінансових ресурсів; обмежена технічна експертиза; консервативність академічної культури.

Технічні бар'єри: застарілі IT-інфраструктури; проблеми інтероперабельності; недостатня стандартизація метаданих; обмежена інтеграція з міжнародними системами (EOSC, OpenAIRE, BASE).

Організаційні виклики: нестача спеціалізованого персоналу для адміністрування репозитаріїв; нечіткий розподіл відповідальності між установами та НРАТ; низька мотивація дослідників щодо самоархівування; конфлікт із традиційними системами оцінювання наукових результатів.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Контент-аналіз вебсайтів українських наукових установ демонструє **неоднорідність упровадження принципів відкритої науки**. Провідні університети та окремі наукові установи демонструють значний прогрес у створенні та підтримці репозитаріїв, тоді як більшість установ перебувають лише на початковому етапі трансформації.

Успішна імплементація потребує системного підходу, що включає:

- політичні ініціативи та нормативне регулювання;
- технічну модернізацію інфраструктур;
- освітні програми та формування культури відкритої науки;
- систему мотивацій і стимулів для дослідників.

Попри численні виклики, позитивна динаміка (зростання кількості репозитаріїв, поява авторських договорів, участь у міжнародних ініціативах) створює основу для подальшої інтеграції України в глобальний дослідницький простір і підвищення міжнародної конкурентоспроможності національної науки.

Рекомендації

Короткострокові заходи (1–2 роки):

1. Розробка типових політик відкритої науки для різних категорій установ.
2. Створення національної платформи для обміну досвідом між адміністраторами репозитаріїв.
3. Запуск програми тренінгів для ключового персоналу бібліотек і наукових відділів.
4. Надання державної технічної підтримки для розвитку та оновлення репозитаріїв.

Середньострокові ініціативи (3–5 років):

1. Інтеграція вимог відкритої науки в системи інституційного та державного оцінювання наукових результатів.
2. Розвиток національної інфраструктури дослідницьких даних.
3. Створення спеціалізованих центрів підтримки Open Science при провідних університетах.
4. Гармонізація стандартів з європейськими вимогами (EOSC, Plan S, OECD).

Довгострокові цілі (5+ років):

1. Повна інтеграція України в Європейський дослідницький простір.
2. Лідерство у вибраних напрямках відкритої науки (наприклад citizen science чи FAIR-data management).
3. Експорт українського досвіду в країни, що розвиваються.
4. Розробка інноваційних моделей наукової комунікації та цифрових освітніх сервісів.

REFERENCES

1. BASE. (2025). <https://www.base-search.net/Search/Results?lookfor=country%3Aua&l=en&oaboo st=1&ling=0&newsearch=1&refid=dcadven&name=>
2. Berezko, O. (2022, zhovten 26). Vidkryta nauka – druhyi shans dlia ukrainskoi naukovoï systemy? ZN.UA. <https://zn.ua/ukr/science/vidkrita-nauka-druhij-shans-dlja-ukrajinskoji-naukovoji-sistemi.html>

3. Björk, B.-C. (2021). Open access to construction IT research articles – developments over the past 25 years. *Journal of Information Technology in Construction*, 26, 23–27. <https://doi.org/10.36680/j.itcon.2021.002>
4. Budapest Open Access Initiative. (2025). <https://www.budapestopenaccessinitiative.org/read/ukrainian-translation/>
5. Burgelman, J. C., Pascu, C., Sjoer, R., et al. (2019). Open Science, Open Data, and Open Scholarship: European Policies to Make Science Fit for the Twenty-First Century. *Frontiers in Big Data*, 2, 43. <https://doi.org/10.3389/fdata.2019.00043>
6. Chmyr, O. S., Kvasha, T. K., Yaroshenko, T. O., & Chukanova, S. O. (2017). *Natsionalnyi repozytarii akademichnykh tekstiv: vidkryti dostup do naukovoï informatsii*. Kyiv: Ukrainskyi instytut naukovotekhnichnoi ekspertyzy ta informatsii.
7. Derzhavnyi torhovelno-ekonomichnyi universytet. (2025). Avtorskyi dohovir pro peredachu nevykliuchnykh prav na vykorystannia akademichnoho tvor. Repozytarii DTEU. <https://ur.knute.edu.ua/bitstreams/cad4f51c-b899-4036-892b-e6c2f3673a13/download>
8. Drach, I. (2020). Vidkryta nauka v universytetakh: tsili ta perevahy. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Serii: Pedahohika. Sotsialna robota*, 1(50), 90–93.
9. European Commission. (2020). Access to and preservation of scientific information in Europe: Report on the implementation of Commission recommendation C(2018)2375 final. Publications Office of the EU. <https://op.europa.eu/s/xcpo>
10. Kabinet Ministriv Ukrainy. (2022). Pro zatverdzhennia natsionalnoho planu shchodo vidkrytoi nauky: Rozporiadzhennia KMU vid 08.10.2022 r. № 892. <https://www.kmu.gov.ua/npas/prozatverdzhennia-natsionalnoho-planu-shchodo-vidkrytoi-nauky-892-081022>
11. Kersloot, M. G., Jetten, M., Nylander, S., Schoots, F., & Cornet, R. (2025). The FAIR Lesson Plan Handbook: Open Educational Resources for FAIR Training. *Studies in Health Technology and Informatics*, 327, 1074–1078. <https://doi.org/10.3233/SHTI250548>
12. Kopanieva, V. (2023). Naukova komunikatsiia v tsyrovomu seredovyschi. *Visnyk Knyzhkovoi palaty*, 9(326), 27–37. [https://doi.org/10.36273/2076-9555.2023.9\(326\).27-37](https://doi.org/10.36273/2076-9555.2023.9(326).27-37)
13. Levin, N., Leonelli, S., Weckowska, D., Castle, D., Dupré, J. (2016). How Do Sc
14. Mohammed Benhamed, O., Burger, K., Kaliyaperumal, R., Santos, L. O. B. D. S., Suchánek, M., Slifka, J., & Wilkinson, M. D. (2023). The FAIR Data Point: Interfaces and Tooling. *Data Intelligence*, 5(1), 184–201. https://doi.org/10.1162/dint_a_00161
15. Moradi, S., & Abdi, S. (2023). Open science–related policies in Europe. *Science and Public Policy*, 50(3), 521–530. <https://doi.org/10.1093/scipol/scac082>
16. OECD. (2021). *Open Science – Enabling discovery in the digital age*. Paris: OECD. <https://is.gd/EMIG9E>
17. Open Journal Systems (OJS). (2025). <https://openscience.in.ua/ojs>
18. OpenAIRE. (2025). <https://www.openaire.eu>
19. OpenDOAR. (2025). <https://www.jisc.ac.uk/opensoar>
20. Pence, H. (2023). Will Open Science Succeed in Higher Education? *Journal of Educational Technology Systems*, 51(3), 261–270. <https://is.gd/Oho9Kd>
21. Prykhodkina, N. O. (2024). Vidkryta nauka v suchasnomu doslidnytskomu prostori. *Visnyk pisliadyploinoi osvity: zb. nauk. pr. Seriiia «Pedahohichni nauky»*, 30(59), 109–134. [https://doi.org/10.58442/3041-1831-2024-30\(59\)-109-134](https://doi.org/10.58442/3041-1831-2024-30(59)-109-134)
22. ROAR (Registry of Open Access Repositories). (2025). <https://roar.eprints.org>
23. Shyshkina, M. P., & Spirin, O. M. (2021). Rozvytok vidkrytoi nauky v Ukraini: problemy ta perspektyvy. *Informatsiini tekhnolohii i zasoby navchannia*, 81(1), 1–19.
24. Suber, P. (2022). *Open Access*. MIT Press Essential Knowledge series. Cambridge, MA: MIT Press.
25. Vidkryta nauka – druhyi shans dlia ukrainskoi naukovoï systemy? [Open science – a second chance for the Ukrainian scientific system?]. (2022, October 26). ZN.UA. <https://zn.ua/ukr/science/vidkrita-nauka-druhij-shans-dlja-ukrajinskoji-naukovoji-sistemi.html>
26. Vidkryta nauka v Ukraini: postup i shliakhy rozvytku. (2021). *U Teoretyko-praktychni problemy vykorystannia matematychnykh metodiv i kompiuterno-orientovanykh tekhnolohii v osviti ta nautsi*:

- Zbirnyk materialiv III Vseukrainskoi konferentsii (s. 131–134). Kyiv: Kyivskiy universytet imeni B. Hrinchenka.
27. Yaroshenko, T. (2011). Zeleniy shliakh vidkrytoho dostupu. Repozytarii ta yikh rol u naukovii komunikatsii: pershi dvadtsiat rokiv. Bibliotechnyi visnyk, 5, 3–10.
28. Yaroshenko, T. (2021). Vidkrytyi dostup, vidkryta nauka, vidkryti dani: yak tse bulo i kudy ydemo (do 20-littia Budapeshtskoi initsiatyvy vidkrytoho dostupu). Ukrainskyi zhurnal z bibliotekoznavstva ta informatsiinykh nauk, 8, 10–26. <https://doi.org/10.31866/2616-7654.8.2021.247582>
29. Yaroshenko, T., Serbin, O., & Yaroshenko, O. (2022). Vidkryta nauka: rol universytetiv ta bibliotek u suchasnykh zminakh naukovoii komunikatsii. Tsyfrova platforma: informatsiini tekhnolohii v sotsiokulturnii sferi, 5(2), 277–292.

CONTENT ANALYSIS OF OPEN ACCESS AND OPEN SCIENCE POLICIES IN UNIVERSITIES AND RESEARCH INSTITUTIONS OF UKRAINE

Abstract. *The study is devoted to a systematic analysis of the implementation of open science principles in Ukrainian higher education institutions and research organizations. The methodological basis is the content analysis of official websites of universities, research institutes, and libraries, which made it possible to assess the level of openness of scientific communications and the availability of research outputs. Particular attention is paid to the evaluation of the National Open Science Plan and the provisions reflected in the draft law “On Amendments to Certain Laws of Ukraine Regarding the Implementation of Open Science Principles.”*

The purpose of the article is to determine the degree of integration of open access policies, research data management, and FAIR principles (Findable, Accessible, Interoperable, Reusable) into the activities of Ukrainian universities and research institutions. The study focuses on key terms, criteria, and indicators that make it possible to assess progress in implementing open science at the institutional level and to compare Ukrainian practices with international standards.

The results highlight the uneven nature of open science implementation: leading universities and institutions engaged in international projects demonstrate higher levels of adaptation, while the majority of organizations remain at the initial stage of establishing open access and research data management policies. Both positive practices (creation of institutional repositories, introduction of copyright transfer agreements, organization of seminars and training courses) and barriers (technical, organizational, and regulatory) were identified.

Thus, this research has practical significance for developing recommendations on harmonizing national science policy with European requirements, as well as for defining priorities for the further development of Ukraine’s institutional open science infrastructure.

Keywords: *open science, open access, repository, FAIR, research data, science policy, legislation, Ukraine, European integration.*

ІНФОРМАЦІЯ ПРО АВТОРА

Рачинська Олена — молодший науковий співробітник, Державна науково-технічна бібліотека України, вул. Антоновича, 180, м. Київ, 03150, Україна; e-mail: rachynska.o@dntb.gov.ua; ORCID: 0009-0001-3979-8756

INFORMATION ABOUT THE AUTHOR

Rachynska Olena — researcher, The State Scientific and Technical Library of Ukraine, e-mail: rachynska.o@dntb.gov.ua; ORCID: 0009-0001-3979-8756

DIGITIZATION OF DOCUMENT FLOW IN THE SCIENTIFIC FIELD: PRACTICAL ASPECTS BASED ON THE EXAMPLE OF THE “NAUKA” SYSTEM

Shapovalov Yevhen,

State Scientific and Technical Library of Ukraine, NC “Junior Academy of Sciences of Ukraine”

Shapovalov Viktor,

State Scientific and Technical Library of Ukraine, NC “Junior Academy of Sciences of Ukraine”

Rudakova Tetiana,

State Scientific and Technical Library of Ukraine

Rybalko Yaroslav,

State Scientific and Technical Library of Ukraine

Vasylenko Andrii,

State Scientific and Technical Library of Ukraine

Abstract. *The fragmentation of scientific data across disparate systems in Ukraine poses significant challenges to effective research management, strategic planning, and integration into the global scientific community. This article introduces the Ukrainian Research Information System (URIS), a comprehensive framework of interconnected registries aimed at streamlining the management of scientific activities. Developed in alignment with the Law of Ukraine «On Public Electronic Registries» (No. 1907-IX, dated 18.11.2021), URIS integrates data on research projects, results, institutions, publications, infrastructure, certifications, dissertations, intellectual property, researchers, and supporting documentation. By ensuring compliance with national legislation and incorporating international standards such as ORCID for researcher identification, ROR for organizations, and DOI for digital objects, the system enhances transparency, interoperability, and operational efficiency within Ukraine’s scientific ecosystem.*

The literature review examines key areas including methodologies for persistent identifiers (PIDs), development of integrated scientific information systems (CRIS), standards for data quality and confidentiality in public registries, and the impact of interoperability on cross-border data exchange. Drawing from global best practices, the analysis highlights the importance of standards like CERIF, SDMX, and OAI-PMH for data harmonization, while addressing challenges such as data heterogeneity, privacy concerns, and governance structures.

Methodologically, the study employs a multifaceted approach: a detailed review of Ukrainian legislation, conceptual modeling using Entity-Relationship Diagrams (ERD), and analysis of international CRIS implementations to design URIS as a legally compliant, automated system that minimizes administrative burdens through single data entry and validation.

The results detail URIS’s architecture, comprising nine core registries and an intellectual property integration module. For instance, the Registry of Projects manages funding and status details with unique identifiers; the Registry of Scientific Results documents outputs like technologies and datasets; the Registry of Institutions builds on EDRPOU with scientific specifics; and the Registry of Publications aggregates metadata from sources like Scopus, ensuring deduplication and verification. Interconnections enable seamless data flow, automated dossier generation, and public access to non-sensitive information, while security protocols protect confidentiality.

In conclusion, URIS represents a transformative step toward a unified, efficient scientific infrastructure in Ukraine, fostering evidence-based policymaking, reducing redundancy, and promoting international collaboration. Future enhancements could incorporate AI for advanced analytics, further elevating Ukraine’s position in the global research landscape.

Keywords: *Scientific registries, URIS, research information system, data integration, interoperability, Ukraine, public electronic registries, ORCID, DOI, ROR.*

INTRODUCTION

In today's scientific environment, characterized by rapid growth in data volumes and increasing demands for transparency and accessibility, effective information management is becoming critically important. The development of digital technologies opens up new opportunities for automation, integration, and data exchange, but at the same time creates significant challenges related to standardization, compatibility, and quality and security assurance. The lack of unified approaches to identifying digital objects, integrating disparate information systems, and ensuring cross-border interaction hinders scientific progress and reduces the effectiveness of research.

THEORETICAL BACKGROUND

This literature review systematizes empirical data and analytical conclusions from four key areas that form the basis of modern scientific infrastructure. First, it examines methodologies and standards for persistent identifiers (PIDs), which are the foundation for reliable citation and linking of digital objects. Second, it analyzes approaches to the development of integrated scientific information systems (CRIS), similar to the Ukrainian URIS system, which serve as central hubs for the collection and management of scientific information. Third, it examines international standards for ensuring data quality and confidentiality in public electronic registries, which is particularly important in sensitive areas such as healthcare. Finally, the impact of international standards on cross-border data exchange, which is a key factor for global scientific cooperation, is assessed. The purpose of this review is to provide a comprehensive overview of the current state, challenges, and best practices in these interrelated areas.

Methodologies and Standards for Persistent Identifiers (PID). Persistent identifiers (PID) are the cornerstone of modern digital scientific infrastructure, providing stable and unambiguous references to digital objects such as datasets, publications, and software. An analysis of existing research shows that the leading technologies in this field are systems based on the Digital Object Identifier (DOI) and Handle

System, which are most often cited as the main models in the context of publishing and scientific data (Paskin, 2009; Weigel et al., 2013). These systems are complemented by other important standards such as the Archival Resource Key (ARK), Uniform Resource Name (URN), and Open Researcher and Contributor ID (ORCID) for identifying researchers (Agosti et al., 2022).

Key topics that constantly arise in the literature are the problems of interoperability, management, scalability, and long-term sustainability of identification systems. Researchers propose various conceptual models to solve these problems. For example, to overcome the heterogeneity of different PID systems, framework solutions based on the semantic web and ontologies have been proposed, which facilitate the translation of metadata and ensure compatibility (Bellini et al., 2012). Other approaches focus on developing context-oriented frameworks that preserve links between different identifiers, which is especially important for complex scientific projects (Weigel et al., 2013).

Ensuring the long-term sustainability of PID goes beyond purely technical solutions and requires considerable attention to organizational and political aspects. Research highlights the critical importance of governance structures involving stakeholders and the development of clear policies to ensure financial sustainability and adaptation to technological change (Car et al., 2017). Technical solutions such as location-independent identifiers (Handle System) and abstract layers (Platform-Independent Model) are proposed as means to increase system reliability (Weigel et al., 2013; Car et al., 2017). The successful implementation of PIDs also depends on alignment with recognized standards and registration agencies such as the DOI Foundation, Crossref, and DataCite (Paskin, 2009; Hardisty et al., 2021). Although some fields, such as biodiversity, have already developed best practices at the community level, many other domains are still in the conceptual stage, indicating the need for further empirical research to assess the real effectiveness of different approaches (Agosti et al., 2022).

Development of Integrated Scientific Information Systems (CRIS). Integrated sci-

entific information systems (CRIS) are central elements of national and institutional scientific infrastructure, ensuring the collection, management, and analysis of research activities. The development of such systems, such as the Ukrainian URIS, is based on a set of international standards and methodologies aimed at ensuring interoperability and functionality. An analysis of existing research shows that the de facto standard for metadata and data models in CRIS is the Common European Research Information Format (CERIF), which is mentioned in most thematic studies as the basis for harmonizing data at the institutional and national levels (Bollini et al., 2016; Karaiskos et al., 2017).

Alongside CERIF, other standards are used for specific tasks. ORCID is widely used for the unique identification of researchers, which is critical for eliminating ambiguity and correctly linking data (Bollini et al., 2016; Karaiskos et al., 2017). Statistical Data and Metadata eXchange (SDMX) is used for statistical data exchange, while Dublin Core and Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH) are used to collect metadata from various repositories (Sousa Pinto et al., 2014). For conceptual modeling of complex systems, some studies refer to models such as the DELOS Digital Library Reference Model (DELOS DLRM) and the Open Archival Information System Reference Model (OAIS RM) (Sadirmekova et al., 2021).

Architectural approaches to CRIS construction are mainly based on open source modular platforms (e.g., DSpace-CRIS), which promotes flexibility and interoperability, as well as on federated or service-oriented architectures for aggregating data from heterogeneous sources (Bollini et al., 2016; Scholze and Maier, 2012). To ensure data reliability and consistency, especially in complex ecosystems such as the Portuguese PTCRIS, formal software engineering methods and automated verification tools are used (Moreira et al., 2015).

Despite the existence of standards, developers face a number of challenges. The main problems include the heterogeneity of data formats, the technical difficulties of integrating leg-

acy systems, and ensuring the quality of meta-data (Leiva-Mederos et al., 2017; Moreira et al., 2015). Other significant obstacles are the lack of national researcher registries and the complexity of integration processes, as noted in the analysis of Ukrainian infrastructure (Kaliuzhna and Auhunas, 2022). Thus, the successful development of CRIS requires not only compliance with standards, but also local customization and the application of advanced methodologies to overcome technical and organizational barriers.

Data Quality and Confidentiality Standards in Public Electronic Registries. Public electronic registries, especially in the healthcare sector, play a key role in monitoring, research, and clinical decision-making. The effectiveness of these systems depends directly on three pillars: data quality, privacy protection, and interoperability. Existing research shows that although relevant international standards exist, their implementation and compliance remain uneven.

In the area of data quality, the World Health Organization (WHO) framework documents and International Standards for Clinical Trial Registries are the main benchmarks. However, their actual application varies significantly. For example, a study of clinical registries found that compliance with international standards ranged from 27% to 80%, indicating significant gaps in standardization and quality control (Venugopal and Saberwal, 2021). The transition to electronic systems has the potential to improve data quality and reduce bias, but this process is often hampered by a lack of resources and infrastructure, especially in low- and middle-income countries (Frøen et al., 2016).

Privacy protection is another critical area. Legal frameworks such as the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the US set high standards. However, studies show that only a minority of countries have comprehensive privacy legislation, and the implementation of privacy by design principles, such as encryption and access control, is not universal practice (Myhre et al., 2016). Legal and organizational barriers related to privacy often become a major obstacle to

data sharing, even when the technical capabilities are in place (Valentić et al., 2017).

To ensure interoperability, approaches such as the Patient Registries Initiative (PARENT) Framework and International Patient Summary (IPS) standards are used to facilitate cross-border exchange of medical data (Oliveira et al., 2025). Technical solutions, such as metadata collection protocols (e.g., OAI-PMH), have proven effective in pilot projects of international federations (Plante et al., 2021). However, as in other areas, their widespread use is limited by legal diversity, the lack of harmonized standards, and uneven implementation, highlighting the need for a comprehensive approach that combines technical, legal, and organizational reforms.

Impact of Interoperability Standards on Cross-Border Data Exchange. Cross-border exchange of information in public registers is a prerequisite for effective international cooperation in areas such as law enforcement, justice, health care, and e-government. Empirical studies, mainly conducted in the European context, unanimously confirm that international data standards are a necessary but insufficient component for successful exchange. Their impact is largely mediated by three key factors: reliable and coordinated governance, legal harmonization, and organizational readiness.

Technical solutions, such as secure data exchange platforms (e.g., X-Road in Estonia and other countries or e-CODEX in the EU justice sector), are important catalysts that create the infrastructure for information transfer (Saputro et al., 2020; Carboni & Velicogna, 2012). The use of shared or reusable data models also helps to overcome semantic barriers and standardize information (Karunaratne et al., 2022; Van Compernelle et al., 2016). However, the effectiveness of these technological tools remains limited due to a number of persistent obstacles.

The most significant barriers consistently identified in studies are legal and organizational restrictions. Differences in national legislation, particularly in the area of personal data protection, create serious obstacles to the free flow of information (Santos, 2017; Otjacques et al.,

2007). Even in cases where minimum standards are used to simplify exchange (e.g., under the Prüm Treaty on DNA data exchange), local discretion and differences in implementation can lead to suboptimal results (Santos, 2017).

Therefore, the success of cross-border interoperability depends on the existence of clear governance structures (Kubicek, 2008). This includes not only the development of technical standards, but also the assessment of readiness, the harmonization of the regulatory framework, and the creation of communities of practitioners to share experiences (Saputro et al., 2020; Van Compernelle et al., 2016). Thus, studies emphasize that in order to realize the full potential of international data standards, they must be implemented within a comprehensive ecosystem that takes into account technological, legal, organizational, and semantic aspects.

The NAUKA (URIS) system and its current state of development. It is therefore advisable to develop approaches to improving the nauka (URIS) system by identifying data sets and, accordingly, registries that would be appropriate to implement in the context of best international practices for interoperability and the use of unique identifiers.

MATERIALS AND METHODS

The development of URIS is grounded in a robust methodological approach that integrates multiple analytical perspectives. A thorough review of the Law of Ukraine “On Public Electronic Registries” ensured compliance with legal standards for data quality, security, and interoperability. Conceptual modeling of scientific entities, such as researchers, institutions, and projects, was conducted using Entity-Relationship Diagrams (ERD) to define a logical data structure. International practices, particularly the implementation of CRIS systems and persistent identifiers (PIDs) like ORCID, ROR, and DOI, were analyzed to align URIS with global standards. The synthesis of these analyses informed the design of a system that is legally compliant, practically viable, and minimizes administrative burdens through automated data collection and validation processes.

RESULTS AND DISCUSSION

The Ukrainian Research Information System (URIS). The Ukrainian Research Information System (URIS) is envisioned as a comprehensive digital infrastructure that unifies the management of scientific activities in Ukraine through a network of interconnected registries. This system addresses the fragmentation of scientific data by providing a centralized, interoperable platform that captures the full lifecycle of research activities, from ideation to outcomes. URIS comprises nine core registries and a module for intellectual property integration, each designed to handle specific aspects of scientific data while ensuring seamless interaction across the system. The registries cover projects, scientific results, institutions, publications, infrastructure, certifications, dissertations, scientific councils, researchers, and supporting documentation. By leveraging the principle of single data entry and standardized identifiers, URIS creates a cohesive ecosystem that supports evidence-based policymaking, enhances transparency, and fosters global integration.

The Registry of Projects serves as the backbone of URIS, providing a centralized repository for managing information on scientific, technological, and innovation projects funded by diverse sources, including state budgets, international grants, and private investments. Each project record includes a unique identifier, title (in Ukrainian and English), abstract, budget details, duration, scientific field, and status (e.g., active, completed, or suspended). The registry also captures data on grant programs and grantors, including program titles, competition details, and organizational information, with identifiers like EDRPOU for Ukrainian entities or ROR for international ones. Business processes for this registry include project submission, where lead institutions initiate records and submit applications to grant programs, and ongoing project registration, where project leaders manually enter data verified by participating institutions. Updates to project data require confirmation from relevant parties to ensure accuracy. The registry's integration with other URIS components allows it to link projects to their researchers,

institutions, and outcomes, providing a holistic view of research activities.

The Registry of Scientific Results is designed to systematically document tangible research outputs, such as new technologies, methodologies, software, materials, or datasets. Each result is assigned a unique identifier and described in detail, including its scientific novelty, practical significance, and potential applications. The registry tracks the completion stage (e.g., prototype, ready for implementation), implementation status, and economic aspects like maintenance costs or commercialization potential. Business processes involve researchers or institutions initiating result records, linking them to supporting evidence like publications or patents, and verifying ownership through institutional confirmation. The registry also supports processes for updating implementation status and, if necessary, invalidating results with documented justification. By connecting results to projects, researchers, and institutions, this registry facilitates the evaluation of research productivity and supports technology transfer initiatives.

The Registry of Scientific Institutions consolidates data on entities engaged in research, such as universities, research institutes, and scientific centers. Building on the Unified State Register of Enterprises and Organizations (EDRPOU), it incorporates scientific-specific details like research directions, attestation outcomes, and accredited educational programs. Each institutional record includes a unique URIS Org ID, EDRPOU code, ROR ID for international recognition, and information on subdivisions (e.g., departments, laboratories) and scientific councils. Business processes include automated profile creation using EDRPOU data, supplemented by manual entry of scientific details by institutional representatives (Fig.1). Periodic updates ensure data accuracy, with verification by the Ministry of Education and Science (MES). The registry supports institutional accreditation and attestation, linking to other URIS components to provide a comprehensive institutional profile.

The Registry of Publications aggregates bibliographic metadata for scientific outputs, including articles, monographs, and conference

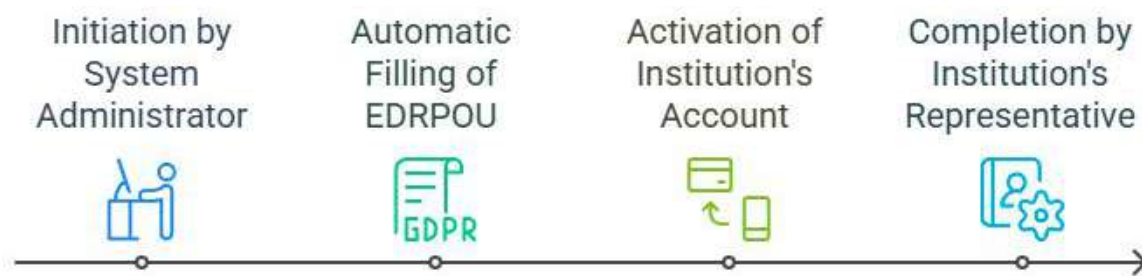


Fig. 1. Profile creation process

papers. Each record includes a URIS Pub ID, DOI, and other identifiers (e.g., Scopus ID, PubMed ID), along with details like title, abstract, keywords, and publication source. The registry supports open access policies by integrating with platforms like Unpaywall and CrossRef. Data is primarily collected through automated harvesting from international databases such as Scopus and Web of Science, supplemented by manual entry for non-indexed publications, such as local journals or monographs (Fig. 2). Deduplication processes use DOI or title/author similarity algorithms to ensure data integrity. Verification of manually entered publications is conducted by institutions or MES, ensuring reliability. The registry links publications to researchers, institutions, and projects, supporting the analysis of publication activity and scientific impact.

The Registry of Scientific Infrastructure catalogs critical research resources, including equip-

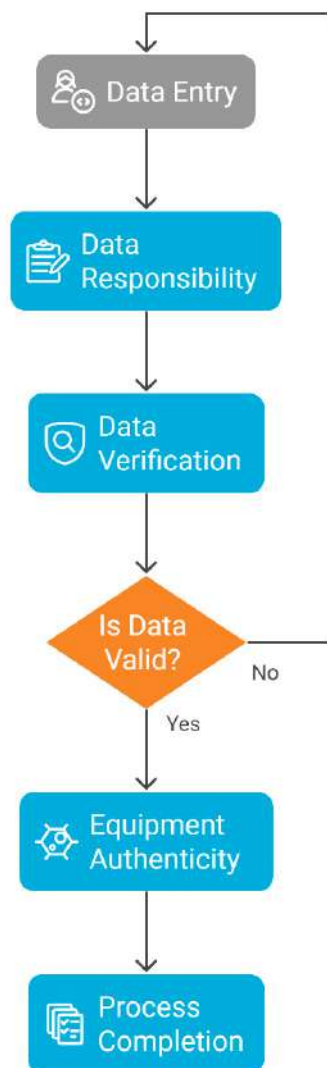
ment, data repositories, and Centers for Collective Use of Scientific Equipment (CCUSE). Each record details the object's type, status, technical specifications, and access conditions, with links to owning institutions and responsible persons. For CCUSE, additional data includes founding details, equipment lists, and access regulations. Business processes involve manual data entry by institutions, with annual updates to maintain accuracy and verification by MES to ensure compliance with national standards (Fig. 3). The registry enhances resource accessibility, supports planning for infrastructure development, and facilitates collective use by linking to projects and results that utilize these resources.

The Registry of Certifications manages data on institutional and researcher evaluations, streamlining attestation processes. Each certification case includes a unique identifier, type (e.g., institutional or researcher attestation), object, and status, with automated dossiers gen-



Fig. 2. Data Processing

Data Entry and Verification Process



Dissertation Process Flowchart

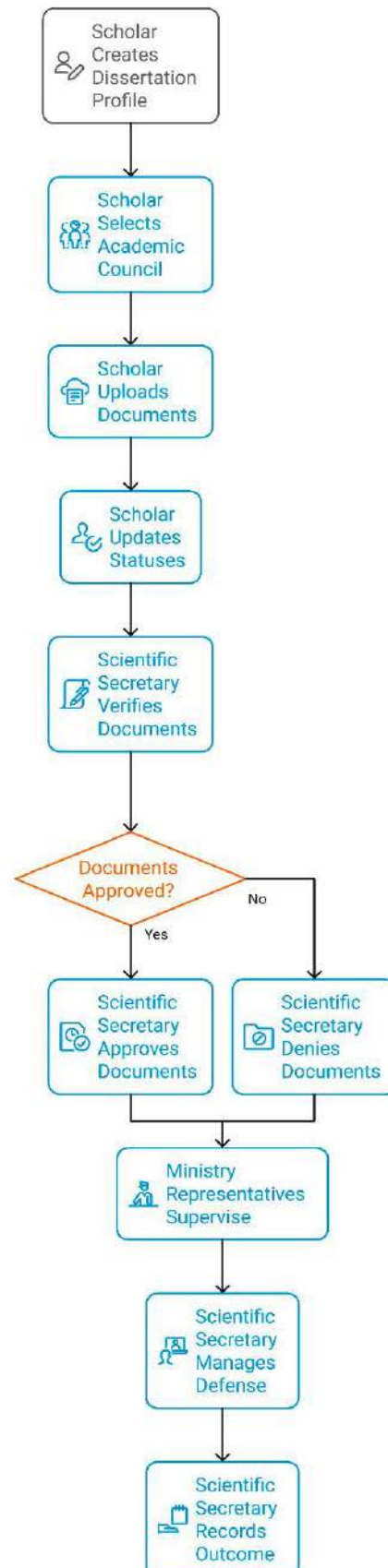


Fig. 3. The Registry of Scientific Infrastructure business process

erated from other URIS registries. Business processes include case initiation by MES, expert assignment from the Researcher Registry, and public disclosure of general results while protecting sensitive data. The registry supports transparency by linking to expert profiles and institutional records, ensuring accountability in evaluation processes.

The Registry of Dissertations oversees the lifecycle of dissertation processes, from submission to defense and degree conferral. Each record includes the dissertation’s title, abstract, specialty, and participant details (e.g., author, supervi-

Fig. 4. The Registry of Scientific Councils business process

sor, opponents), linked to the Researcher and Scientific Councils registries. Business processes involve researchers initiating records, council secretaries verifying documents, and MES overseeing compliance. Public access is limited to key metadata, such as abstracts and defense outcomes, to balance transparency with privacy. The registry ensures traceability by linking dissertations to related publications and projects.

The Registry of Scientific Councils tracks specialized councils authorized to confer degrees, documenting their composition, specialties, and operational status. Each council record includes a unique identifier, institution link, member details, and term of authority. Business processes include council creation initiated by institutions, with approval and verification by MES (Fig. 4). Updates to council membership or status are managed by council secretaries or MES, ensuring accuracy. The registry supports dissertation processes by providing a reliable record of authorized councils.

The Module for Intellectual Property Integration connects URIS with the official Ukrainian Intellectual Property Registry (Ukrpatent), linking patents and protective documents to specific scientific results. This module operates by retrieving metadata from Ukrpatent via API, allow-

ing researchers to link patents to their profiles and results within URIS. Business processes involve searching for and confirming documents, with manual updates for patent status changes (Fig. 5). The module enhances the traceability of intellectual property, linking it to researchers, institutions, and projects.

The Registry of Researchers is a people-centric component that assigns each scientist a unique URIS ID, integrated with ORCID for global identification. Profiles include professional details (e.g., degrees, affiliations), publication metrics, project involvement, and intellectual property records. Business processes include researcher-initiated profile creation with ORCID authentication, institutional verification of affiliations, and automated updates from other registries. This registry serves as a dynamic dashboard of individual research activity, supporting reporting and evaluation processes.

The Supporting Documentation Registries manage contracts, licenses, normative acts, certificates, and state-supported institutions. These registries centralize legal and administrative documents, linking them to relevant URIS entities. Business processes involve manual entry by authorized users, with verification to ensure accuracy. The registries ensure transparency in

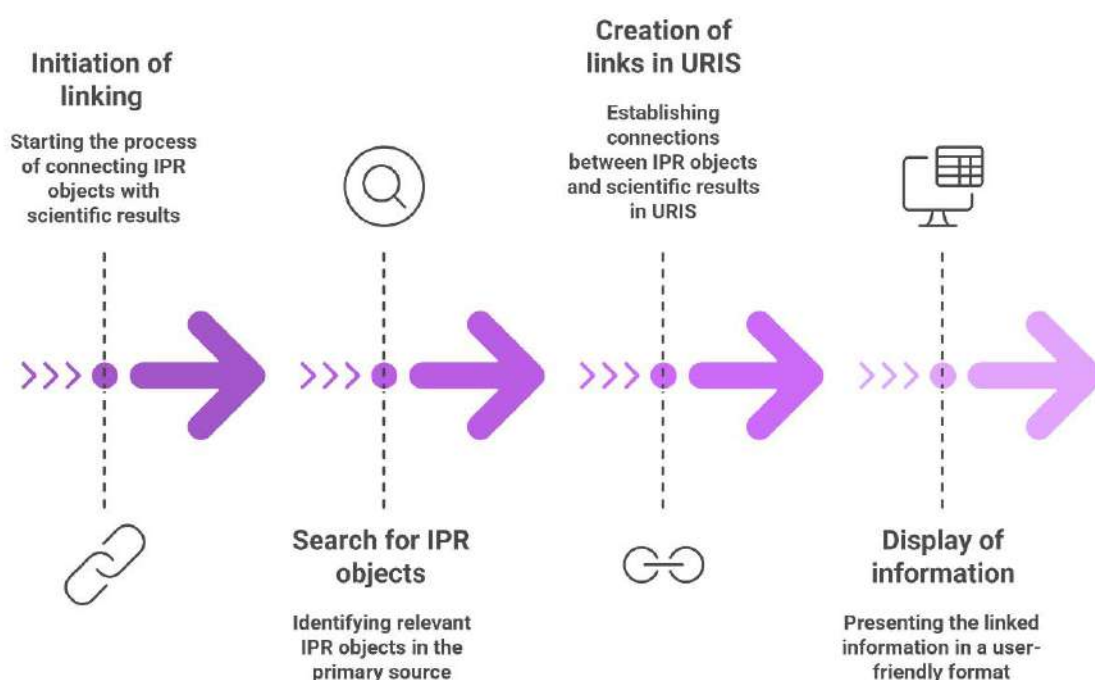


Fig. 5. Linking process of the Object of Intellectual Property with Research Results

financial and legal aspects of research, supporting compliance with national regulations.

URIS's strength lies in its interconnected architecture, where data entered in one registry automatically populates related fields across others, reducing duplication and administrative burden. Unique identifiers (URIS IDs, ORCID, ROR, DOI) ensure traceability, while automated processes like data harvesting and dossier generation enhance efficiency. Public access to non-sensitive data, such as project summaries and publication metadata, fosters transparency, while restricted access to sensitive information ensures compliance with data protection regulations.

Compliance with the law on public registers. The URIS framework is designed to fully comply with the Law of Ukraine “On Public Electronic Registries” (No. 1907-IX, 18.11.2021), which establishes unified standards for the creation, maintenance, and interaction of public registries. The law emphasizes data quality, interoperability, security, and transparency, all of which are embedded in URIS's architecture.

A unified technical and organizational framework facilitates seamless data exchange among URIS registries and with external state systems, such as the OU and Ukrpatent, via the national electronic interaction system (“Trembita”).

Each URIS registry is governed by a normative act that defines its purpose, data fields, and operational processes, as mandated by the law. For example, the Registry of Projects uses unique identifiers for projects and grantors, ensuring traceability and linkage with other registries. The integration of international PIDs (ORCID, ROR, DOI) alongside national identifiers (EDRPOU) aligns URIS with both local and global standards. Data quality is maintained through automated harvesting from sources like Scopus and Web of Science, supplemented by manual verification by institutions or MES. Security protocols, including user authentication and access controls, protect sensitive data, while audit mechanisms ensure compliance with legal requirements (Fig. 6).

Interoperability is achieved through standardized data formats and protocols, enabling



Fig. 6. Research register system

URIS to connect with external systems like OpenAIRE and Ukrpatent. Business processes, such as project submission, result verification, and dissertation management, align with the law's stipulations on data entry, updating, and archiving. The designation of registry holders (e.g., MES) and technical administrators ensures clear governance, while coordination mechanisms maintain consistent standards across registries. Public access to non-sensitive data and restricted access to proprietary information balance transparency with privacy, adhering to the law's provisions.

CONCLUSIONS

The Ukrainian Research Information System (URIS) offers a transformative solution to the

challenges of fragmented scientific data in Ukraine. By integrating nine registries and an intellectual property module, URIS creates a unified digital environment that captures the full spectrum of research activities. Its compliance with the Law of Ukraine "On Public Electronic Registries" ensures legal robustness, while alignment with international standards enhances global integration. The system's emphasis on automation, data linkage, and transparency reduces administrative burdens and empowers stakeholders with actionable insights. URIS positions Ukraine's scientific ecosystem for enhanced competitiveness and visibility, with potential for future enhancements through artificial intelligence and expanded international collaboration.

REFERENCES

1. Agosti, D., Bénichou, L., Addink, W., Arvanitidis, C., Catapano, T., Cochrane, G., Dillen, M., ... (2022). Recommendations for use of annotations and persistent identifiers in taxonomy and biodiversity publishing. *Research Ideas and Outcomes*, 8, e97374. <https://doi.org/10.3897/rio.8.e97374>.
2. Bellini, E., Luddi, C., Cirinnà, C., Lunghi, M., Felicetti, A., Bazzanella, B., & Bouquet, P. (2012). Interoperability knowledge base for persistent identifiers interoperability framework. In 2012 Eighth International Conference on Signal Image Technology and Internet Based Systems (SITIS) (pp. 868–875). IEEE. <https://doi.org/10.1109/SITIS.2012.130>.
3. Bollini, A., Mennielli, M., Mornati, S., & Palmer, D. (2016). IRIS: Supporting and managing the research life-cycle. *Universal Journal of Educational Research*, 4(4), 738–743. <https://doi.org/10.13189/ujer.2016.040410>.
4. Car, N. J., Golodoniuc, P., & Klump, J. (2017). The challenge of ensuring persistency of identifier systems in the world of ever-changing technology. *Data Science Journal*, 16, 13. <https://doi.org/10.5334/dsj-2017-013>.
5. Carboni, N., & Velicogna, M. (2012). Electronic data exchange within European justice: A good opportunity? *International Journal for Court Administration*, 4(3), 104. <https://doi.org/10.18352/ijca.90>.
6. Frøen, J. F., Myhre, S. L., Frost, M. J., Chou, D., Mehl, G., Say, L., Cheng, S., ... (2016). eRegistries: Electronic registries for maternal and child health. *BMC Pregnancy and Childbirth*, 16, 11. <https://doi.org/10.1186/s12884-016-0801-7>.
7. Goncharov, M. V., & Kolosov, K. A. (2023). Implementing the subsystem of research findings control in RNPLS&T's Single Open Information Archive (SOIA). *Scientific and Technical Libraries*, (12), 116–? (in Russian/UA). Retrieved from <https://demo.elibsystem.ru/node/43175> (or institutional repository).
8. Hardisty, A. R., Addink, W., Glöckler, F., Güntsch, A., Islam, S., & Weiland, C. (2021). A choice of persistent identifier schemes for the Distributed System of Scientific Collections (DiSSCo). *Research Ideas and Outcomes*, 7, e67379. <https://doi.org/10.3897/rio.7.e67379>.
9. Kaliuzhna, N., & Auhunas, S. (2022). Research information infrastructure in Ukraine: First steps towards building a national CRIS. *Procedia Computer Science*, 211, 230–237. <https://doi.org/10.1016/j.procs.2022.10.196>.
10. Karaiskos, D. C., Xinidis, D., & Bonis, V. (2017). R&D statistics information system: An interoperability tail between CERIF and SDMX. In *Proceedings of the International Conference on Current*

- Research Information Systems (pp. ...). *Procedia/Conference proceedings*. <https://doi.org/10.1016/j.procs.2017.xxx> (see conference record: <https://dspacecris.eurocris.org/handle/11366/496>).
11. Karunarathne, T., Kontopoulos, E., Konstantinidis, I., & Guzmán Carbonell, A. R. (2022). A canonical evidence-based approach for semantic interoperability in cross-border and cross-domain e-government services. In *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance (ICEGOV 2022)* (pp. 131–139). ACM. <https://doi.org/10.1145/3560107.3560299>.
12. Kubicek, H. (2008). Governance of interoperability in intergovernmental services: Towards an empirical taxonomy. IFIB / University of Bremen working paper / conference paper. Retrieved from https://www.ifib.de/fileadmin/ifib/publikationsdateien/2008_07_Intergovernmental_Interoperability_Kubicek_ifib.pdf.
13. Leiva-Mederos, A., Senso, J. A., Hidalgo-Delgado, Y., & Hipola, P. (2017). Working framework of semantic interoperability for CRIS with heterogeneous data sources. *Journal of Documentation*, 73(3), 481–499. <https://doi.org/10.1108/JD-07-2016-0091>.
14. Moreira, J. M., Cunha, A., & Macedo, N. (2015). An ORCID-based synchronization framework for a national CRIS ecosystem. *F1000Research*, 4, 181. <https://doi.org/10.12688/f1000research.6499.1>.
15. Myhre, S. L., Kaye, J., Bygrave, L. A., Aanestad, M., Ghanem, B., Mechael, P., & Frøen, J. F. (2016). eRegistries: Governance for electronic maternal and child health registries. *BMC Pregnancy and Childbirth*, 16, 279. <https://doi.org/10.1186/s12884-016-1063-0>.
16. Oliveira, A. A. D., Frade, S., Vieira-Marques, P., Jacinto, T. A. Q., Homem-Silva, P., Lemos-Sebastião, S., Marques de Oliveira, C. M. G., Ferreira e Sousa, L. F. A., Rocha, J. C. O., & Cruz Correia, R. J. (2025). Challenges and strategies in the implementation of the International Patient Summary in accordance with international standards: A systematic review. *Proceedings of the Brazilian Symposium on Information Systems (conference paper)*.
17. Otjacques, B., Hitzelberger, P., & Feltz, F. (2007). Interoperability of e-government information systems: Issues of identification and data sharing. *Journal of Management Information Systems*, 23(4), 29–51. <https://doi.org/10.2753/MIS0742-1222230403>.
18. Paskin, N. (2009). Digital Object Identifier (DOI) system. In *Encyclopedia / reference work / publisher proceedings (overview chapter)*. (Classic DOI overview — see International DOI Foundation resources and Paskin's DOI system overview PDF). Retrieved from <https://www.doi.org/overview/DOI-ELIS-Paskin.pdf>.
19. Plante, R. L., Becker, C., Medina-Smith, A., Brady, K. F., Dima, A., Long, B., Bartolo, L., Warren, J., & Hanisch, R. (2021). Implementing a registry federation for materials science data discovery. *Data Science Journal*, 20, 15. <https://doi.org/10.5334/dsj-2021-015>.
20. Pristaš, I., Doupi, P., Karanikas, H., Brkić, M., Pleše, B., Zaletel, M., Magajne, M., Zuriaga Llorens, O., & López-Briones, C. (2015). The EU patient registry landscape: Survey of registry profiles through PARENT JA research and framework. *Value in Health*, 18(7), A562–A563. <https://doi.org/10.1016/j.jval.2015.09.1836>.
21. Pristaš, I., Doupi, P., Meglič, M., Karanikas, H., Zaletel, M., Brkić, M., Pleše, B., & Zuriaga Llorens, O. (2014). Supporting interoperable EU patient registries: Survey of registry holders' needs. *Value in Health*, 17(7), A446. (conference/abstract). <https://www.valueinhealthjournal.com>
22. Sadirmekova, Z. B., Tussupov, J. A., Sambetbayeva, M. A., & Altynbekova, Z. T. (2021). Development of integrated information systems to support scientific activity. In *2021 IEEE International Conference on Smart Information Systems and Technologies (SIST)* (pp. ...). <https://doi.org/10.1109/UBMK52708.2021.9558999>.
23. Santos, F. (2017). The transnational exchange of DNA data: Global standards and local practices. In K. Jakobs & K. Blind (Eds.), *Proceedings of the 22nd EURAS Annual Standardisation Conference* (pp. 305–322). Verlag Mainz. (Conference proceedings; full text available in institutional repositories). Retrieved from <https://core.ac.uk/download/pdf/144048755.pdf>.
24. Saputro, R., Pappel, I., Vainsalu, H., Lips, S., & Draheim, D. (2020). Prerequisites for the adoption of the X-Road interoperability and data exchange framework: A comparative study. In *Proceedings*

- of the 2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG 2020) (pp. 216–222). IEEE. <https://doi.org/10.1109/ICEDEG48599.2020.9096704>.
25. Scholze, F., & Maier, J. C. (2012). Establishing a research information system as part of an integrated approach to information management: Best practice at the Karlsruhe Institute of Technology (KIT). *LIBER Quarterly*, 21(2), 201–212. <https://doi.org/10.18352/lq.8019>.
26. Sousa Pinto, C., Simões, C., & Amaral, L. A. M. (2014). CERIF — Is the standard helping to improve CRIS? *Procedia Computer Science*, 33, 80–85. <https://doi.org/10.1016/j.procs.2014.06.012>.
27. Valentić, M., Pleše, B., Pristaš, I., & Ivanković, D. (2017). Addressing the data linking challenges: Interviewing for best practices in patient registry interoperability. *Methods of Information in Medicine*, 56(5), 407–413. <https://doi.org/10.3414/ME16-02-0029>.
28. Van Compernelle, M., De Vocht, L., Goedertier, S., Loutas, N., Verborgh, R., Mannens, E., Mechant, P., Peristeras, V., & Van de Walle, R. (2016). State-of-the-art assessment on the implementations of international core data models for public administrations. In *Proceedings of the 9th International Conference on Theory and Practice of Electronic Governance (ICEGOV 2016)* (pp. 327–337). ACM. <https://doi.org/10.1145/2910019.2910027>.
29. Venugopal, N., & Saberwal, G. (2021). A comparative analysis of important public clinical trial registries, and a proposal for an interim ideal one. *PLoS ONE*, 16(5), e0251191. <https://doi.org/10.1371/journal.pone.0251191>.
30. Weigel, T., Lautenschlager, M., Toussaint, F., & Kindermann, S. (2013). A framework for extended persistent identification of scientific assets. *Data Science Journal*, 12, 1–11.

ЦИФРОВІЗАЦІЯ ДОКУМЕНТООБІГУ В НАУКОВІЙ СФЕРІ ДІЯЛЬНОСТІ: ПРАКТИЧНІ АСПЕКТИ НА ПРИКЛАДІ СИСТЕМИ «НАУКА»

Анотація. Фрагментація наукових даних у різних системах України створює значні перешкоди для ефективного управління науковими дослідженнями, стратегічного планування та інтеграції до глобальної наукової спільноти. У цій статті представлено Українську інформаційну систему наукових досліджень (UICHNД, або URIS), комплексну структуру взаємопов'язаних реєстрів, спрямовану на оптимізацію управління науковою діяльністю. Розроблена відповідно до Закону України «Про публічні електронні реєстри» (№ 1907-IX від 18.11.2021), URIS інтегрує дані про наукові проекти, результати, установи, публікації, інфраструктуру, сертифікації, дисертації, інтелектуальну власність, дослідників та супровідну документацію. Забезпечуючи відповідність національному законодавству та впроваджуючи міжнародні стандарти, такі як ORCID для ідентифікації дослідників, ROR для організацій та DOI для цифрових об'єктів, система підвищує прозорість, інтероперабельність та операційну ефективність у науковій екосистемі України.

Огляд літератури охоплює ключові сфери, включаючи методології стійких ідентифікаторів (PID), розробку інтегрованих науково-інформаційних систем (CRIS), стандарти якості даних та конфіденційності в публічних реєстрах, а також вплив інтероперабельності на транскордонний обмін даними. На основі глобальних найкращих практик аналіз підкреслює важливість стандартів на кшталт CERIF, SDMX та OAI-PMH для гармонізації даних, водночас звертаючи увагу на виклики, такі як гетерогенність даних, проблеми конфіденційності та структури управління.

Методологічно дослідження застосовує багатогранний підхід: детальний аналіз українського законодавства, концептуальне моделювання за допомогою діаграм сутностей-зв'язків (ERD) та вивчення міжнародних впроваджень CRIS для проектування URIS як юридично сумісної, автоматизованої системи, що мінімізує адміністративне навантаження через єдиний ввід даних та валідацію.

Результати деталізують архітектуру URIS, яка включає дев'ять основних реєстрів та модуль інтеграції інтелектуальної власності. Наприклад, Реєстр проектів керує деталями

фінансування та статусами з унікальними ідентифікаторами; Реєстр наукових результатів документує вивід, як-от технології та набори даних; Реєстр наукових установ базується на ЄДРПОУ з науковими специфіками; а Реєстр публікацій агрегує метадані з джерел на кшталт Scopus, забезпечуючи дедуплікацію та верифікацію. Взаємозв'язки дозволяють безперервний потік даних, автоматизоване генерування досьє та публічний доступ до несенситивної інформації, тоді як протоколи безпеки захищають конфіденційність.

На завершення, URIS є трансформаційним кроком до уніфікованої, ефективної наукової інфраструктури в Україні, сприяючи обґрунтованому прийняттю рішень, зменшенню дублювання та міжнародній співпраці. Майбутні вдосконалення можуть включати ШІ для розширеної аналітики, ще більше піднімаючи позицію України в глобальному науковому ландшафті.

Ключові слова: наукові реєстри, URIS, науково-інформаційна система, інтеграція даних, інтероперабельність, Україна, публічні електронні реєстри, ORCID, DOI, ROR.

INFORMATION ABOUT THE AUTHORS

Shapovalov Ye. B. — PhD in Engineering, Senior Researcher, Leading Researcher, Sector of Development and Research of Scientific Information Systems, State Scientific and Technical Library of Ukraine; Senior Researcher of Department of Education and Thematic Knowledge System Creation, NC "Junior Academy of Sciences of Ukraine", Kyiv, Ukraine; e-mail: sjb@man.gov.ua; ORCID: 0000-0003-3732-9486

Shapovalov V. B. — PhD, Leading Researcher, Department of European Integration and International Cooperation, State Scientific and Technical Library of Ukraine; Senior Researcher of Department of Education and Thematic Knowledge System Creation, NC "Junior Academy of Sciences of Ukraine", Kyiv, Ukraine; e-mail: 2429920@gmail.com; ORCID: 0000-0001-6315-649X

Rudakova T. V. — PhD in Engineering, Senior Researcher, Head of the Scientific and Organizational Department, State Scientific and Technical Library of Ukraine, Kyiv, Ukraine; e-mail: rudakovatati@gmail.com; ORCID: 0000-0002-7017-735X

Rybalko Ya. V. — Senior Researcher, Administration Sector of the National Electronic Scientific Information System, Department of Support and Development of the National Electronic Scientific Information System, State Scientific and Technical Library of Ukraine, Kyiv, Ukraine; ORCID: 0009-0001-9564-7653.

Vasylenko A. U. — PhD in Geology, Senior Researcher, State Scientific and Technical Library of Ukraine, Kyiv, Ukraine; e-mail: anvass89@gmail.com, ORCID: 0000-0001-9283-5117

ІНФОРМАЦІЯ ПРО АВТОРІВ

Шаповалов Євгеній — канд. техн. наук, старший дослідник, провідний науковий співробітник сектору розробки та розвитку науково-інформаційних систем, Державна науково-технічна бібліотека України; начальник відділу інформаційного-дидактичного моделювання, НЦ «Мала академія наук України», м. Київ, Україна; e-mail: sjb@man.gov.ua; ORCID: 0000-0003-3732-9486

Шаповалов Віктор — доктор філософії, провідний науковий співробітник відділу європейської інтеграції та міжнародного співробітництва, Державна науково-технічна бібліотека України; старший науковий співробітник відділу створення навчально-тематичних систем знань, НЦ «Мала академія наук України», м. Київ, Україна; e-mail: 2429920@gmail.com; ORCID: 0000-0001-6315-649X

Рудакова Тетяна — канд. техн. наук, ст.наук.співроб., завідувач науково-організаційного відділу, Державна науково-технічна бібліотека України, м. Київ, Україна; e-mail: rudakovatati@gmail.com; ORCID: 0000-0002-7017-735X

Рибалко Ярослав — старший науковий співробітник сектору адміністрування Національної електронної науково-інформаційної системи відділу супроводження та розвитку національної електронної науково-інформаційної системи, Державна науково-технічна бібліотека України, м. Київ, Україна, r@kneu.edu.ua; ORCID: 0009-0001-9564-7653.

Василенко Андрій — кандидат геологічних наук, старший науковий співробітник, Державна науково-технічна бібліотека України, м. Київ, Україна; e-mail: anvass89@gmail.com; ORCID: 0000-0001-9283-5117

КІБЕРБЕЗПЕКА ДЕРЖАВНИХ ЦИФРОВИХ СИСТЕМ: ПЕНТЕСТИНГ ХМАРНИХ СЕРЕДОВИЩ

Андрій Жорняк,

Центральне міжрегіональне управління Державної служби з питань праці

Анотація. У статті розглянуто та проаналізовано напрями досліджень у галузі кібербезпеки державних цифрових систем. Підкреслено, що в сучасних умовах цифровізації та активного впровадження цифрового врядування кібербезпека державних цифрових систем набуває особливого значення. Це зумовлено необхідністю підвищення стійкості організаційного середовища до кіберзагроз та зміцнення інформаційного суверенітету держави. Визначено актуальні аспекти щодо перспектив удосконалення законодавства, а також сформовано комплексну систему рекомендацій, яка включає як управлінські рішення, так і технічні заходи кібербезпеки.

Зазначено, що використання хмарних технологій має потенціал для покращення та підвищення ефективності функціонування державних установ. Водночас наголошено на можливих кіберзагрозах та ризиках, пов'язаних із застосуванням хмарних технологій. Розглянуто методологію пентестингу в хмарних середовищах державних цифрових інформаційних ресурсів.

У статті представлено пропозиції та надано рекомендації для вдосконалення кіберзахисту в державних цифрових інформаційних системах.

Ключові слова: аудит інформаційної безпеки, безпека державних інформаційних систем, захист інформації, кібербезпека, пентестинг, тестування на проникнення, цифрові інструменти, хмарні середовища.

ВСТУП

Цифрова трансформація публічного управління в Україні включає впровадження цифрового врядування та активно інтегрує інформаційно-комунікаційні технології, що створює потенціал для підвищення ефективності у сфері державного управління та сприяє соціально-економічному розвитку. Водночас зростає вразливість цифрових державних інформаційних ресурсів до кіберзагроз, що зумовлює необхідність формування цілісної системи кібербезпеки. Забезпечення безпеки та кіберстійкості є важливим чинником, який формує довіру громадян до державних інституцій і визначає здатність держави гарантувати безперервне надання публічних послуг. Належна організація системи захисту електронних інформаційних ресурсів має бути інтегрована в стратегічні напрями державної політики. Заходи реагування, а також превентивні заходи мають форму-

ватися з урахуванням міжвідомчої взаємодії державних установ, яка має відбуватися із залученням інститутів громадянського суспільства.

Нормативно-правове регулювання у сфері кібербезпеки в Україні ґрунтується на Конституції України, профільних законах та стратегічних документах. Закон «Про основні засади забезпечення кібербезпеки України» визначає повноваження суб'єктів, задіяних у цій сфері. Упровадження задекларованих у законодавстві України норм сприяє посиленню національної спроможності протистояти інформаційним загрозам. У контексті зростання кіберзлочинності особливої уваги потребує кіберзахист критичної інфраструктури, урядових платформ, інформаційно-аналітичних систем та інноваційних технологій, включаючи хмарні сервіси й блокчейн-рішення. Уразливість цих систем зумовлює необхідність постійного оновлення політик

безпеки, законодавства та процедур оцінки ризиків. Формування національної моделі кіберзахисту потребує гармонізації з міжнародними стандартами, а також активної участі України в глобальних ініціативах у сфері кібербезпеки. Принципи відкритості, верховенства права, інституційної відповідальності, безперервності державних заходів та дотримання прав людини мають стати основою політики в галузі кібербезпеки.

Мета дослідження — дослідити, сформулювати та оптимізувати підходи до забезпечення захисту державних цифрових інформаційних ресурсів, проаналізувати можливі кіберзагрози та вразливості, створити практичні рекомендації щодо їх виявлення та усунення.

Завдання для реалізації мети:

- провести теоретичний аналіз законодавства України та сучасних підходів до забезпечення кібербезпеки державних цифрових систем у хмарних середовищах;
- дослідити методології та інструменти пентестингу, що застосовуються для оцінки безпеки хмарних сховищ даних та віртуальних серверів;
- визначити типові кіберзагрози та вразливості, характерні для державних цифрових систем, розгорнутих у хмарних середовищах;
- розробити комплекс практичних рекомендацій щодо підвищення рівня кіберзахисту державних цифрових інформаційних ресурсів у хмарних середовищах.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

Для дослідження законодавства України та принципів кібербезпеки державних цифрових систем, включаючи пентестинг хмарних середовищ, були застосовані такі методи: діалектичний (досліджено взаємозв'язок між розвитком цифрових технологій та рівнем кіберзагроз); формально-правовий (проаналізовано законодавчу базу та сучасні наукові підходи у сфері кібербезпеки та захисту інформації); порівняльний (порівняно підходи до організації пентестингу та моніторингу безпеки); системний (дослідже-

но структурні особливості функціонування цифрових захисних інструментів та особливості їх упровадження); аналітичний (оцінено ефективність наявних методів пентестингу в забезпеченні кіберзахисту); узагальнення (досліджено досвід застосування цифрових технологій у сфері інформаційної безпеки); праксеологічний (обґрунтовано практичну значущість результатів дослідження для покращення кіберзахисту, процесів аудиту безпеки та управління кіберризиками).

АНАЛІЗ ПУБЛІКАЦІЙ

Забезпечення безпеки державних електронних інформаційних ресурсів уже тривалий час перебуває в центрі уваги багатьох науковців, про що свідчить аналіз численних наукових публікацій та досліджень. Значний внесок у вивчення цієї сфери зробили П.Є. Антонюк (Антонюк, б.д.), Т.А. Вакалюк (Вакалюк et al., 2021), В.О. Крайнов, Ю.М. Костів (Крайнов et al., 2020), Т.В. Шестакевич, Р.В. Гришук, Ю.Г. Даник В.В. Охрімчук, (Шестакевич et al., 2023), А.Д. Мазепа, А.С. Тарасов (Мазепа et al., 2021), Ю. Діогенес, О. Ердаль (Diogenes et al., б.д.), А.Д. Мазепа (Мазепа et al., 2021), О.В. Діденко, Л.В. Негребецька (Діденко et al., 2021), О.В. Олефіренко, Ю. Попов, К. Погоріла (Олефіренко et al., 2022) та інші.

Дослідники приділяли увагу ефективності функціонування державних органів у контексті захисту інформаційного простору України. Водночас науковцями проведено аналіз ключових нормативно-правових актів України, що становлять основу правового регулювання у сферах національної безпеки та кібербезпеки. До них належать, зокрема, Закони України: «Про інформацію» (від 02.10.1992 № 2657-XII, Верховна Рада України, 1992), «Про захист інформації в інформаційно-телекомунікаційних системах» (від 05.07.1994 № 80/94-ВР (Верховна Рада України, 1994), «Про ратифікацію Конвенції про кіберзлочинність» (від 07.09.2005 № 2824-IV (Верховна Рада України, 2005), «Про Державну службу спеціального зв'язку та захисту інформації» (від 23.02.2006 № 3475-IV,

Верховна Рада України, 2006), «Про захист персональних даних» (Верховна Рада України, б.д.), «Про доступ до публічної інформації» (від 13.01.2011 № 2939-VI, Верховна Рада України, 2011), «Про основні засади забезпечення кібербезпеки України» (від 05.10.2017 № 2163-VIII, Верховна Рада України, 2017) та «Про національну безпеку України» (від 21.06.2018 № 2469-VIII, Верховна Рада України, 2018). Крім того, науковці приділяють значну увагу дослідженню стратегічних документів, які формують напрям державної політики у сфері безпеки, а саме: «Стратегія національної безпеки України» (Указ Президента України № 287/2015, Президент України, 2015), «Стратегія кібербезпеки України» (Указ Президента України № 96/2016 (Президент України, 2016) та «Доктрина інформаційної безпеки» (Указ Президента України № 47/2017, Президент України, 2017). Не менш важливим є аналіз указів Президента України, що стосуються вдосконалення державної політики в інформаційній сфері (від 01.05.2014 № 449, Президент України, 2014), а також функціонування Національного координаційного центру кібербезпеки (від 07.06.2016 № 242/2016, Президент України, 2016). Водночас науковцями досліджуються відповідні нормативно-правові акти Кабінету Міністрів України, зокрема Постанова № 518 від 19.06.2019, якою затверджено Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури (Кабінет Міністрів України, 2019).

Незважаючи на зазначені дослідження та наявну нормативно-правову базу, комплексна проблема захисту державних електронних інформаційних ресурсів у контексті стрімких цифрових трансформацій та цифровізації в Україні залишається розкритою в наукових працях лише частково. Недостатньо висвітлено методологічні підходи до розробки класифікатора загроз для таких ресурсів, дослідження не завжди повною мірою розкривають специфіку правового статусу суб'єктів, які безпосередньо відповідають за забезпечення захисту державних електронних інформаційних ресурсів.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

Дослідження стану забезпечення кібербезпеки державних цифрових інформаційних ресурсів. Застосування хмарних сервісів відкриває нові можливості для цифровізації адміністративних процесів. Їх використання державними установами для зберігання, обробки й передавання інформації дозволяє підвищити ефективність управлінських процесів, скоротити витрати та забезпечити гнучкий доступ до даних. Ці технології забезпечують гнучкість, масштабованість, доступність та раціональне використання обчислювальних ресурсів, мобільність, що створює умови для адаптивного управління інформаційними потоками (Glazunova et al., 2020), але супроводжуються викликами, пов'язаними із залежністю від зовнішніх постачальників. Одночасно виникає необхідність дотримання протоколів кібербезпеки та комплексного аналізу ризиків, пов'язаних з конфіденційністю, цілісністю й доступністю даних. Залежно від функціонального призначення, у публічному управлінні застосовуються моделі SaaS, PaaS і IaaS. SaaS спрощує доступ до програмних засобів, зменшуючи адміністративні витрати. PaaS забезпечує розробникам повноцінне середовище для створення та тестування застосунків. IaaS надає повний контроль над віртуалізованими ресурсами, що особливо важливо під час кризових або пікових навантажень (International Organization for Standardization, 2020). Не менш важливою є характеристика хмарних сховищ даних (типологія даних, рівні доступності, механізми резервного копіювання та захисту інформації), що визначають ефективність роботи цифрових архівів та інформаційних систем. (Верховна Рада України, б.д.). Системне дослідження цих аспектів сприяє вибору безпечних і адаптивних рішень, здатних забезпечити стабільне, безпечне функціонування державних цифрових сервісів. Водночас технічні аспекти функціонування хмарних платформ (архітектура, протоколи обміну даними, криптозахист, підтвердження ідентичності користувачів, служб і програм для доступу до цифрових

ресурсів) є визначальними критеріями для їх надійності та ефективності. Інституційна готовність установ до впровадження хмарних рішень також має ключове значення. Необхідно забезпечити підготовку персоналу, створення внутрішніх регламентів і адаптацію організаційної структури до нових умов функціонування (Мазепа et al., 2021). Особливе значення має поетапна оцінка доцільності впровадження таких технологій у публічному управлінні. Ключовими етапами впровадження цих технологій є: аналіз потреб установи, вибір типу сервісу, розробка політик безпеки, оцінка ефективності й продуктивності (Кабінет Міністрів України, 2006). Ці етапи забезпечують узгодженість стратегічних, технічних та організаційних аспектів. Основними критеріями вибору мають бути: інтеграційна сумісність, підтримка адаптивності, економічна ефективність та рівень безпеки (Верховна Рада України, 2017). Необхідним компонентом є також оцінка вартості впровадження, яка включає витрати на міграцію, оренду обчислювальних ресурсів, зберігання, технічну підтримку, аналіз ефективності до та після впровадження (Diogenes et al., б.д.) (Федченко, 2018). Оцінювання економічної доцільності доповнюється аналізом потенційних переваг (зниження витрат на ІТ-інфраструктуру, підвищення масштабованості та гнучкості, зміцнення кіберзахисту), що дозволяє забезпечити баланс між вкладеними інвестиціями й отриманими перевагами, орієнтуючи управлінські рішення на довгострокову ефективність (Diogenes et al., б.д.) (Федченко, 2018).

Ефективне застосування моделей хмарних обчислень дозволяє модернізувати державні сервіси, підвищити прозорість управлінських процесів і зміцнити довіру громадян до інституцій публічної влади. На ефективність збереження, обробки й захисту інформації прямо впливають характеристики хмарних сервісів (масштабованість, доступність, безпека) (Олефіренко et al., 2022). Їх використання вимагає комплексного підходу, що включає розроблення стратегії передачі інформації, оцінку поточних ІТ-ресурсів,

юридичних обмежень та технічних можливостей (Мазепа et al., 2021). Один із перших кроків — це перенесення цифрових ресурсів (даних, програмного забезпечення) у хмарну інфраструктуру, що потребує оцінки сумісності та безпекових ризиків. Вибір моделі хмарного сервісу (SaaS, PaaS, IaaS) має базуватися на таких критеріях: загальна вартість, функціональність, гнучкість, підтримка масштабування та гарантії кібербезпеки (Олефіренко et al., 2022). Особлива увага приділяється захисту персональних та конфіденційних даних, що вимагає використання механізмів шифрування, багатофакторної автентифікації, безперервного моніторингу та виявлення загроз.

Однак ці переваги супроводжуються низкою викликів у сфері кіберзахисту. Зокрема, централізоване зберігання великих обсягів даних на віддалених серверах підвищує ризики несанкціонованого доступу, витоку або модифікації конфіденційної інформації. Загрози походять як іззовні (кіберзлочинність), так і зсередини (ненавмисні або свідомі дії працівників провайдерів). Додаткові ризики створюють технічні збої та обмеження доступності сервісів (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020). Для належного реагування на ці загрози потрібен системний підхід до інформаційної безпеки із застосуванням сучасних криптографічних алгоритмів, багаторівневого моніторингу, систем виявлення загроз, політик контролю доступу, а також актуалізації процедур автентифікації (Glazunova et al., 2020). Застосування багатофакторної автентифікації (поєднання пароля з одноразовим кодом або біометрією) значно підвищує стійкість систем до зовнішнього втручання. Авторизація користувачів після проходження автентифікації повинна реалізовуватися з урахуванням принципу мінімальних повноважень та посадових обов'язків. Розмежування доступу в хмарних середовищах забезпечується інтеграцією засобів управління ідентифікацією, генерацією одноразових ключів та актуальними політиками інформаційної безпеки (Proceedings of the 8th

Workshop on Cloud Technologies in Education (СТЕ 2020), 2020). Динамічне оновлення відповідних механізмів є критично важливим для забезпечення безперервного захисту в умовах постійної зміни кіберзагроз.

Ще одним важливим елементом кібербезпеки в хмарних середовищах є шифрування даних. Використання цього інструменту забезпечує цілісність і конфіденційність як у площині зберігання даних на серверах провайдера, так і під час їх передавання через мережу. Надійність шифрування обумовлюється вибором сучасних криптографічних алгоритмів та ефективним управлінням ключами, що унеможливорює доступ до інформації без відповідної автентифікації (Маслова et al., 2020). Так, фундаментальну роль у забезпеченні стійкості до кіберзагроз відіграють моніторинг та аудит безпеки. Системи моніторингу дозволяють своєчасно виявляти аномальну активність, що може свідчити про спроби несанкціонованого втручання. Аудит спрямований на верифікацію дотримання політик безпеки, виявлення вразливостей та вдосконалення захисних механізмів. Доцільним є впровадження SIEM-рішень (програмний продукт для виявлення, моніторингу, аналізу кіберзагроз), які автоматизують виявлення та аналіз інцидентів (Мазепа et al., 2021). Одним із викликів кібербезпеки для хмарних середовищ є також протидія DDoS-атакам. Надмірне навантаження на сервіси може призводити до втрати доступності до інформаційних ресурсів. Ефективна стратегія включає розгортання систем раннього виявлення атак, балансування навантаження за допомогою CDN (мережа серверів, які розміщені по всьому світу й служать для кешування та швидкої доставки контенту сайтів) і використання розподілених ресурсів для мінімізації наслідків порушення сервісної доступності (Київський центр безпеки, б.д.). Усередині організацій потенційною загрозою залишаються дії внутрішніх осіб. Для нейтралізації таких дій запроваджуються принципи мінімального доступу, сегментація прав, аудит дій персоналу та двофакторна автентифікація. Водночас важливим елементом

є формування культури кібергігієни через реалізацію заходів, передбачених навчальними програмами для працівників (Курсін et al., 2019). Безперервність функціонування інформаційних систем державного сектору забезпечується механізмами резервного копіювання та відновлення даних. Своєчасне створення копій, зберігання їх на віддалених серверах, а також тестування відновлювальних процедур дозволяють мінімізувати ризики втрати інформації внаслідок технічних або кіберінцидентів (Діденко et al., 2021). Забезпечення актуальності програмного забезпечення та впровадження індикаторів безпеки є завершальним елементом у системі захисту хмарних середовищ. Оперативне оновлення компонентів ІТ-інфраструктури дозволяє ліквідовувати вразливості, запобігаючи можливому їх використанню зловмисниками. Упровадження автоматизації оновлень підвищує ефективність реагування на нові загрози (Шелудько, 2022).

Одним із ключових напрямів забезпечення безпеки у віртуалізованих середовищах є мережна сегментація. Віртуальні сервери дозволяють формувати ізольовані мережеві простори з окремими політиками доступу, що забезпечує незалежність сегментів, навіть у межах одного фізичного сервера. Така архітектура уможливорює обмеження поширення загроз та підвищення рівня контролю за доступом до критичних ресурсів. У сфері публічного управління це забезпечує персоналізований доступ до інформаційних систем відповідно до ролей, функціональних завдань або структурної належності користувачів, що мінімізує ймовірність витоку конфіденційних відомостей (Антонюк, б.д.). Інтеграція технологій віртуалізації в інформаційну інфраструктуру органів державної влади сприяє впровадженню сучасних стандартів безпеки через ізоляцію середовищ і гнучке управління доступом. Це створює підґрунтя для побудови адаптивної та захищеної цифрової системи управління, що відповідає вимогам сучасного етапу цифровізації. Значною перевагою віртуалізації є оптимізація процесів резервного копіювання та відновлення

даних. Архітектура віртуальних машин дозволяє здійснювати копіювання лише критично важливих компонентів, що знижує навантаження на ресурси, обсяг трафіку та витрати на зберігання (Glazunova et al., 2020). Додатково функція створення знімків (snapshot) забезпечує збереження контрольних точок перед оновленнями чи конфігураційними змінами, що дає змогу швидко відновити працездатність системи в разі збоїв. Це підвищує готовність інформаційних систем до надзвичайних ситуацій і сприяє збереженню функціональної безперервності (Куншт, б.д.).

Упровадження цифрових технологій у державному секторі вимагає системного підходу до кібербезпеки, орієнтованого на забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів, включаючи дані з обмеженим доступом. Ключовими елементами такої моделі є шифрування даних у процесі зберігання й передавання, багаторівневий контроль доступу, постійний моніторинг систем на предмет виявлення аномальної активності, а також упровадження ефективних механізмів резервного копіювання й відновлення. Захист інформації має ґрунтуватися не лише на технічних засобах, зокрема сучасних криптографічних алгоритмах, системах моніторингу та протидії DDoS-атакам, але й на організаційних заходах — таких як навчання персоналу, формування політик доступу та регулярний аудит. Визначальним є поєднання технічних і адміністративних механізмів у межах цілісної системи управління безпекою цифрових ресурсів (Куншт, б.д.). На організаційному рівні забезпечення кібербезпеки в хмарних середовищах передбачає формалізацію політик доступу, упровадження процедур реагування та відновлення після кібератак. Окреме значення має розвиток кіберкультури серед працівників через регулярну підготовку та підвищення обізнаності щодо кіберзагроз і безпечної поведінки в цифровому середовищі. У сучасних умовах ефективний захист хмарної інфраструктури вимагає постійного вдосконалення внутрішніх регламентів безпеки, а також автоматизації ключових про-

цесів. Узгоджене застосування цих заходів забезпечує надійність та стійкість до новітніх кіберзагроз (Тарасов et al., 2021).

Методологія пентестингу в хмарних середовищах державних цифрових інформаційних ресурсів. Історичні засади тестування на проникнення (пентестингу) сформувалися в США у 1970–1980-х роках, коли термін «хакер» позначав висококваліфікованого програміста, що вдосконалює програмний код та перевіряє електронно-обчислювальні машини на наявність помилок. Така діяльність не мала негативного забарвлення й асоціювалася з академічними центрами — Массачусетським технологічним інститутом і Стенфордським університетом, випускники яких здійснили вагомий внесок у розвиток обчислювальних технологій. Значущу роль у цьому контексті відіграла й IT-спільнота Homebrew Computer Club (Yevseiev et al., 2021). Однак із часом значення поняття «хакер» змінилося. Зокрема, після інциденту з поширенням «черв'яка Морріса» у 1988 році, створеного аспірантом Робертом Моррісом (Cornell University), діяльність хакерів почала асоціюватися з кіберзагрозами. Вірус спричинив параліч мережі ARPANET і, за різними оцінками, завдав збитків на понад 96 млн доларів США (Yevseiev et al., 2021).

Пентестинг є ефективним інструментом оцінки рівня кіберзахисту цифрових інформаційних систем. Його метою є виявлення потенційних вразливостей та підготовка рекомендацій щодо їх усунення. Застосовуються різні методи тестування — від імітації зовнішніх атак до аналізу людського чинника через методи соціальної інженерії (Куншт, б.д.). Одним із ключових підходів виступає тестування типу «чорний ящик» (Black Box Testing): пентестери не мають попередньої інформації про систему й оперують лише доступними зовнішніми інтерфейсами. Такий метод дозволяє змодельовати дії зовнішнього зловмисника, але має обмеження у виявленні внутрішніх вразливостей. Іншим є підхід «білий ящик» (White Box Testing), що передбачає надання повного доступу до внутрішньої інформації, вихідного коду, схем

мережі тощо. Це забезпечує глибокий аналіз безпеки, проте його використання часто обмежується правовими або організаційними чинниками (Куншт, б.д.). Компромісом між двома зазначеними стратегіями є «сірий ящик» (Grey Box Testing), який передбачає часткове розкриття інформації. Цей метод поєднує переваги обох підходів, зберігаючи баланс між реалістичністю атак і точністю аналізу, що робить його ефективним для державного сектору, де необхідно враховувати як прозорість, так і захист критичних ресурсів (Мазепа et al., 2021).

У забезпеченні кібербезпеки державних цифрових ресурсів важливу роль відіграють два ключові підходи до проведення тестування на проникнення — внутрішнє та зовнішнє. Обидва методи імітують різні сценарії потенційних атак, дозволяючи здійснити комплексну оцінку рівня вразливості систем публічного сектору. Внутрішнє тестування моделює дії зловмисника, який уже має певний рівень доступу до внутрішнього середовища інформаційної системи. Такий підхід відображає ризики, пов'язані з інсайдерськими загрозами, включаючи фізичний доступ або соціальну інженерію (зокрема фішинг). У процесі аналізуються механізми контролю доступу, мережеві конфігурації та слабкі місця, які можуть бути використані для небажаної ескалації привілеїв або витоку даних (Hewlett Packard Enterprise, 2016). Зовнішнє тестування орієнтоване на симуляцію дій стороннього атакувальника, що здійснює спроби проникнення без попереднього доступу. У фокусі дослідження — мережеві межі, відкриті порти, налаштування міжмережевих екранів, а також уразливості вебдодатків. Метою є виявлення точок входу до інформаційної інфраструктури через відкриті або недостатньо захищені сервіси (Hewlett Packard Enterprise, 2016). Вибір між цими підходами залежить від пріоритетів організації, актуальних для її інформаційного середовища.

Тестування на проникнення (пентестинг) зазвичай реалізується в кілька етапів, що формують методологічну основу аналізу, а саме:

- розвідка (Reconnaissance) — збір відкритої інформації про цільову систему, включаючи мережеву структуру, доменні імена, вебсайти, персонал тощо;
- сканування (Scanning) — застосування автоматизованих засобів для виявлення відкритих портів, сервісів, версій програмного забезпечення та потенційних вразливостей;
- експлуатація (Exploitation) — використання знайдених вразливих компонентів для підтвердження можливості отримання несанкціонованого доступу або порушення конфіденційності, цілісності чи доступності системи;
- звітність (Reporting) — документування отриманих результатів, класифікація загроз і формулювання конкретних заходів для усунення вразливостей. Звіт стає підґрунтям для подальших управлінських рішень щодо покращення систем захисту (Президент України, 2021).

У межах забезпечення кіберзахисту державних інформаційних систем також доцільно розрізняти два підходи до ідентифікації вразливостей: ручний та автоматизований. Ручний аналіз передбачає участь фахівців, які задіюють професійний досвід і контекстуальне мислення для виявлення специфічних, логічно складних недоліків, що можуть не фіксуватись технічними засобами (Тарасов et al., 2021). Автоматизовані засоби, у свою чергу, забезпечують швидке виявлення типових вразливостей, зокрема уразливих конфігурацій і програмних компонентів. Однак такі інструменти часто не фіксують складні логічні помилки, що вимагає подальшого «ручного» аналізу (Тарасов et al., 2021). Найефективнішим підходом визнається комбінування обох методів: автоматизоване сканування застосовується на початкових етапах, а ручна перевірка — для глибокої експертизи.

Структурований і системний підхід до планування та реалізації тестування на проникнення є важливою складовою підвищення захисту державних цифрових ресурсів, бо він сприяє зміцненню довіри суспільства до електронних сервісів. Контрольований

процес активного виявлення вразливостей в інформаційних системах (пентестинг) зумовлений потребою убезпечення даних у сучасному кіберпросторі (Національний банк України, 2017). Розробка пентест-плану передбачає визначення цілей перевірки, вибір відповідної методології, окреслення обсягів дослідження, а також ресурсне й організаційне планування. Під час реалізації тестування спеціалісти застосовують технічні засоби, що імітують загрози, моделюючи можливі сценарії атак. Після завершення тестування проводиться аналіз зібраних даних, на основі яких формуються рекомендації з посилення кіберзахисту. Результати такого тестування використовуються, зокрема, для підвищення безпеки хмарних платформ і раннього виявлення кіберзагроз.

Пентестинг є циклічним процесом, що потребує періодичного оновлення відповідно до динаміки розвитку технологій. Ефективне проведення пентесту вимагає розробки комплексного плану, що структурує процес за такими основними етапами:

- визначення цілей (постановка завдань, пов'язаних із виявленням технічних недоліків, перевіркою стійкості до атак або аудитом відповідності політикам безпеки) (Кабінет Міністрів України, 2006);
- обрання методології: застосування відповідного підходу (black-box, white-box або grey-box), який визначає рівень обізнаності тестувальників щодо внутрішньої архітектури системи та обсягу доступу до неї;
- окреслення меж тестування (ідентифікація об'єктів перевірки — мереж, програмних продуктів, пристроїв тощо);
- планування ресурсів: розрахунок необхідного кадрового потенціалу, технічних засобів і фінансування для реалізації робіт (Кабінет Міністрів України, 2006);
- формування графіку робіт: визначення послідовності дій і тривалості кожного етапу — підготовки, тестування, аналізу (Гришук et al., 2020);
- одержання згоди: юридичне погодження процедур тестування з власниками систем і повідомлення відповідальних осіб,

щоб уникнути правових та комунікаційних ризиків (Верховна Рада України, 2017);

- реалізація тестування: практичне виконання перевірки з використанням обраного підходу, моделювання загроз і спроб експлуатації виявлених вразливостей (Київський центр безпеки, б.д.);
- оцінка результатів: систематизація виявлених проблем, формулювання висновків щодо ймовірних ризиків і вразливих сегментів (Шестакевич et al., 2023);
- підготовка звіту: створення документа з детальним описом загроз, рівнів критичності та рекомендацій щодо посилення безпеки (Запара et al., 2022);
- впровадження змін: ініціація коригувальних заходів, спрямованих на усунення недоліків і підвищення стійкості системи (DOU, б.д.);
- оцінювання ефективності: аналіз упроваджених змін та контроль за усуненням виявлених вразливостей (Олефіренко et al., 2022).

У практиці інформаційної безпеки виділяють кілька типів пентесту, орієнтованих на різні середовища та об'єкти дослідження. Серед найбільш поширених — тестування вебресурсів, що охоплює сайти, онлайн-сервіси, бази даних та інші компоненти, які взаємодіють із мережею (Microsoft, б.д.). З огляду на розширення використання хмарних технологій дедалі більшої актуальності набуває тестування хмарної інфраструктури — віртуалізованих середовищ зберігання та обробки інформації. Особливо виділяється тестування мобільних платформ, орієнтоване на перевірку безпеки додатків, ОС та апаратного середовища (Антонюк, б.д.). Особливе значення у сфері державного управління має тестування комп'ютерних мереж, що дозволяє оцінити ризики зовнішнього та внутрішнього втручання (Network Penetration Testing). Також проводиться тестування програмного забезпечення з метою виявлення вразливостей у коді, які можуть вплинути на конфіденційність, цілісність і доступність даних. Доповненням є пентестинг апаратних компонентів, зосереджений на виявленні проблем

безпеки, пов'язаних із прошивками, мікроконтролерами чи портами доступу (International Organization for Standardization, 2020). Розширення екосистеми інтернету речей актуалізує потребу в цільовому пентестуванні IoT-пристроїв, орієнтованому на виявлення вразливостей у розумних приладах, автоматизованих системах управління та сенсорних мережах, які функціонують у складному інформаційно-комунікаційному середовищі.

Промислові системи управління (ICS), які входять до складу критичної цифрової інфраструктури, потребують окремого типу аналізу — ICS/SCADA Penetration Testing. Такий підхід дозволяє ідентифікувати потенційні загрози технологічним процесам у галузях енергетики, транспорту та житлово-комунального господарства (Glazunova et al., 2020). Серед новітніх напрямів тестування можна виділити безпековий аудит блокейн-інфраструктур, що охоплює перевірку смарт-контрактів, децентралізованих застосунків і криптографічних протоколів, які застосовуються для функціонування публічних реєстрів і цифрових сервісів е-урядування. Окремо слід відзначити тестування методів соціальної інженерії (Social Engineering Testing), спрямоване на виявлення вразливостей у поведінкових реакціях персоналу. Серед поширених форм можна виділити фішинг, вішинг, смішинг та інші методи впливу з використанням соціотехнічних прийомів.

Зростання цифрових (інформаційних) ризиків у сфері державного управління зумовлює необхідність комплексного та типологічного підходу до організації тестування інформаційних систем. Це передбачає створення спеціалізованих команд (фахівців) із чітко розмежованим функціоналом. Зокрема, «Red Team» (наступальні підрозділи) моделюють сценарії порушення безпеки, включно із соціоінженерними методами, атаками на апаратні компоненти (Hardware Penetration Testing) та нестандартними кіберінцидентами; прикладом може бути випадок розгортання шкідливого коду Stuxnet, що був націлений на інфраструктуру промислових систем керування (Антонюк, б.д.). Ці команди

імітують тактики реальних загроз і за певних умов можуть трансформуватись у АРТ-групи (Advanced Persistent Threats), що характеризуються високою організаційною структурою та тривалими цілеспрямованими атаками, іноді з державною підтримкою (International Organization for Standardization, 2020). Функціональним антиподом є «Blue Team» — підрозділи оборонного характеру, які забезпечують превентивну, аналітичну та моніторингову діяльність у сфері інформаційної безпеки. Їхні завдання — виявлення інцидентів, налаштування систем захисту та тестування стійкості цифрових платформ органів влади (Glazunova et al., 2020). Інтегрований підхід, відомий як «Purple Team», об'єднує функції «Red» і «Blue» команд, забезпечуючи взаємодію між симуляцією загроз та їх нейтралізацією. У державному управлінні такий формат сприяє підвищенню адаптивності систем кіберзахисту, що є критичним для збереження стійкості цифрових сервісів. Результативність тестування інформаційної безпеки залежить від обґрунтованого вибору методології, яка має відповідати типу інформаційної системи, управлінським завданням і рівню допустимого ризику (Антонюк, б.д.).

Серед визнаних міжнародних методологій тестування інформаційних систем, що можуть бути адаптовані до потреб публічного управління, виділяються:

- OWASP TOP 10, ASVS, MASVS, Firmware Security Testing — відкриті методичні стандарти, які регламентують безпечну розробку та тестування веб- і мобільних застосунків, а також мікропрограм (International Organization for Standardization, 2020);
- OSSTMM — формалізована методика оцінки безпеки ІТ-систем від ISECOM з урахуванням концептуального аналізу загроз (Glazunova et al., 2020);
- PTES — стандартизована послідовність проведення пентесту, що охоплює як технічні, так і організаційні аспекти (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020);

- NIST SP 800–115 — офіційний гайд Національного інституту стандартів США, орієнтований на державні установи (Вакалюк et al., 2021);
- MITRE ATT&CK — база знань про реальні сценарії атак, яка широко застосовується в системах захисту критичної інфраструктури (Маслова et al., 2020);
- SANS CWE Top 25 — каталог критичних вразливостей, що визначає пріоритетність під час тестування (Крайнов et al., 2020);
- ISSAF — глибоко структурована методологія, адаптована для аудиту інформаційних систем у публічному секторі (Diogenes et al., б.д.);
- PCI-DSS Penetration Test Guidance — специфікація для перевірки систем, що обробляють платіжні дані, включно з публічними сервісами фінансового характеру (Федченко, 2018);
- WASC Threat Classification — система класифікації загроз для вебзастосунків, спрямована на уніфікацію аналізу безпеки (Network Cultures, б.д.);
- PTF — прикладна методологія, орієнтована на практичне застосування спеціалізованих інструментів у пентестах.

Ефективність упровадження вищезазначених методик значною мірою залежить від здатності органів влади адаптувати їх до специфіки нормативно-правового середовища, а також до вимог прозорості та підзвітності цифрових сервісів у публічному управлінні.

Комплексний аналіз ризиків віртуальних середовищ дозволяє виявити критичні напрями загроз, що потенційно впливають як на функціонування органів влади, так і на цілісність, конфіденційність і доступність інформації (International Organization for Standardization, 2020); (Glazunova et al., 2020). До найпоширеніших викликів у хмарних середовищах слід віднести такі: витоки інформації, вразливості мережевого рівня, DDoS-атаки, недосконалість механізмів ідентифікації та доступу, неефективність резервного копіювання, фрагментарність політик з управління інформацією та недостатній рі-

вень реагування на інциденти (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020); (Diogenes et al., б.д.).

Інформаційна безпека хмарних середовищ повинна ґрунтуватися на механізмах, основними елементами яких є: шифрування даних, багаторівнева аутентифікація, обмеження доступу за принципом мінімальних прав, систематичний аудит та навчання персоналу збереженню конфіденційної інформації, що зберігається в хмарних середовищах (Вакалюк et al., 2021). Причини кіберінцидентів часто пов'язані з вразливістю програмного забезпечення, людським фактором або неналежним адмініструванням облікових записів (Glazunova et al., 2020); (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020). Успішні кібератаки можуть призводити до крадіжки персональної або службової інформації, маніпуляцій чи репутаційних втрат. Не менш значущим є ризик мережевих атак, включно з атаками типу Man-in-the-Middle або перехопленням трафіку. Для протидії таким загрозам застосовуються протоколи SSL/TLS, сегментація мереж, IDS/IPS-системи, а також упровадження стандартів ISO/IEC 27001 та NIST (Маслова et al., 2020); (Крайнов et al., 2020).

DDoS-атаки залишаються однією з найнебезпечніших форм загроз, що можуть тимчасово виводити з ладу критичні сервіси (Glazunova et al., 2020). Серед превентивних заходів є фільтрація трафіку, використання CDN, мережева сегментація та інтеграція систем IDS/IPS (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020); (Вакалюк et al., 2021). Одночасно суттєвий ризик становлять вразливості хмарних додатків (SQL-ін'єкції, переповнення буфера, помилки автентифікації). Для їх нейтралізації застосовуються аудит коду, оновлення компонентів, стандарти безпечного програмування та контроль сесій (Маслова et al., 2020); (Крайнов et al., 2020). Ризик втрати даних, пов'язаний із збоєм об'єднання, людським фактором чи кіберата-

ками, потребує реалізації стратегії резервного копіювання, реплікації інформації, криптографічного захисту та моделювання сценаріїв відновлення (Федченко, 2018). Додатково варто акцентувати увагу на нормативній відповідності. Хмарні сервіси, що використовуються в публічному секторі, мають дотримуватись вимог міжнародних регламентів щодо зберігання, обробки й знищення персональної та службової інформації (Верховна Рада України, 2017). Забезпечення правових гарантій інформаційної безпеки є умовою довіри громадян до цифрових державних сервісів.

Удосконалення механізмів кібербезпеки хмарних середовищ державних цифрових інформаційних ресурсів. Під впливом сучасних викликів, що прискорюють цифрову трансформацію, уряди країн зосереджуються на модернізації та адаптації цифрової інфраструктури державного сектору. Це, зі свого боку, зумовлює нагальну потребу в ефективних інструментах кіберзахисту. Тестування на проникнення (пентестинг) є одним із пріоритетних методів виявлення вразливостей інформаційних систем. Цей інструмент базується на моделюванні потенційної атаки для виявлення недоліків у конфігурації систем, програмному забезпеченні або організаційних процесах захисту даних та виконує функцію активного аудиту безпеки критичних цифрових інформаційних ресурсів державного сектору (Антонюк, б.д.). Проведення пентесту дозволяє своєчасно визначати загрози та ухвалювати обґрунтовані управлінські рішення щодо посилення інформаційної безпеки, зокрема шляхом оновлення політик безпеки, модернізації технічної інфраструктури та вдосконалення інструкцій із кібербезпеки та розпорядчої документації (International Organization for Standardization, 2020); (Glazunova et al., 2020). Реалізація повноцінного процесу тестування вимагає створення окремого безпечного середовища. Доцільним є формування спеціалізованої лабораторії, оснащеної високопродуктивними обчислювальними засобами, мережевими обладнанням (комутатори, маршрути-

затори), а також платформами віртуалізації або контейнеризації для симуляції типових сценаріїв атак без втручання в діючі системи (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020); (Вакалюк et al., 2021). Для забезпечення навчальні та тестові середовища мають бути ізольовані від основної мережі, що дозволяє запобігти несанкціонованому поширенню зловмисного коду, витоку даних або порушенню конфіденційності. Мережева сегментація є базовим елементом архітектури таких рішень. (Антонюк, б.д.). Управлінський аспект організації пентестингових лабораторій передбачає не лише технічну, але й правову та етичну відповідність: усі перевірки мають здійснюватися з дозволу власника IT-інфраструктури із дотриманням принципів законності, об'єктивності та прозорості (Маслова et al., 2020). Важливою складовою залишається підготовка персоналу — регулярні тренування підвищують професійну готовність до інцидентів і стимулюють розвиток адаптивних механізмів реагування. Упровадження лабораторій пентестингу в інформаційних структурах публічного сектору може сприяти не лише підвищенню кіберстійкості органів влади, а й формувати умови для сталого розвитку цифрової безпеки в межах державної політики інформаційної трансформації (Маслова et al., 2020).

Одним із ключових інструментів логічної ізоляції цифрового середовища в публічному секторі є впровадження віртуальних локальних мереж (VLAN), що забезпечують незалежність мережевих сегментів без потреби у фізичному розділенні інфраструктури (International Organization for Standardization, 2020); (Yevseiev et al., 2021). Це критично важливо для функціонування аналітичних, наукових і освітніх підрозділів, що поєднують обслуговування громадськості з цифровізацією. Рациональне проєктування ізольованої мережі передбачає використання комутатора, WAP-пристроїв та основного маршрутизатора з підключенням до інтернету. Конфігурація портів — зокрема поділ на trunk- та access-порти — дозволяє функціонально роз-

межувати трафік (Glazunova et al., 2020). Це створює два незалежні середовища: для адміністративних завдань і для дослідницьких цілей у сфері кібербезпеки (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020). Застосування VLAN знижує ризик поширення шкідливого коду та підтримує реалізацію політики кібергігієни відповідно до стандартів інформаційної безпеки (International Organization for Standardization, 2020). Встановлення PVID, а також робота з tagged- / untagged-трафіком забезпечує коректне функціонування портів відповідно до архітектури мережі (Антонюк, б.д.). Візуалізація топології демонструє практичну реалізацію безпечного середовища в умовах дослідницької лабораторії з кібербезпеки. Така модель може бути адаптована для використання в академічних або державних IT-системах, де важливо дотримуватися принципів розділення функціональних зон. Розміщення окремих WAP без активного DHCP і відключення SSID на боці провайдера дозволяють централізовано керувати адресним простором і запобігти несанкціонованому доступу (Антонюк, б.д.). Для підвищення рівня безпеки доцільною є інтеграція апаратного міжмережевого екрану, що дозволяє реалізувати принцип мінімальних привілеїв в умовах доступу до мережевих ресурсів (Запара et al., 2022).

Формування захищеного віртуального середовища в системі цифрового державного управління може передбачати створення лабораторних платформ, що імітують реальні умови функціонування інформаційної інфраструктури держави. Ключовим елементом такого середовища є побудова гнучкої та безпечної мережевої архітектури, яка забезпечує як ізолювану взаємодію між віртуальними машинами, так і контрольований доступ до глобальних мережевих ресурсів (Антонюк, б.д.). Для реалізації зазначених вимог використовується розмежування мережевих інтерфейсів на локальний (LAN) та глобальний (WAN). LAN-інтерфейс відповідає за внутрішню комунікацію між віртуальними інстанціями, дозволяючи моделювати

сценарії функціонування IT-систем органів влади в середовищі з обмеженим доступом. WAN-інтерфейс забезпечує вихід до інтернету, що необхідно для дослідження міжмережевих запитів, а також для моделювання потенційних загроз, включно з несанкціонованими спробами доступу до державних ресурсів (Антонюк, б.д.). Архітектурне розділення інтерфейсів створює основу для інформаційної гігієни — ключової передумови розробки політик безпеки цифрового урядування. У межах дослідницької моделі всі віртуальні машини, за винятком захисної, приєднуються до локального сегмента, що дозволяє досягти ізоляції, оптимізувати внутрішній трафік і знизити ризики витоку інформації. Централізовану маршрутизацію виконує віртуальний шлюз, який контролює взаємодію між сегментами (Антонюк, б.д.). Зазначена конфігурація дозволяє ефективно тестувати політики кібербезпеки, зокрема у сфері захисту критичної інформаційної інфраструктури, що є важливою складовою цифровізації публічного сектору.

Отже, забезпечення стійкості державних цифрових інформаційних систем до зовнішніх і внутрішніх загроз є ключовим чинником цифрової трансформації публічного сектору. Одним із пріоритетів виступає виявлення вразливостей у програмному забезпеченні, пов'язаних із помилками коду, дефіцитом перевірок даних, порушеннями логіки функціонування або недосконалістю архітектури (Diogenes et al., б.д.). Першим етапом виступає ідентифікація вразливостей, що потенційно загрожують доступності, цілісності або конфіденційності даних. Такий аналіз базується на вивченні архітектури, взаємодії модулів і механізмів автентифікації (Антонюк, б.д.). Наступний крок — моделювання наслідків, серед яких витоки даних, DoS-атаки, маніпуляції, фінансові втрати (International Organization for Standardization, 2020). Оцінка загального рівня загрози здійснюється з урахуванням поширеності вразливості, доступності експлойтів та ролі системи в інфраструктурі державного управління (Glazunova et al., 2020). Це дозволяє диференціювати

рівень ризику та сформувати відповідні сценарії реагування. Фінальним етапом є впровадження захисних заходів, зокрема оновлень, модифікацій коду, змін автентифікаційних процедур і зонування доступу (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020). У державному секторі такі дії повинні відповідати правовим нормам, зокрема Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (Верховна Рада України, 1994). Моніторинг та аудит безпеки є постійними елементами ризик-менеджменту. Вони включають аналіз журналів подій, перевірку конфігурацій, контроль за доступом і виявлення аномалій (Kursin et al., 2019). Ці заходи спрямовані на вчасне виявлення нових загроз та підтримку відповідності стандартам. Інтеграція технічного й управлінського підходів до кібербезпеки дозволяє забезпечити цілісність функціонування державних цифрових сервісів, зменшити репутаційні втрати та сформувати довіру громадськості (Президент України, 2021).

Висновки та рекомендації щодо підвищення ефективності рівня безпеки державних цифрових інформаційних ресурсів. Забезпечення належного рівня кібербезпеки є одним із ключових завдань органів державної влади. Воно потребує системного підходу до формування державної політики, що охоплює міжвідомчу взаємодію між органами влади, інститутами громадянського суспільства, бізнесу, достатнє ресурсне забезпечення, а також постійне оновлення стратегічних підходів відповідно до змін у цифровому середовищі (Антонюк, б.д.); (International Organization for Standardization, 2020).

Державна політика в галузі кібербезпеки охоплює такі основні напрями:

- міжнародна взаємодія, яка передбачає участь України в глобальних ініціативах, уніфікацію законодавства з міжнародними стандартами, посилення співпраці з міжнародними структурами та організацію спільних заходів (Glazunova et al., 2020);

- національна безпека та внутрішня політика, що включає створення Національної системи кібербезпеки, стандартизацію захисту критичної інфраструктури та вдосконалення нормативного забезпечення правоохоронної діяльності у сфері кіберзлочинності (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020);
- безпека та оборона, де акцент робиться на підготовці відповідних державних структур до кібероперацій, захисті військових та державних інформаційних систем, розвитку фахового кадрового потенціалу (Вакалюк et al., 2021);
- освіта, наука та інновації, що передбачають розвиток освітніх програм із кібербезпеки, популяризацію знань серед молоді, підвищення кваліфікації працівників критичної інфраструктури та формування цифрової культури (Маслова et al., 2020). Системна реалізація державної політики потребує створення ефективної інституційної архітектури. До суб'єктів національної системи кібербезпеки належать Служба безпеки України, Міністерство внутрішніх справ, Міністерство оборони, Генеральний штаб Збройних Сил України, Державна служба спеціального зв'язку та інші уповноважені органи (Крайнов et al., 2020). Для координації їхньої діяльності доцільним є створення Державного агентства з питань кіберзахисту, функції якого включатимуть аналітику загроз, нормативно-методичне забезпечення, ведення реєстрів об'єктів критичної інфраструктури та надання дозволів на використання засобів захисту (Diogenes et al., б.д.).

Важливим завданням є адаптація чинного законодавства до нових викликів, зокрема внесення змін до законів України «Про основи національної безпеки», «Про кібербезпеку», «Про критичну інфраструктуру», а також до Кримінального кодексу та КУпАП — із метою чіткого визначення відповідальності за кіберзлочини, інтеграції поняття цифрових доказів та вдосконалення процедур реагування на інциденти (Федченко, 2018). Окрему увагу слід приділити

гармонізації національного законодавства із стандартами ЄС та НАТО — зокрема у сферах сертифікації, аудитів, ліцензування, кібергігієни, оцінки ризиків та спільного реагування (Верховна Рада України, 2017). У цьому контексті рекомендовано ухвалити Національний план реагування на інциденти інформаційної безпеки, який має передбачати алгоритми дій, строки реагування, канали комунікації та механізми відновлення систем (Куншт, б.д.). Також необхідно розвивати кадровий потенціал у сфері публічного управління через оновлення державних освітніх стандартів із включенням компетентностей з кіберзахисту, створення системи підвищення кваліфікації держслужбовців із використанням сертифікованих платформ (Мазепа et al., 2021). Важливою складовою є розвиток державно-приватного партнерства, зокрема через угоди про спільне реагування на кіберінциденти, обмін інформацією про загрози, участь бізнесу у формуванні політик та залучення ІТ-компаній до аудиту безпеки державних систем (Мазепа et al., 2021). Комплексна реалізація цих заходів забезпечить не лише стійкість публічного управління до цифрових загроз, але й підвищить рівень довіри до органів державної влади, що є критично важливим в умовах воєнного стану та глобальної цифровізації (Курсін et al., 2019).

Ефективне функціонування цифрового середовища державних установ вимагає впровадження цілісної системи заходів з кібербезпеки, що включає: аудит безпеки, перегляд політик інформаційного захисту, виявлення вразливостей, адаптацію нормативно-правової бази та розробку комплексної стратегії захисту інформації (Залижнюк et al., 2021). Значну роль відіграє впровадження антивірусних рішень, систем шифрування, обмеження доступу до об'єктів критичної інфраструктури, а також підвищення цифрової грамотності персоналу. Одночасно важливими є постійний моніторинг загроз, резервне копіювання даних, а також проведення тестування на проникнення (пентестингу) як дієвого інструмента для оцінки ступеня вразливості систем. Пентестинг виконує не лише технічну, а й управлінську функцію — результати

випробувань є основою адаптації заходів із кіберзахисту. Вивчення ризиків, пов'язаних із виявленими вразливостями, потребує динамічного підходу до оцінки загроз у цифровому середовищі. Систематичний аналіз потенційних наслідків дозволяє своєчасно реагувати на інциденти й мінімізувати політичні, репутаційні та економічні втрати (Пономаренко et al., 2021). Запропоновано модель інтегрованого управління інформаційною безпекою, яка поєднує нормативно-правові, технічні та освітні компоненти. Серед пріоритетних заходів — удосконалення політик контролю доступу, реалізація навчальних програм з кібергігієни, оновлення стратегій захисту інформації та підвищення цифрової компетентності працівників органів державної влади.

Запропоновані в статті рекомендації з підвищення рівня кіберзахисту державних цифрових систем у хмарних середовищах мають комплексний характер і охоплюють ключові рівні управління кібербезпекою — стратегічний, технічний та організаційний.

Стратегічний рівень включає формування та реалізацію державної політики у сфері кібербезпеки, відповідність законодавства з міжнародними стандартами, участь у глобальних ініціативах, розвиток міжнародного партнерства, створення національної інституційної архітектури та міжвідомчої координації тощо.

Технічний рівень охоплює проведення пентестингу, аудитів безпеки, впровадження сучасних рішень із шифрування та захисту даних, резервне копіювання, постійний моніторинг загроз, використання сертифікованих засобів захисту та адаптацію технічних заходів до нових вразливостей тощо.

Організаційний рівень має включати розвиток кадрового потенціалу, впровадження навчальних програм із кібергігієни та підвищення кваліфікації державних службовців, розширення державно-приватного партнерства, впровадження ефективних політик контролю доступу та процедур реагування на інциденти тощо.

Реалізація запропонованих заходів сприятиме зміцненню кіберстійкості державних цифрових ресурсів, зниженню ризиків витоку або компрометації даних, підвищенню до-

віри громадян та міжнародних партнерів до цифрової інфраструктури України. Комплексний підхід, що поєднує управлінські, технічні та організаційні інструменти, є критично важливим в умовах воєнного стану та глобальної цифрової трансформації.

Забезпечення цифрового суверенітету України можливе лише за умови цілісного підходу до кібербезпеки, що інтегрує інноваційні технології, управлінські рішення та правове регулювання.

REFERENCES

1. Антонюк, П. Є. (б.д.). Класифікація ймовірних способів вчинення атак на інформацію як на-прям протидії комп'ютерній злочинності. Боротьба з організованою злочинністю і корупцією (теорія і практика). http://www.nbu.gov.ua/portal/Soc_Gum/bozk/19text/g1927.htm
2. Вакалюк, Т. А., & Мар'єнко, М. В. (2021). Досвід використання хмаро орієнтованих систем відкритої науки в процесі навчання і професійного розвитку вчителів природничо-математичних предметів. Інформаційні технології і засоби навчання, 81(1), 340–355. <https://doi.org/10.33407/itlt.v81i1.4225>
3. Верховна Рада України. (1992). Про інформацію (Закон України від 02 жовтня 1992 р. № 2657-XII). <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
4. Верховна Рада України. (1994). Про захист інформації в інформаційно-телекомунікаційних системах (Закон України від 05 липня 1994 р. № 80/94-ВР). <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
5. Верховна Рада України. (2005). Про ратифікацію Конвенції про кіберзлочинність (Закон України від 07 вересня 2005 р. № 2824-IV). <https://zakon.rada.gov.ua/laws/show/2824-15#Text>
6. Верховна Рада України. (2006). Про Державну службу спеціального зв'язку та захисту інформації (Закон України від 23 лютого 2006 р. № 3475-IV). <https://zakon.rada.gov.ua/laws/show/3475-15#Text>
7. Верховна Рада України. (2011). Про доступ до публічної інформації (Закон України від 13 січня 2011 року № 2939-VI). <https://zakon.rada.gov.ua/laws/show/2939-17>
8. Верховна Рада України. (2017). Про основні засади забезпечення кібербезпеки України (Закон України від 05 жовтня 2017 року № 2163-VIII). <https://zakon.rada.gov.ua/laws/show/2163-19>
9. Верховна Рада України. (2018). Про національну безпеку України (Закон України від 21 червня 2018 року № 2469-VIII). <https://zakon.rada.gov.ua/laws/show/2469-19>
10. Верховна Рада України. (б.д.). Про захист персональних даних (Закон України від 01 червня 2010 року № 2297-VI).
11. Верховна Рада України. (1994). Про захист інформації в інформаційно-телекомунікаційних системах (Закон України від 05 липня 1994 року № 80/94-ВР). <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
12. Гришук, Р. В., & Охрімчук, В. В. (2020). Напрямки підвищення захищеності комп'ютерних систем та мереж від кібератак. У Матеріали II Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації» (с. 60–61). Видавництво Європейського університету.
13. Діденко, О. В., & Негребецька, Л. В. (2021). Методика оцінювання рівня захищеності інформаційної системи на основі нечіткої логіки. Науковий вісник Ужгородського національного університету. Серія: Економіка, 1(57), 164–168.
14. Diogenes, Y., & Ozkaya, E. (б.д.). Cybersecurity – Attack and Defense Strategies (Second Edition).
15. DOU. (б.д.). Що варто знати про GDPR. <https://dou.ua/lenta/articles/what-gdpr-is/>
16. Залижнюк, О. А., & Скулиш, С. С. (2021). Забезпечення кібербезпеки: теорія і практика. Національна академія внутрішніх справ.
17. Запара, С. В., Бондаренко, В. О., & Гриша, С. В. (2022). Основи кібербезпеки та захисту інформації. Державний університет телекомунікацій.
18. Запара, С. В., & Гуменюк, О. Ю. (2022). Аналіз вразливостей та методів захисту мережевих екранів нового покоління. Системи управління, навігації та зв'язку, (6 (72)), 96–101.

19. Glazunova, O., Voloshyna, T., Korolchuk, V., & інші. (2020). Cloud-oriented environment for flipped learning of the future IT specialists. E3S Web of Conferences.
20. Hewlett Packard Enterprise. (2016). Наукове дослідження Інтернету речей від Hewlett Packard Enterprise. https://json.tv/tech_trend_find/nauchnoe-issledovanie-interneta-veschey-ot-hewlett-packard-enterprise-20160503115845
21. International Organization for Standardization. (2020). ISO/IEC 27035-3:2020: Information security incident management – Part 3: Guidelines for ICT incident response operations.
22. Кабінет Міністрів України. (2006). Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373). <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text>
23. Кабінет Міністрів України. (2019). Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури (Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518). <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text>
24. Київський центр безпеки. (б.д.). Украинский ресурс по безопасности. <http://kiev-security.org.ua>
25. Крайнов, В. О., Маланчук, М. Ф., & Грозовський, Р. І. (2020). Методика оцінки ефективності комплексної системи захисту інформації автоматизованих інформаційних систем органів військового управління. Сучасні інформаційні технології у сфері безпеки та оборони, 1(37), 103–106.
26. Куншт. (б.д.). Заради вашої безпеки. <https://kunsht.com.ua/zaradi-vashoi-bezpeki/>
27. Курсін, Н. С., Семенко, О. П., & Щербак, С. О. (2019). Методичні рекомендації до виконання кваліфікаційної роботи здобувачами другого (магістерського) рівня вищої освіти спеціальності 125 «Кібербезпека». Київський національний університет імені Тараса Шевченка.
28. Мазепа, А. Д., & Тарасов, А. С. (2021). Безпечна автентифікація до веб-додатку з використанням JWT та browser fingerprinting. У Матеріали XXII Міжнародного молодіжного форуму «Радіoeлектроніка та молодь у XXI столітті» (Том 4, с. 60–61). Харківський національний університет радіoeлектроніки.
29. Мазепа, А. Д., & Тарасов, А. С. (2021). Розуміння та захист від атаки DNS rebinding. У Матеріали XXII Міжнародного молодіжного форуму «Радіoeлектроніка та молодь у XXI столітті» (Том 4, с. 62–63). Харківський національний університет радіoeлектроніки.
30. Маслова, Н. О., & Полуніна, Д. О. (2020). Методи біометричної автентифікації при ідентифікації особи за рисами обличчя.
31. Microsoft. (б.д.). Керівництво по GDPR. <https://docs.microsoft.com/en-us/office365/admin/security-and-compliance/gdpr-compliance?view=o365-worldwide>
32. Національний банк України. (2017). Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України (Постанова НБУ від 28.09.2017 № 95). <http://zakon2.rada.gov.ua/laws/show/en/v0095500-17/page>
33. Network Cultures. (б.д.). The Internet of Things: A Critique of Ambient Technology and the AllSeeing Network of RFID. https://www.networkcultures.org/_uploads/notebook2_theinternetofthings.pdf
34. Олефіренко, О. В., & Лазарєв, Є. М. (2022). Аналіз методів захисту від SQL-ін'єкцій. Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація, 2(33), 160–166.
35. Пономаренко, В. О., & Скляр, О. В. (2021). Моделі та методи визначення ефективності протидії кіберзагрозам в умовах гібридної війни. Проблеми кібербезпеки: Збірник наукових праць, (1), 74–80.
36. Президент України. (2014). Про заходи щодо вдосконалення державної політики в інформаційній сфері (Указ Президента України від 01 травня 2014 року № 449/2014). <https://zakon.rada.gov.ua/laws/show/449/2014>
37. Президент України. (2015). Про Стратегію національної безпеки України (Указ Президента України від 26 травня 2015 року № 287/2015). <https://zakon.rada.gov.ua/laws/show/287/2015>
38. Президент України. (2016). Питання Національного координаційного центру кібербезпеки (Указ Президента України від 07 червня 2016 року № 242/2016). <https://zakon.rada.gov.ua/laws/show/242/2016>

39. Президент України. (2016). Про Стратегію кібербезпеки України (Указ Президента України від 15 березня 2016 року № 96/2016). <https://zakon.rada.gov.ua/laws/show/96/2016>
40. Президент України. (2017). Про Доктрину інформаційної безпеки (Указ Президента України від 25 лютого 2017 року № 47/2017). <https://zakon.rada.gov.ua/laws/show/47/2017>
41. Президент України. (2021). Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» (Указ Президента України від 26.08.2021 р. № 447/2021). <https://zakon.rada.gov.ua/laws/show/447/2021#Text>
42. Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020). (2020).
43. Федченко, Д. (2018). Система забезпечення кібербезпеки: проблеми формування та ефективною діяльності. Молодий вчений, (57), Юридичні науки. <http://elar.naiau.kiev.ua>
44. Шелудько, І. В. (2022). Забезпечення кібербезпеки критичної інфраструктури банківської системи. У Правове життя сучасної України: Матеріали Міжнародної науково-практичної конференції, присвяченої 25-річчю Національного університету «Одеська юридична академія» (м. Одеса, 20 травня 2022 р.) (с. 345–347).
45. Шестакевич, Т. В., & Бєсєдов, А. А. (2023). Метод імітаційного моделювання кібератак на основі аналізу дерев атак. Системи обробки інформації, (2 (175)), 85–91.
46. Yevseiev, V., & other. (2021). Development of conception for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies, 3(9 (111)), 63–83.

CYBERSECURITY OF GOVERNMENT DIGITAL SYSTEMS: PENTESTING OF CLOUD ENVIRONMENTS

Abstract. *The article reviews and analyzes research areas in the field of cybersecurity of state digital systems. It is emphasized that in the context of digitalization and the implementation of digital governance, cybersecurity of state digital systems is of particular importance. This is due to the need to increase the resilience of the organizational environment to cyber threats and strengthen the information sovereignty of the State. Relevant aspects regarding the prospects for improving legislation are identified, and a comprehensive system of recommendations is formed, which includes both management solutions and technical cybersecurity measures.*

It is noted that the use of cloud technologies has the potential to improve and increase the efficiency of the functioning of state institutions. At the same time, possible cyber threats and risks associated with the use of cloud technologies are emphasized. The methodology of pen-testing in cloud environments of state digital information resources is considered.

The article presents proposals and provides recommendations for improving cyber protection in state digital information systems.

Keywords: *information security audit, security of government systems, information protection, cybersecurity, pentesting, penetration testing, digital tools, cloud environments.*

ІНФОРМАЦІЯ ПРО АВТОРА

Жорняк Андрій — доктор філософії в галузі публічного управління та адміністрування, головний державний інспектор відділу з питань безпеки праці південного напрямку управління інспекційної діяльності у Київській області Центрального міжрегіонального управління Державної служби з питань праці, Україна, м. Київ, вул. Вавілових, 10, 04060; +380 67 956 95 99; e-mail: dr.andrij.zhorniak@gmail.com; ORCID: 0000-0001-9515-0180

INFORMATION ABOUT THE AUTHOR

Zhorniak Andrii — PhD, Doctor of Philosophy in Public Administration and Management, Chief State Inspector of the Labour Safety Department of the Southern Division of the Inspection Department in Kyiv Region of the Central Interregional Directorate of the State Labour Service of Ukraine, 10 Vavilovych Street, Kyiv, Ukraine, 04060; +380 67 956 95 99; e-mail: dr.andrij.zhorniak@gmail.com; ORCID: 0000-0001-9515-0180

ВДОСКОНАЛЕННЯ ДЕРЖАВНИХ СТАНДАРТІВ УКРАЇНИ У СФЕРІ НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ: ШЛЯХ ДО ГАРМОНІЗАЦІЇ З МІЖНАРОДНИМИ ТА ЄВРОПЕЙСЬКИМИ НОРМАМИ (на прикладі ДСТУ 3008:2015 «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання»)

Людмила Грищенко,

Державна науково-технічна бібліотека України

Віктор Кипоренко,

Державна науково-технічна бібліотека України

Анотація. Стаття присвячена дослідженню проблем модернізації державних стандартів України в галузі науково-технічної інформації з фокусом на ДСТУ 3008:2015 «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання». Проведено системний аналіз поточного стану стандарту, який виявив критичні недоліки: неузгодженість з чинною нормативно-правовою базою України, розбіжності із сучасними міжнародними практиками, недостатнє врахування національної специфіки, уповільнену динаміку оновлення, слабку інтеграцію цифрових рішень та обмежену участь ключових стейкхолдерів у процесі розробки. Запропоновано комплексну систему принципів модернізації стандартів, що ґрунтується на синхронізації з європейськими та міжнародними нормами, впровадженні цифрових технологій у процесі стандартизації, уніфікації форматів науково-технічної документації, забезпеченні прозорості розробки стандартів та активному залученні представників бізнес-середовища, академічної спільноти й організацій громадянського суспільства. Практичне значення дослідження полягає у формуванні науково обґрунтованої основи для оновлення вказаного державного стандарту, підвищення якості та прозорості звітності про наукову, науково-технічну та інноваційну діяльність закладів вищої освіти і наукових установ України, а також оптимізації аналітичних процесів у державних органах управління.

Ключові слова: державні стандарти, ДСТУ 3008:2015, науково-технічна інформація, стандартизація, цифровізація, міжнародна гармонізація, відкритість, наукова звітність.

ПОСТАВЛЕННЯ ПРОБЛЕМИ

У сучасну епоху інновацій наука і техніка розвиваються бурхливими та швидкими темпами, пронизуючи всі сфери людського життя та створюючи передумови для кардинальних змін у суспільстві та економіці. Але сучасний науково-технічний прогрес не лише визначає майбутнє цивілізаційного розвитку, а й вимагає зваженого та усвідомленого підходу до використання своїх досягнень, створення ефективних механізмів, здатних забезпечити узгодженість, безпеку та конкурентоспроможність результатів науково-технічної діяльності.

У цих процесах саме стандарти забезпечують суспільству не лише своєчасну адаптацію до змін, але й ефективно впровадження результатів науково-технічного прогресу у виробництво, наукову та освітню сферу, повсякденне життя. Це впливає саме із **суті стандартизації, яка** полягає у встановленні єдиних правил, норм і вимог, що регулюють процеси, продукцію, послуги та технології з метою забезпечення їх якості, безпеки, сумісності та ефективності, адже стандарти й розробляються з метою забезпечення єдиних підходів у різних сферах суспільного життя та господарської діяльності. Це своє-

рідний «місток» між науковими відкриттями та їх практичним застосуванням, адже саме завдяки стандартам створюються єдині правила та критерії, що спрощують упровадження інновацій, полегшують міжнародну співпрацю та сприяють інтеграції України у світовий науково-технічний простір.

З огляду на це пріоритетного значення набуває вдосконалення державних стандартів України. Особливо це стосується сфери науково-технічної інформації: створення ефективної системи стандартизації, що забезпечує єдність вимог до оформлення, збереження та поширення наукових знань, сприяє інтеграції наукових результатів у міжнародний інформаційний простір. Одним із ключових у цій сфері є ДСТУ 3008:2015 «Документація. Звіти у сфері науки і техніки. Структура та правила оформлення», який є основою для наукової звітності, оскільки визначає структуру та правила оформлення звітів у сфері науки і техніки. Це єдиний національний стандарт, що регулює процес офіційної звітності про науково-дослідні роботи (НДР), забезпечує уніфіковану систему звітності для МОН, НАН, галузевих академій та державних установ. Він є обов'язковим для підготовки підсумкових звітів про виконані НДР, які передаються у державні фонди науково-технічної інформації, виступає нормативною базою для формування статистики науки, планування та моніторингу наукової діяльності, створює основу для наукометричного аналізу, регламентуючи структуру даних, що збираються у звітах. Фактично без цього стандарту наукова установа не може офіційно завершити НДР та передати її результати до державної системи обліку. Дослідження із цієї проблематики у сфері науково-технічної інформації виявило низку проблем, які фактично зводять нанівець ефективність чинного стандарту. Серед них варто зупинитися на двох, які найбільше впливають на його ефективність, — уніфікації термінології та гармонізації з міжнародними стандартами. Проведений аналіз звертає увагу на потребу в якісному науковому дослідженні проблематики оновлення

та вдосконалення стандартів, упровадження його результатів у практики українських науковців та створення відповідної методології моніторингу ефективності впровадження належного управління дослідницькими даними.

АКТУАЛЬНІСТЬ ДОСЛІДЖЕННЯ

Актуальність дослідження полягає в необхідності оновлення, уніфікації та гармонізації вищезгаданого стандарту з міжнародними та європейськими (ISO, EN, стандартами ЄС у сфері досліджень та інновацій), забезпечення сумісності форматів наукових документів з глобальними базами даних та репозитаріями; сприяння підвищенню конкурентоспроможності українських наукових розробок на світовій арені, уніфікації вимог до звітності у сфері науки і техніки відповідно до потреб держави, бізнесу та академічної спільноти.

Відповідно до Закону України «Про стандартизацію» (Закон України «Про стандартизацію», 2014) стандарт є нормативним документом, що встановлює для загального і неодноразового використання правила, настанови або характеристики щодо діяльності чи її результатів та спрямований на досягнення оптимального ступеня впорядкованості в певній сфері, тобто є складовою нормативно-правової бази, що регулює діяльність у сфері науки, техніки, виробництва та економіки. Розробляються і затверджуються стандарти уповноваженими органами відповідно до чинного законодавства та мають юридичну силу нормативного документа. В Україні стандарти класифікуються за сферою дії та призначенням. Основні види включають державні стандарти (ДСТУ), галузеві стандарти (ГСТУ), стандарти підприємств (СТП), а також стандарти науково-технічних та інженерних товариств і спілок (СТТУ). Крім того, з 1 січня 2016 року в Україні почали діяти європейські та міжнародні стандарти як національні стандарти замість старих національних відповідно до наказу Міністерства економічного розвитку і торгівлі України №1493 від 30 грудня 2014 року «Про прийняття європейських та міжнародних нормативних

документів як національних стандартів України, змін до національних стандартів України та скасування національних стандартів України» (Міністерство економічного розвитку і торгівлі України, 2014).

Розвиток науки і техніки зумовив масове створення нових термінів і терміносистем. Масового поширення, як у повсякденному вжитку, так і в професійній сфері, набула велика кількість нових понять (Курносова Н.О., Курносова Р.В., 2005). Практично щодня з'являються нові програми, формати файлів, способи захисту інформації й автоматизації різних процесів. Наприклад технології штучного інтелекту, хмарні технології, великі дані (big data), блокчейн, віртуальна реальність та інші інновації. Як наслідок — ускладнюється обмін науковою інформацією не тільки між українськими установами й підприємствами, а й на міжнародному рівні, знижується ефективність систем пошуку та класифікації науково-технічних даних, виникає ризик помилкових тлумачень у документації та звітах. Тому вельми нагальною стала необхідність перекладу та застосування нових термінів в умовах термінології, що швидко змінюється, зростає за обсягом та призводить до оновлення сформованих і формування нових понять; уніфікації термінів із міжнародними стандартами (ISO, IEC) із впровадженням відповідних найменувань в українську мову (Курносова Н.О., Курносова Р.В., 2005). Іншою актуальною проблемою є гармонізація міжнародних стандартів, яка в Україні відбувається вкрай повільно (Калінічева Г.І., Романовський Р.В., 2015); частина термінології є застарілою та не відображає сучасні технології, методи та відкриті дані. Українські терміни часто мають досить вільну інтерпретацію та відрізняються від термінології ISO або IEC, що ускладнює інтеграцію в міжнародну наукову комунікацію.

Мета і завдання статті. Метою статті є аналіз та обґрунтування шляхів вдосконалення державних стандартів України у сфері науково-технічної інформації (на прикладі ДСТУ 3008:2015) з метою гармонізації з міжнародними та європейськими нормами, під-

вищення їх актуальності, цифровізації, гнучкості та інтеграції в науково-інформаційний простір.

ОГЛЯД ДЖЕРЕЛ

Проблематика вдосконалення стандартів у сфері науково-технічної інформації активно досліджується вітчизняними науковцями, однак аналіз практик і уявлень свідчить, що проблематика є недостатньо дослідженою. Певні аспекти втілення ідей і принципів удосконалення стандартів у практику наукових й академічних інституцій розглянуто в працях Курносової Н.О., Курносової Р.В. (Курносова Н.О., Курносова Р.В., 2005), Жарінової А.Г. та Ярошенко Т.О. (Жарінова А.Г., Ярошенко Т.О., 2023), Калінічевої Г.І. та Романовського Р.В. (Калінічева Г.І., Романовський Р.В., 2015), Шаповалова Є.Б. (Шаповалов Є.Б., 2023)), однак вони не мають глобального характеру, тому не спроможні представити об'єктивну картину щодо порушеного питання. Проблема в тому, що не вироблено єдиного підходу до розуміння вирішення проблематики вдосконалення стандартів з урахуванням досвіду провідних європейських країн та в контексті європейської інтеграції України (Гудзь, 2023).

ТЕОРЕТИЧНЕ ПІДґРУНТЯ

Для дослідження було застосовано такі теоретичні методи: контент-аналіз нормативно-правових документів, технічних стандартів та наукових публікацій, порівняльно-правовий аналіз національного законодавства та міжнародних норм, синтез та логіко-теоретичне узагальнення результатів аналізу для формування принципів модернізації. Джерела інформації: нормативно-правова база України, міжнародні стандарти (ISO, IEC, EN), наукові публікації та монографії, статистичні дані державних органів, протоколи ТК, методичні рекомендації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Сучасні умови розвитку науки та технологій зумовлюють потребу в оновленні дер-

жавних стандартів, що має забезпечити їх гармонізацію з міжнародними нормами та відповідність викликам цифрової трансформації, зокрема у сфері електронної звітності та метаданих.

Стандартизація як своєрідне «дзеркало» розвитку суспільства має відображати сучасний стан у сфері науки і техніки, тому стандарти не повинні бути статичними документами — вони повинні регулярно переглядатися й удосконалюватися, щоб відповідати актуальним суспільним вимогам, а їх розробка та оновлення мають базуватися на комплексних підходах, що враховують:

- наукову обґрунтованість — стандарти повинні базуватися на сучасних досягненнях науки, техніки та практичного досвіду, поєднуючи в собі теоретичні принципи, міжнародні практики й національні потреби, що в кінцевому підсумку забезпечить їх дієву ефективність;
- відповідність законодавству — дотримання вимог як національних, так і міжнародних нормативно-правових актів;
- універсальність і сумісність — можливість застосовуватися в різних сферах, використовуватися різними установами, бути придатними для різних форматів та бути зрозумілими різними мовами;
- міжнародну гармонізацію — узгодження з міжнародними нормами для забезпечення сумісності та інтеграції. Це не лише «переклад» українських стандартів на світові мови, а й створення умов для повноцінної участі України в глобальній науковій екосистемі;
- консенсусність — урахування думок усіх стейкхолдерів (наука, держава, бізнес, громадськість).

Дотримання цих принципів дозволяє створювати гнучкі, актуальні та інтегровані стандарти, які відповідатимуть сучасним викликам цифрової науки, сприятимуть ефективності наукової діяльності та інтеграції України в міжнародний інформаційний простір.

Окремо слід акцентувати увагу на відповідності стандартів законодавчим і регуляторним вимогам, адже це є ключовою умо-

вою їх легітимності, практичної застосовності та інтеграції в міжнародний науково-технічний простір. Стандарти повинні відповідати національному законодавству, узгоджуватися з постановами Кабінету Міністрів, наказами міністерств та іншими нормативними актами, що регулюють сферу їх застосування, що забезпечує правову визначеність, усуває суперечності між нормами, сприяє прозорості та стабільності правового поля. Гармонізація з міжнародними правовими нормами передбачає врахування директив, регламентів та рекомендацій ЄС (CEN, CENELEC) та міжнародних стандартів (ISO, ASTM), що впроваджуються в Україні. В кінцевому підсумку це забезпечує сумісність національної стандартизації з міжнародною та спрощує інтеграцію української науки у світовий науковий простір.

Попри значні переваги, які надає стандартизація, є низка проблем і викликів, які впливають на ефективність її реалізації, зокрема в науково-технічному просторі. При цьому необхідно враховувати, що стандарти, пов'язані з наукою, мають свої особливості. Перш за все вони створюються на основі досягнень науки та задоволення потреб її розвитку, бо забезпечують якість, уніфікацію, відкритість та міжнародну інтеграцію наукової інформації, а отже повинні бути динамічними, враховувати швидкий розвиток науки й технологій та гармонізуватися з міжнародними стандартами. Щоб відповідати цим вимогам, вони не повинні бути статичними, а мають постійно, через певний проміжок часу, переглядатися й удосконалюватися.

Кабінетом Міністрів України у 2017 році було прийнято постанову «Про внесення змін до постанови КМУ від 31.05.2017 №373 «Про затвердження Порядку розроблення, введення в дію та перегляду професійних стандартів» (Кабінет Міністрів України, 2017), якою затверджувалася нова редакція Порядку розроблення, введення в дію та перегляду професійних стандартів, що формує єдині прозорі правила для розроблення та оновлення професійних стандартів.

Однак наша система залишається орієнтованою на традиційні підходи й не повною

мірою враховує виклики цифровізації та вимоги відкритої науки, що поступово призводить до збільшення розриву між новими технологіями та нормативними вимогами (Кремень В.Г., Цибаль-Міхальська А., 2024). Недостатня гармонізація з міжнародними стандартами уповільнює інтеграцію у світовий економічний і науковий простір, а бюрократичні перепони, тривалі процедури затвердження, обмежена прозорість процесу та складність у залученні всіх зацікавлених сторін значно гальмують цей процес.

ДСТУ 3008:2015 «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлення» встановлює загальні вимоги до структурних елементів і правил оформлювання звітів у сфері науки й техніки. Це єдиний національний стандарт, що регулює процес офіційної звітності про науково-дослідні роботи (НДР), забезпечує уніфіковану систему звітності для МОН, НАН, галузевих академій та державних установ, є обов'язковим для підготовки підсумкових звітів про виконанні НДР, які передаються в державні фонди науково-технічної інформації, виступає нормативною базою для формування статистики науки, планування та моніторингу наукової діяльності, створює основу для наукометричного аналізу, оскільки регламентує структуру даних, що збираються у звітах. Без дотримання вимог цього стандарту наукова установа не може офіційно завершити НДР та передати її результати до державної системи обліку.

ДСТУ 3008:2015 не оновлювався з 2015 року, а отже почав втрачати актуальність — застаріла термінологія не враховує динаміку технологічного розвитку та цифрової трансформації. Українські терміни часто мають вільну інтерпретацію та відрізняються від термінології ISO або IEC, що ускладнює інтеграцію в міжнародну наукову комунікацію. Це є однією з ключових проблем — брак механізмів швидкого оновлення. Для порівняння, міжнародні стандарти у сфері науково-технічної інформації ISO та ASTM регулярно переглядаються раз на 3–5 років з урахуванням нових технологій, змін у науковій

комунікації та потреб ринку. ДСТУ 3008:2015 орієнтований переважно на друковані документи та не враховує сучасних електронних форматів і відкритих наукових даних.

Оновлення потребує ДСТУ 3008:2015 і в частині приведення у відповідність до законодавчої бази. Після 2015 року Верховною Радою України було прийнято декілька законів, які мають безпосереднє відношення до сфери науково-технічної інформації, зокрема Закони України «Про наукову і науково-технічну діяльність» (Закон України «Про наукову і науково-технічну діяльність», 2016), «Про внесення змін до деяких законодавчих актів України щодо забезпечення укладення угоди між Україною та Європейським Союзом про взаємне визнання кваліфікованих електронних довірчих послуг та імплементації законодавства Європейського Союзу у сфері електронної ідентифікації» (Закон України «Про внесення змін до деяких законодавчих актів України щодо забезпечення укладення угоди між Україною та Європейським Союзом про взаємне визнання кваліфікованих електронних довірчих послуг та імплементації законодавства ЄС у сфері електронної ідентифікації», 2022), який спрямований на приведення у відповідність близько 90 законів України, що регулюють ЕДП та електронну ідентифікацію з європейськими стандартами, вводяться положення щодо створення, подання та зберігання звітів у електронній формі, визначаються вимоги до цифрових підписів, електронних архівів та довгострокового збереження даних. Ці норми вимагають закріплення в стандарті з метою уникнення ризиків юридичної сили електронних документів та їх прийнятності в офіційних процесах. Крім того, в українському науковому середовищі вже активно поширюються та функціонують інституційні та тематичні репозитарії наукових публікацій, створюються репозитарії даних, використовуються міжнародні ідентифікатори дослідників ORCID, присвоюються DOI науковим публікаціям, а в стандарті офіційного тлумачення досі немає.

Міністерство освіти і науки України у 2024 році вже зробило важливий крок в цьому

напрямі — спрощену форму звітності, затверджену наказом МОН України від 11.09.2024 року №1304 «*Про затвердження Змін до Порядку державної реєстрації та обліку науково-дослідних, дослідно-конструкторських робіт і дисертацій*» (Міністерство освіти і науки України, 2024), яким, зокрема, передбачено введення єдиної уніфікованої форми звітності для всіх наукових проєктів усіх сфер управління, можливість використання форми як для проміжних, так і для остаточних звітів, скорочення обсягу інформації, що вимагається для подання звітів, і головне — часу на її підготовку. Це не просто чергова зміна в адміністративних процесах — це реальний крок для всіх учасників наукового процесу, який дасть змогу більше уваги приділяти безпосередньо дослідженням, а не паперовій роботі.

Серед переваг нового формату звітів важливим, зокрема, є те, що громадськість, яка зацікавлена в результатах науково-технічної діяльності, отримає швидший і зручніший доступ до інформації про результати досліджень, замовники (грантодавачі), що працюють у сфері науки, зможуть оперативніше обробляти звітні документи, що надходять від виконавців (університетів і наукових установ). Спрощена форма звітності не лише зменшує обсяг паперової роботи, але й робить дані про результати досліджень доступнішими для широкої аудиторії. Це важливо як для підвищення прозорості наукової діяльності, так і для зміцнення довіри громадськості до системи фінансування науки.

Іншим кроком Міністерства освіти та науки України стало затвердження наказом МОН України від 13.06.2025 року №854 «*Про затвердження методичних рекомендацій щодо підготовки інформаційних матеріалів про підсумки наукової, науково-технічної та інноваційної діяльності закладів вищої освіти та наукових установ що належать до сфери управління Міністерства освіти і науки України, за 2024 рік*» (Міністерство освіти і науки України, 2025), методичних рекомендацій, у яких визначено, як саме готувати інформаційні матеріали про підсумки наукової, на-

уково-технічної та інноваційної діяльності ЗВО та наукових установ. Однак процедурні питання та методичні рекомендації — не державний стандарт, тому наведені поняття повинні бути чітко та офіційно закріплені безпосередньо в ДСТУ, що забезпечить узгодженість термінології та правильність її застосування в практичній і нормативній діяльності.

Динаміка технологічного розвитку та виклики цифрової трансформації вимагають активної інтеграції України до європейського й світового науково-інформаційного простору. Однак наявна редакція стандарту не в повному обсязі відповідає міжнародним вимогам, що зумовлює необхідність його адаптації до сучасних практик і регламентів.

ДСТУ 3008:2015 не повністю узгоджений з положеннями міжнародних стандартів ISO/IEC, що регламентують вимоги до науково-технічних звітів та метаданих. Основні відмінності стосуються структури звітів, яка в ДСТУ має жорстко регламентований, орієнтований на друкований формат вигляд, тоді як міжнародні стандарти, зокрема ISO 5966 (International Organization for Standardization [ISO], 1982) та ISO 5127 (International Organization for Standardization [ISO], 2017), пропонують гнучкіші моделі, адаптовані до електронного середовища та цифрового обміну. Крім того, ДСТУ 3008 не враховує сучасних вимог до метаданих, що забезпечують ідентифікацію, пошук та інтеграцію звітів у міжнародні бази даних (Scopus, Web of Science) і національні дослідницькі інформаційні системи. В Україні вже впроваджено електронні репозитарії, ORCID, DOI, проте профільні стандарти не забезпечують їх регулювання.

Невідповідність законодавчої та стандартизаційної бази реальним потребам наукової спільноти, закладів освіти та інноваційного бізнесу призводить до правової невизначеності й зниження конкурентоспроможності української науки, перешкоджає ефективній інтеграції України до європейського дослідницького простору.

Додаткові бар'єри для оновлення стандартів створюють сучасні виклики, зумовле-

ні воєнними діями та кризами. Руйнування інституційної інфраструктури, концентрація державних ресурсів на обороні, міграція висококваліфікованих кадрів та обмеженість фінансування призводять до відставання від міжнародних тенденцій щодо розробки та оновлення стандартів, скорочення інновацій та уповільнення інтеграції України в європейський і світовий простір.

Пропозиції щодо вдосконалення ДСТУ 3008:2015

1. Оновлення стандарту необхідно здійснювати відповідно до Закону України «Про стандартизацію» (Закон України «Про стандартизацію», 2014), комплексу ДСТУ серії 1.0–1.7:2015 (Київ: ДП «УкрНДНЦ», 2015) та практик міжнародних організацій (ISO, IEC, CEN). Схема цього процесу повинна містити такі етапи: визначення необхідності в оновленні стандарту, підготовку пропозицій та затвердження плану, розробку проекту, громадське обговорення й експертизу, затвердження та реєстрацію, набуття чинності та впровадження. Крім того, згідно з ДСТУ 1.2:2015 «Національна стандартизація. Правила проведення робіт з національної стандартизації» (Київ: ДП «УкрНДНЦ», 2015), постановою Кабінету Міністрів України «Про внесення змін до постанови КМУ від 31.05.2017 №373 «Про затвердження Порядку розроблення, введення в дію та перегляду професійних стандартів» (Кабінет Міністрів України, 2017) та міжнародною практикою, передбачається перегляд кожного стандарту не рідше ніж раз на 5 років. Ключова роль у цьому процесі належить ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості», який координує весь цикл — від аналізу потреби до затвердження та впровадження.

2. ДСТУ 3008:2015 необхідно гармонізувати відповідно до положень ДСТУ 1.5:2015 «Національна стандартизація. Правила побудови, викладання, оформлення та вимоги до змісту нормативних документів» (Київ: ДП «УкрНДНЦ», 2015), який входить до цього комплексу та встановлює єдині вимоги до розроблення, оформлення та структури

нормативних документів, з метою уніфікації структури та забезпечення узгодженості нормативних документів.

Приведення у відповідність дозволить уніфікувати структуру та оформлення звітів про науково-дослідні роботи шляхом упровадження обов'язкових елементів, таких, зокрема, як передмова, бібліографія, чітка нумерація розділів та класифікація додатків на обов'язкові й довідкові. Також необхідно переглянути терміни та визначення, узгодивши їх із чинними стандартами, відповідними політиками та рекомендаціями міжнародних організацій, оновити вимоги до оформлення тексту й електронних версій звітів, зокрема запровадити метадані з урахуванням постійних ідентифікаторів (анотації, ключові слова, DOI, ROR, ORCID). Крім того, у стандарті варто передбачити англomовні титульні аркуші, шаблони для прикладів та сучасні інструменти електронного документообігу, що забезпечить підвищення якості наукової звітності, її прозорість та відповідність міжнародним вимогам.

3. Розробити єдину структуру звітності для всіх ЗВО та НУ України, що дозволить створити єдину форму та правила підготовки звітності про наукові дослідження та розробки й забезпечити порівнянність, прозорість і зручність аналізу результатів. Це дозволить забезпечити єдині правила підготовки науково-технічних звітів, уніфікувати термінологічну базу для управління наукою (МОН, НАНУ, галузеві академії наук, НФДУ), використовувати цей стандарт під час підготовки звітів, заявок, наукових публікацій, що відповідають міжнародним вимогам (ЗВО та НУ). Крім того, замість жорстко фіксованої структури варто передбачити кілька варіантів побудови звітів залежно від сфери дослідження та виду робіт і надати можливість включення мультимедійних елементів (графіки, 3D-моделі, інтерактивні додатки).

4. В оновленій редакції стандарту слід обов'язково закріпити унормоване визначення терміну «електронний документ» відповідно до Закону України «Про електронні документи та електронний документообіг»

(Закон України «Про електронні документи та електронний документообіг», 2003), що забезпечить єдність термінології та узгодженість нормативної бази у сфері наукової та науково-технічної діяльності. У тексті чинного ДСТУ 3008:2015 цього визначення немає. Стандарт орієнтований переважно на традиційні (паперові) та універсальні вимоги до структури звітів, хоча в ньому допускається подання в електронному вигляді. Приведення його у відповідність до законів України «Про електронні документи та електронний документообіг» (Закон України «Про електронні документи та електронний документообіг», 2003), «Про внесення змін до деяких законодавчих актів України щодо забезпечення укладення угоди між Україною та Європейським Союзом про взаємне визнання кваліфікованих електронних довірчих послуг та імплементації законодавства Європейського Союзу у сфері електронної ідентифікації» (Закон України «Про внесення змін до деяких законодавчих актів України щодо забезпечення укладення угоди між Україною та Європейським Союзом про взаємне визнання кваліфікованих електронних довірчих послуг та імплементації законодавства ЄС у сфері електронної ідентифікації», 2022), ДСТУ 1.5:2015 «Національна стандартизація. Правила побудови, викладання, оформлення та вимоги до змісту нормативних документів» (Київ: ДП «УкрНДНЦ», 2015) та ДСТУ 2732:2004 «Діловодство й архівна справа. Терміни та визначення понять» (Київ: ДП «УкрНДНЦ», 2004) дозволить оновити стандарт, забезпечивши перехід на цифрові формати звітності в науці та техніці й сумісність з електронним документообігом в державних установах і міжнародних наукових платформах. Крім того, це дозволить забезпечити юридичну та наукову захищеність електронних звітів, надати їм статус офіційних документів (з обов'язковими реквізитами, ЕЦП / КЕП) та виключити дублювання: не буде потреби паралельно подавати паперові та електронні версії.

5. Необхідність оновлення ДСТУ 3008:2015 також обумовлює перехід закладів ви-

щої освіти та наукових установ України до електронної форми звітності через систему URIS (Ukrainian Research Information System) відповідно до рішення колегії Міністерства освіти та науки України від 13 лютого 2020 р. № 1/1-13 «Про створення Української дослідницької інформаційної системи (URIS)» (Міністерство освіти і науки України, 2020) щодо створення системи URIS і постанови КМУ від 27 вересня 2022 р. № 1067 «Про затвердження Положення про Національну електронну науково-інформаційну систему (URIS)» (Кабінет Міністрів України, 2022), якою затверджується не тільки Положення, а й Перелік пріоритетних інформаційних ресурсів цієї системи, що докорінно змінює підхід до організації та стандартизації науково-технічної документації, адже передусім необхідно змінити формат подання звітів з огляду на повну відмову від паперових форм та переходу до електронного документообігу. Оновлений стандарт повинен містити, відповідно до законодавства, чітке та уніфіковане визначення поняття «електронний документ». Крім того, необхідно внести обов'язковий набір електронних метаданих (machine-readable), забезпечити інтероперабельність і метадані шляхом упровадження уніфікованих ідентифікаторів DOI, ORCID, ROR, Grant ID тощо, які одразу ж інтегруються з URIS, ключові слова та класифікатори, які повинні надаватися з контрольованих словників, щоб URIS міг їх індексувати. URIS уже вимагає звітності у формі електронних файлів, але для цього ДСТУ має задати стандартизовану структуру.

6. Метадані та семантичний опис у науці є невід'ємним елементом сучасних стандартів — вони перетворюють інформацію зі «статичного документа» на динамічний цифровий ресурс, адже полегшують уніфікацію звітів та публікацій, дозволяють здійснювати автоматичну обробку, аналіз і повторне використання даних, підвищують відкритість науки (Open Science) та інтеграцію у світові інформаційні системи. В оновленій версії стандарту, крім основних метаданих, необхідно закріпити міжнародні стан-

дати метаданих відповідно до ISO 15836-1:2017 *Information and documentation — The Dublin Core metadata element set — Part 1*: (International Organization for Standardization [ISO], 2017), розширені стандарти метаданих відповідно до ISO 15836-2:2019 *Information and documentation — The Dublin Core metadata element set — Part 2*: (International Organization for Standardization [ISO], 2019), додаткові метадані для наукових звітів (методологічні, результативні, бібліографічні, географічні, темпоральні), цифрові метадані (структурні, адміністративні) та міжнародні профілі для наукових даних (DataCite Metadata Schema, ORCID, DOI, FAIR принципи), що полегшить пошук, класифікацію та управління документами. Також слід визначити вимоги до структурування та опису метаданих (наприклад, Dublin Core, DataCite), що полегшить інтеграцію українських наукових звітів у світові інформаційні системи (Scopus, Web of Science, OpenAIRE). 7. Внести до оновленого ДСТУ 3008:2015 поняття, узгоджені з ISO 7144:1986 *Presentation of theses and similar documents* (International Organization for Standardization [ISO], 1986), вимогами програм Horizon Europe, OECD та положеннями стандартів ISO / IEC щодо наукових звітів і метаданих, зокрема щодо електронних репозитаріїв, ORCID, DOI. 8. Слід запровадити нові мовні та термінологічні норми з урахуванням міжнародної практики та сучасних тенденцій, оскільки сучасна наукова комунікація вимагає чіткості, уніфікації та міжнародного розуміння. Уніфікація української наукової термінології з урахуванням міжнародних аналогів дозволить уникнути дублювання термінів та різночитань та сприятиме формуванню єдиного словника термінів для звітів. А стандартизація структури рефератів, ключових слів, анотацій, правильність вживання одиниць вимірювання, аббревіатур, символів сприятиме підвищенню якості наукових текстів. Також було б доцільним запровадити можливість двомовного (українською та англійською) оформлення титульних та реферативних частин та введення сучасних вимог до стилістики та

оформлення бібліографії (наприклад відповідність APA, Chicago, Harvard).

9. В оновленому стандарті має бути закріплене офіційне впровадження цифровізації на всіх етапах життєвого циклу звітів — від розроблення та погодження до публікації й подальшого моніторингу ефективності застосування, що дозволить значно скоротити час погодження документів, забезпечити відкритий доступ до актуальної інформації для всіх зацікавлених сторін, забезпечить оперативне реагування на зміни в технологіях і ринкових вимогах, підвищить якість і достовірність стандартів, полегшить взаємодію між органами стандартизації, бізнесом, науковими установами та громадськістю.

10. Важливим напрямом удосконалення ДСТУ 3008:2015 є методологічна підтримка, адже навіть досконалий стандарт не працюватиме без практичних посібників. Зокрема, актуальним було б створення методичних рекомендацій та шаблонів для авторів, введення єдиних форматів для різних типів звітів (науково-дослідні, науково-технічні, прикладні).

11. Також важливим є забезпечення більш активної участі стейкхолдерів — науковців, закладів освіти, державних органів, бізнесу та громадськості, залучених до розроблення та впровадження стандартів. Ідеться насамперед про інтеграцію інтересів наукової спільноти, освітніх установ, державних органів, бізнес-сектору та громадських організацій. Такий підхід сприятиме підвищенню прозорості, якості та практичної значущості стандартів, а також їх відповідності реальним потребам суспільства.

ВИСНОВКИ

Аналіз сучасних досліджень і практики впровадження стандартів у сфері науково-технічної інформації показав, що чинний ДСТУ 3008:2015 потребує комплексного оновлення. Основними чинниками є: уніфікація мовних та термінологічних норм із урахування міжнародної практики, цифровізація наукової діяльності, розвиток відкритої науки, управління науковими даними та

запровадження електронних систем звітності. Таку роботу вже заплановано Технічним Комітетом-144 «Інформація і документація», функції секретаріату цього ТК з 2019 року виконує ДНТБ України.

Запровадження оновленого стандарту підвищить надійність обігу наукової та технічної інформації, що має велике значення для сектору оборони і безпеки, зокрема в умовах гібридних загроз та інформаційних атак. Гармонізація із міжнародними стандартами (ISO, IEC, CEN, CENELEC) сприятиме сумісності українських дослідницьких і технічних даних із системами країн-партнерів НАТО та ЄС, що має стратегічне значення для колективної безпеки.

Використання уніфікованих підходів до звітності та наукових даних створить основу для ефективної інтеграції результатів досліджень подвійного призначення (цивільного й оборонного). Гармонізація національних стандартів з ISO та європейськими нормами

полегшить участь українських установ і підприємств у міжнародних проєктах, програмах Horizon Europe та глобальних наукових ініціативах. Використання уніфікованих правил документації та термінології зменшить витрати на підготовку звітів, заявок і публікацій, зокрема шляхом автоматизації в цифрових системах. Наявність міжнародно сумісних стандартів підвищить довіру до української наукової інфраструктури та сприятиме залученню грантового та інституційного фінансування.

Крім того, запровадження оновлених стандартів формуватиме нову культуру наукової комунікації, що сприятиме розвитку кадрового потенціалу та інтеграції молодих учених у світове академічне середовище, а їх відповідність міжнародним стандартам суттєво підвищить рівень довіри суспільства до української науки та її здатності генерувати якісні, верифіковані результати для вирішення національних викликів.

REFERENCES

1. Cabinet of Ministers of Ukraine. (2017, May 31). Resolution No. 373 *On approval of the procedure for the development, implementation, and review of professional standards*. Verkhovna Rada of Ukraine database. <https://zakon.rada.gov.ua/laws/show/373-2017>
2. Cabinet of Ministers of Ukraine. (2022, September 27). Resolution No. 1067 *On approval of the Regulation on the National Electronic Scientific and Information System (URIS)*. <https://zakon.rada.gov.ua/laws/show/1067-2022-%D0%BF#Text>
3. Derzhspozhyvstandart of Ukraine. (2005). *DSTU 2732:2004. Records management and archival science. Terms and definitions*. Kyiv: Derzhspozhyvstandart of Ukraine.
4. Hudz, L. V. (2023). Napriamy vdoskonalennia standartiv roboty ZMI pid chas vyborchoho protsesu v Ukraini iz vrakhuvanniam dosvidu providnykh yevropeyskykh krain [Directions for improving media work standards during the electoral process in Ukraine, considering the experience of leading European countries]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Serii: Pravo*, 79(1), 127–131. <https://doi.org/10.24144/2307-3322.2023.79.1.22>
5. International Organization for Standardization. (1982). *ISO 5966:1982 Documentation — Presentation of scientific and technical reports*. Geneva: ISO.
6. International Organization for Standardization. (1986). *ISO 7144:1986 Documentation — Presentation of theses and similar documents*. Geneva: ISO.
7. International Organization for Standardization. (2017). *ISO 5127:2017 Information and documentation — Foundation and vocabulary*. Geneva: ISO.
8. International Organization for Standardization. (2017). *ISO 15836-1:2017 Information and documentation — The Dublin Core metadata element set — Part 1: Core elements*. Geneva: ISO. <https://www.iso.org/standard/71339.html>
9. International Organization for Standardization. (2019). *ISO 15836-2:2019 Information and documentation — The Dublin Core metadata element set — Part 2: DCMI properties*. Geneva: ISO. <https://www.iso.org/standard/71340.html>

10. Kalinicheva, H. I., & Romanovskyi, R. V. (2015). International standards in the field of archival affairs and records management: Problems of harmonization in Ukraine. **Arkhivy Ukrainy*, 4*(298), 44–63.
11. Kurnosova, N. O., & Kurnosova, R. V. (n.d.). Problems of standardization and unification of scientific and technical terminology. <https://studentam.net.ua/content/view/8616/97/>
12. Kremen, V. H., & Tsybal-Mikhalska, A. (2024). *Tsyfrova transformatsiia osvity yak vyklyk sohodennia* [Digital transformation of education as a challenge of today]. Kyiv: TOV «Yurka Liubchenka». URL:
13. Ministry of Economic Development and Trade of Ukraine. (2014, December 30). Order No. 1493 **On the adoption of European and international normative documents as national standards of Ukraine, amendments to national standards of Ukraine and cancellation of national standards of Ukraine**. <https://zakon.rada.gov.ua/laws/show/z0136-15>
14. Ministry of Economic Development and Trade of Ukraine. (2016). **DSTU 1.0:2015 National standardization. Basic principles and terms**. Kyiv: Ministry of Economic Development of Ukraine.
15. Ministry of Economic Development and Trade of Ukraine. (2016). **DSTU 1.2:2015 National standardization. Standardization and related activities. Procedure for the development of national standards**. Kyiv: Ministry of Economic Development of Ukraine.
16. Ministry of Economic Development and Trade of Ukraine. (2016). **DSTU 1.5:2015 National standardization. Rules for structure, presentation, formatting, and content requirements for normative documents**. Kyiv: Ministry of Economic Development of Ukraine.
17. Ministry of Economic Development and Trade of Ukraine. (2016). **DSTU 1.7:2015 National standardization. Rules and methods for adopting identical international and regional standards as national ones**. Kyiv: Ministry of Economic Development of Ukraine.
18. Ministry of Education and Science of Ukraine. (2020, February 13). Decision of the Board No. 1/1-13 (10) **On the creation of the Ukrainian Research Information System (URIS)**. <https://mon.gov.ua/static-objects/mon/uploads/public/661/68c/961/66168c9616a5f121078556.pdf>
19. Ministry of Education and Science of Ukraine. (2025, June 13). Order No. 854 **On approval of methodological recommendations for preparing information materials on the results of scientific, scientific-technical, and innovative activities of higher education institutions and scientific institutions under the management of the Ministry of Education and Science of Ukraine for 2024**. Verkhovna Rada of Ukraine database. <https://zakon.rada.gov.ua/laws/show/z054-25>
20. Verkhovna Rada of Ukraine. (2003, May 22). Law of Ukraine **On electronic documents and electronic document circulation**. <https://zakon.rada.gov.ua/laws/show/851-15>
21. Verkhovna Rada of Ukraine. (2014). Law of Ukraine **On standardization**. **Vidomosti Verkhovnoi Rady (VVR)*, (31),* Art. 1058. <https://zakon.rada.gov.ua/laws/show/1315-18>
22. Verkhovna Rada of Ukraine. (2016). Law of Ukraine **On scientific and scientific-technical activities**. **Vidomosti Verkhovnoi Rady Ukrainy*, (3),* Art. 25. <https://zakon.rada.gov.ua/laws/show/848-19>
23. Verkhovna Rada of Ukraine. (n.d.). Law of Ukraine **On amendments to certain legislative acts of Ukraine to ensure the conclusion of an agreement between Ukraine and the European Union on mutual recognition of qualified electronic trust services and the implementation of EU legislation in the field of electronic identification**. <https://zakon.rada.gov.ua>

IMPROVEMENT OF STATE STANDARDS OF UKRAINE IN THE FIELD OF SCIENTIFIC AND TECHNICAL INFORMATION: THE PATH TO HARMONIZATION WITH INTERNATIONAL AND EUROPEAN NORMS (Based on the Example of DSTU 3008:2015 «Information and Documentation. Reports in the Field of Science and Technology. Structure and Rules for Formatting»)

Abstract. *The article is devoted to the study of issues related to the modernization of Ukrainian state standards in the field of scientific and technical information, with a focus on*

DSTU 3008:2015 «Information and Documentation. Reports in the Fields of Science and Technology. Structure and Formatting Rules». A systematic analysis of the current state of the standard revealed critical shortcomings: inconsistency with the current legal and regulatory framework of Ukraine, discrepancies with modern international practices, insufficient consideration of national specificities, slow pace of updates, weak integration of digital solutions, and limited involvement of key stakeholders in the development process.

A comprehensive system of principles for standard modernization is proposed, based on synchronization with European and international norms, implementation of digital technologies in standardization processes, unification of formats for scientific and technical documentation, ensuring transparency in the development of standards, and active engagement of representatives from the business sector, the academic community, and civil society organizations.

The practical significance of the study lies in establishing a scientifically grounded foundation for updating the specified state standard, improving the quality and transparency of reporting on scientific, scientific-technical, and innovative activities of higher education institutions and research organizations in Ukraine, as well as optimizing analytical processes in public administration bodies.

Keywords: *state standards, DSTU 3008:2015, scientific and technical information, standardization, digitalization, international harmonization, openness, scientific reporting.*

ІНФОРМАЦІЯ ПРО АВТОРІВ

Грищенко Людмила — кандидат економічних наук, ст. науковий співробітник, Державна науково-технічна бібліотека України, вул. Антоновича, 180, Київ, 03150, Україна, ORCID: 0009-0005-6103-5201

Кипоренко Віктор — кандидат економічних наук, провідний науковий співробітник, Державна науково-технічна бібліотека України, м. Київ, вул. Антоновича, 180, Київ, 03150, Україна, ORCID: 0009-0000-5396-2367

INFORMATION ABOUT THE AUTHORS

Hryshchenko Lyudmila — candidate of Economic Sciences, Senior Researcher, State Scientific and Technical Library of Ukraine, 180 Antonovycha Street, Kyiv, 03150, Ukraine, ORCID: 0009-0005-6103-5201

Kiporenko Viktor — candidate of Economic Sciences, Leading Researcher, State Scientific and Technical Library of Ukraine, Ukraine, Kyiv, 180 Antonovycha Street, Kyiv, 03150, Ukraine, ORCID: 0009-0000-5396-2367

THE POTENTIAL OF SCIENTOMETRIC ANALYSIS FOR STUDYING CLIMATE CHANGE ISSUES: A CASE STUDY OF UKRAINE

Iryna Balanchuk,

State scientific institution “Ukrainian Institute of Scientific and Technical Expertise and Information”

Sergiy Ihnatsevych,

State scientific institution “Ukrainian Institute of Scientific and Technical Expertise and Information”

Abstract. Research on climate change is critically important due to its widespread impacts on ecosystems, economies, and social structures. Climate change, including rising temperatures, rising sea levels, extreme weather events, and droughts, is already causing significant harm to people, biodiversity, and the environment, highlighting the need for research to develop strategies for adaptation and mitigation. Furthermore, understanding the underlying mechanisms of climate change processes is essential for predicting future consequences and creating effective policies and technologies. These efforts are crucial for reducing greenhouse gas emissions, transitioning to renewable energy, and preventing natural disasters.

In addition, climate change research plays a vital role in global scientific and political discussions, influencing the formation of agreements and laws that support sustainable development and environmental protection. Scientific knowledge aids in informed decision-making at international, national, and local levels, contributing to the creation of social support strategies, especially for vulnerable populations such as impoverished regions and small island nations.

This study utilizes bibliometric analysis to examine the research landscape of climate change, highlighting key research areas, identifying gaps in knowledge, and determining priority fields for further study. Bibliometrics also helps assess the interdisciplinary nature of climate change, spanning various disciplines from ecology to social sciences, and it provides insights into the contributions of scientific research to achieving the Sustainable Development Goals. This approach enhances the understanding of the geographical aspects of climate change research and supports the formation of scientific priorities while improving the impact of research on practical solutions.

Data from the Scopus platform on publications related to climate change adaptation, disaster risk reduction, sustainable agricultural practices, and the circular economy were analyzed. A total of 1,689 documents were identified between 1991 and 2024, and descriptive statistics were performed. The study employs structural scientometrics, using bibliometric links, co-citation analysis, and mapping cognitive structures to provide a comprehensive overview of the evolution of climate change research. The findings show that scientific interest in climate change has significantly increased since 2010, marking a turning point in global awareness and research efforts.

Keywords: Scientometric Analysis, Climate Change, Ukraine.

INTRODUCTION

Research on climate change is of paramount importance for several reasons. Firstly, climate change impacts all aspects of life on Earth, ranging from natural ecosystems to economies and social structures. The increase in temperature, rising sea levels, droughts, extreme storms, and

other climate-related consequences are already causing significant harm to people, flora, and fauna, making such research crucial for developing strategies for adaptation and damage mitigation [1].

Secondly, climate change research helps to better understand the mechanisms behind these

processes and to predict their future consequences. This enables timely development and implementation of effective policies and technologies aimed at mitigating the effects of climate change, particularly through reducing greenhouse gas emissions, transitioning to renewable energy sources, and preventing natural disasters.

Moreover, climate change research is an important tool for scientific and political discussions that contribute to the formation of global agreements and laws that support sustainable development and environmental protection. Scientific knowledge about climate change allows for more informed decision-making at the levels of international organizations, governments, and local communities.

Furthermore, climate change is not just an environmental issue but also a social and economic one. Different segments of the population, especially vulnerable groups such as poor regions or small island nations, suffer the consequences of climate change much more severely. Research on these phenomena facilitates more effective planning of social support strategies and the provision of viable living conditions for people worldwide [2].

Thus, climate change research is essential for understanding global processes, developing strategies to combat climate change, and ensuring a sustainable future for the planet and all its inhabitants.

Bibliometric analysis provides extensive opportunities for exploring and addressing the issue of climate change. By using this approach, scientific knowledge can be systematized, key research areas can be identified, gaps in science can be pinpointed, and priority fields for further study can be established. Bibliometrics enables an assessment of the interdisciplinary nature of climate change, as these issues encompass various fields of knowledge, from ecology to social sciences. It also helps to identify leading researchers and scientific institutions, as well as to evaluate the impact of scientific work on political decisions and technological innovations [3]. Moreover, bibliometric tools allow for the determination of the contribution of research to achieving the Sustainable Development Goals and contribute to a better under-

standing of the geographical aspects of climate change research. As a result, bibliometrics is an effective tool for examining trends, forming scientific priorities, and enhancing the influence of research on practical solutions in the fight against climate change.

MATERIALS AND METHODS

The data from the Scopus platform on the number of publications related to climate change adaptation, disaster risk reduction, sustainable agriculture practices, and the circular economy were used. Descriptive statistics were performed on studies published between 1991 and 2024. During this period, 1,689 document results were found using these keywords.

Scientometrics is regarded as one of the most significant disciplines within the sciences, defined as an informational process carried out through the quantitative study of science. For the purposes of this study, we adopt the epistemological understanding of science, which encompasses the overall development of the system under analysis, focusing on interrelationships and disciplinary structures. Structural scientometrics, as a component of this field, was approached using bibliometric links, co-citation analysis, and mapping cognitive structures of scientific perceptions.

The goal of this process is to provide an objective overview of how science evolves over time, how it assesses timeliness by identifying key topics of interest in academic work, and how it efficiently organizes research systems, activities, management, and productivity.

The term “bibliometrics” was first coined by Alan Pritchard in 1969 and is considered a statistical and mathematical method focused on books and publications, which is also regarded as a branch of scientometrics[4]. In this study, search results from the Scopus database were exported into text format, including scientific articles on the topics of climate change adaptation, disaster risk reduction, sustainable agricultural practices, and the circular economy. Using the keywords extracted from the database, we obtained unique insights into the publications in Ukraine related to these subjects.

RESULTS

The analysis of trends in scientific research related to climate change issues is one of the key tasks of bibliometrics. With powerful tools for gathering and analyzing data on publications, citations, authors, and institutions, bibliometrics allows not only tracking the quantity of scientific works in a particular field but also determining the qualitative aspects of the research [5].

Firstly, analyzing publication activity helps to understand how the scientific community's interest in climate change has evolved over time. For example, it is possible to trace which aspects of this issue were prioritized in the past, how the focus of contemporary research has shifted, and which directions have potential for further development. Such data reveal patterns in scientific activity: periods of increased publication activity often correlate with the emergence of new methodologies, breakthrough technologies, or global events (such as international climate agreements).

In the case of Ukraine (Fig. 1), a significant increase in the number of articles addressing climate change issues begins only in 2010 (16 articles compared to one in 1991 or 1993).

Furthermore, by using scientometric tools, it is possible to explore emerging topics. For ex-

ample, modern machine learning and text analysis technologies allow publications to be automatically classified by key themes, enabling the identification of the most discussed issues, such as the impact of climate change on biodiversity, climate scenario modeling, or renewable energy research.

An especially important aspect is identifying topics that are developing most dynamically. These are the areas that are just beginning to gain scientific attention but already show high rates of growth in publication and citation numbers. Such "hotspots" in science indicate potential breakthroughs that could significantly change approaches to solving climate change-related issues.

For instance, in the field of climate change research, the subject areas exhibit varying degrees of focus, each contributing a unique perspective to understanding and addressing the complex challenges posed by climate change. Environmental Science, with the highest number of publications (288), is the central field, reflecting its pivotal role in understanding the direct impacts of climate change on ecosystems, environmental processes, and mitigation strategies. Close behind, Earth and Planetary Sciences (207 publications) plays an important role by investigating the physical processes affecting

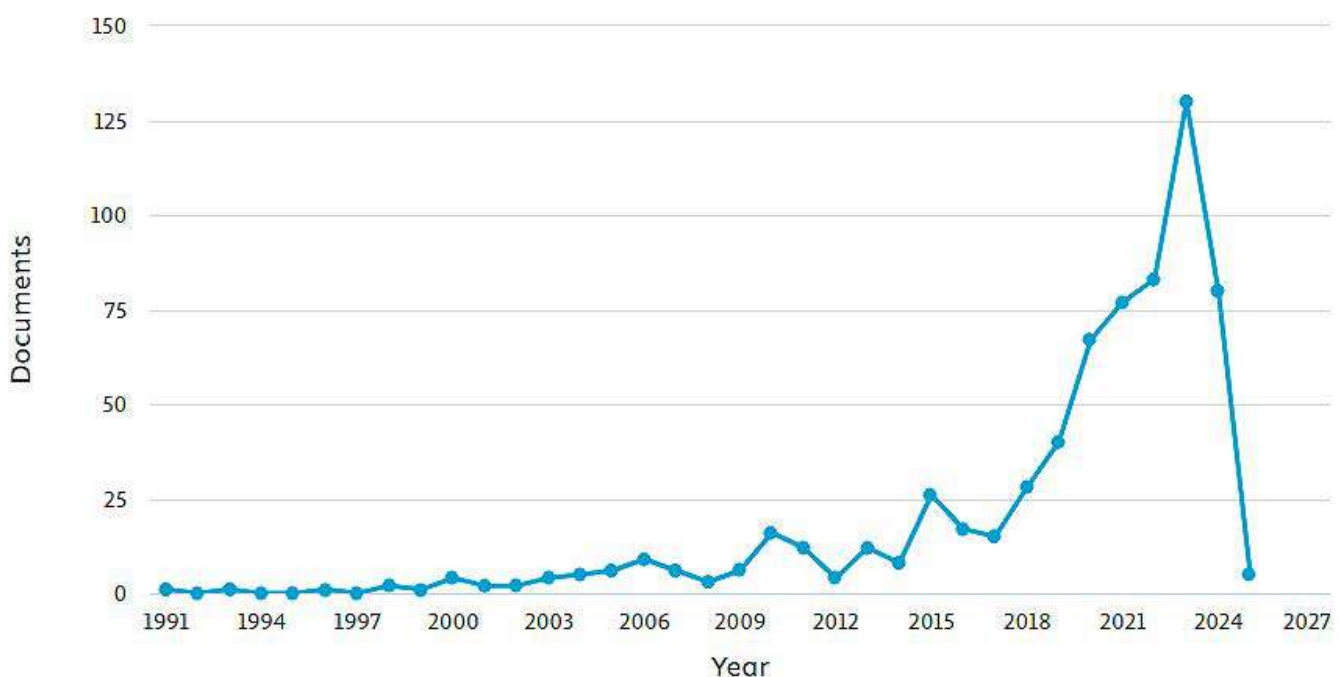


Fig. 1. Dynamics of publications by Ukrainian researchers on climate change (1991–2023)

the Earth, such as atmospheric dynamics and ocean currents, both crucial for climate modeling and predicting future scenarios (Fig 2).

Agricultural and Biological Sciences (166 publications) highlight the growing recognition of the profound effects climate change has on agriculture and biodiversity. Researchers in this area are increasingly focused on how climate variations affect crop yields, biodiversity, and overall food security, making this a vital area of concern. Engineering (117 publications) underscores the importance of technological solutions, with research focusing on climate adaptation technologies, sustainable infrastructure, and green innovations aimed at reducing emissions and enhancing resilience.

The contributions from Nursing (2 publications), Health Professions (1 publication), Neuroscience (1 publication), Psychology (1 publication), and Veterinary (1 publication) are smaller but still significant, focusing on the human and animal health implications of climate change. These fields address issues such as the physical and mental health consequences of climate change, particularly in vulnerable populations, and the impact on animal species and ecosystems.

Overall, the distribution of research across these subject areas reflects the diverse and interconnected nature of climate change challenges. The leading fields like Environmental Science, Earth and Planetary Sciences, and Energy showcase the centrality of understanding the scientific and technological aspects of climate change. Meanwhile, the growing presence of disciplines such as Social Sciences, Economics, and Decision Sciences highlights the increasing recognition of the need for interdisciplinary solutions that address not only the scientific but also the social, economic, and policy-related dimensions of climate change.

At the same time, scientometrics enables the identification of knowledge gaps. For example, regions or aspects of climate change that remain under-researched due to limited resources or data access. This is particularly important for science policy, as such findings can be used to adjust funding or direct resources toward addressing the most urgent or under-explored issues [6].

Thus, analyzing research trends through scientometrics is a powerful tool for forming a comprehensive understanding of the state of scientific activity in the field of climate change. It allows for the comprehension of the dynamics

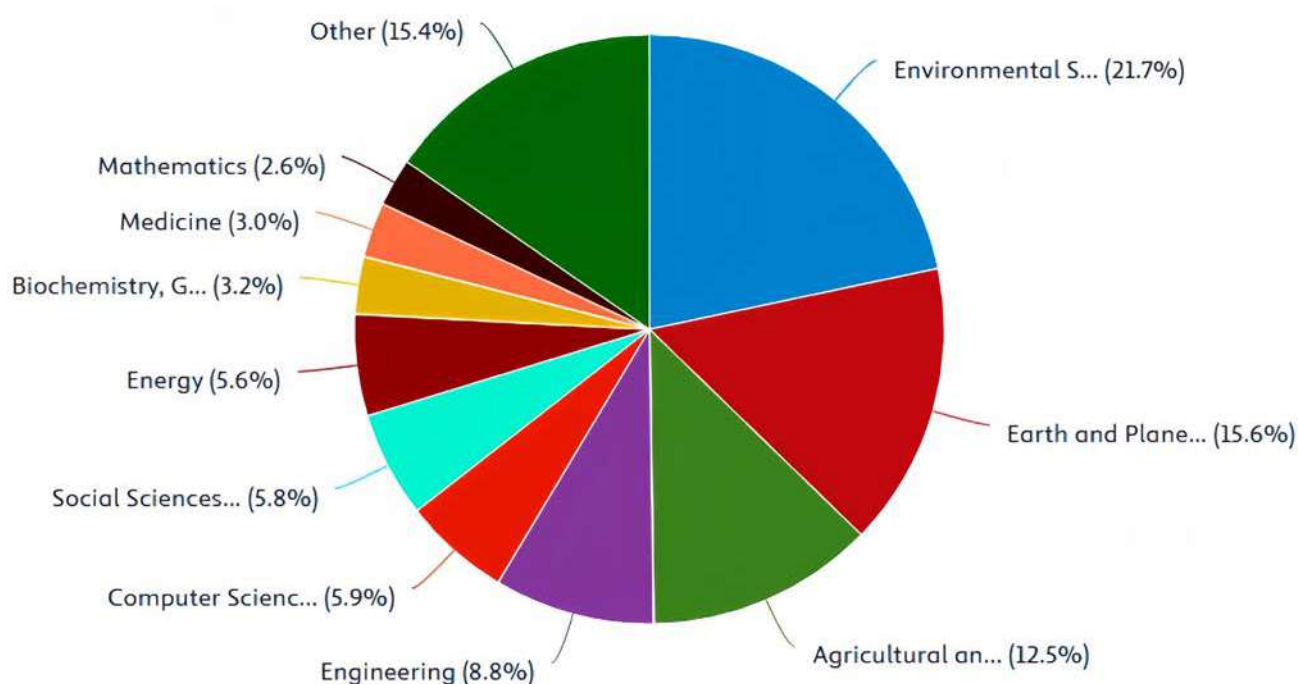


Fig. 2. Documents by subject area

of the subject's development, forecasting future trends, efficiently directing resources toward key issues, and providing strategic support for the most promising areas.

The assessment of interdisciplinarity is a crucial aspect of studying climate change issues, as this global challenge spans a wide range of scientific disciplines and requires the integration of knowledge from different fields. Through scientometrics, it is possible to gain deeper insights into how various scientific areas collaborate to create innovative solutions and identify potential intersection points that remain insufficiently explored.

One of the key advantages of scientometric data is the ability to analyze co-authorship patterns in scientific publications. For example, research with authors from different disciplines, such as ecology and economics or engineering and social sciences, indicates an interdisciplinary approach to solving climate change issues. This type of analysis allows us to identify the most active research groups working at the intersection of fields and explore how they combine their expertise to achieve common goals.

Scientometrics also enables the analysis of publication topics related to climate change in the context of interdisciplinarity. Modern analytical tools allow for the classification of scientific works by keywords, themes, or citations, providing the opportunity to track how certain concepts or technologies migrate between disciplines. For instance, one can detect how engineering methods for assessing greenhouse gas emissions are applied in ecological research, or how economic models are used to forecast the socio-economic impacts of climate change.

An important aspect is also the evaluation of the impact of interdisciplinary research. Scientometrics allows us to measure how such works are cited across other scientific fields, serving as an indicator of their significance and influence on the broader scientific community. For example, studies exploring the relationship between renewable energy sources and economic policy may be cited in both the energy sector and economics, highlighting their interdisciplinary nature and practical value.

Furthermore, the analysis of scientometric data enables the assessment of interactions between institutions working on climate change issues. For example, it is possible to determine how universities, research institutes, and industrial partners collaborate to jointly develop new technologies or adaptation strategies. This information is valuable not only for understanding the structure of scientific cooperation but also for identifying key centers that promote knowledge integration and innovation development.

Ultimately, interdisciplinarity in climate change research is fundamental to creating innovative solutions that address both technical and socio-economic aspects of the problem. Scientometric analysis helps not only to assess the current level of knowledge integration but also to identify new opportunities for cross-sector collaboration, which is a crucial step in addressing the global challenges posed by climate change.

Identifying leading researchers and institutions is one of the key aspects of scientometric analysis, which helps understand who is setting the agenda in climate change research. This process contributes to the identification of scientific leaders, the creation of effective partnerships, and the development of global-level cooperation.

Scientometric tools allow for the analysis of performance indicators of individual researchers and institutions, such as the number of publications, citation index, impact of works in key journals, and collaboration with other organizations. Databases such as Scopus or Web of Science, along with specialized analytical platforms like SciVal or InCites, are used for this purpose. Through these tools, one can identify researchers whose works are most cited in the field of climate change, as well as those making significant contributions to the development of new research directions.

Scientometric analysis also allows for the identification of institutions that are leaders in the field. These could include universities, research centers, government organizations, or international institutions. For example, an analysis of the number of publications or the ratio of quality

Compare the document counts for up to 15 authors.

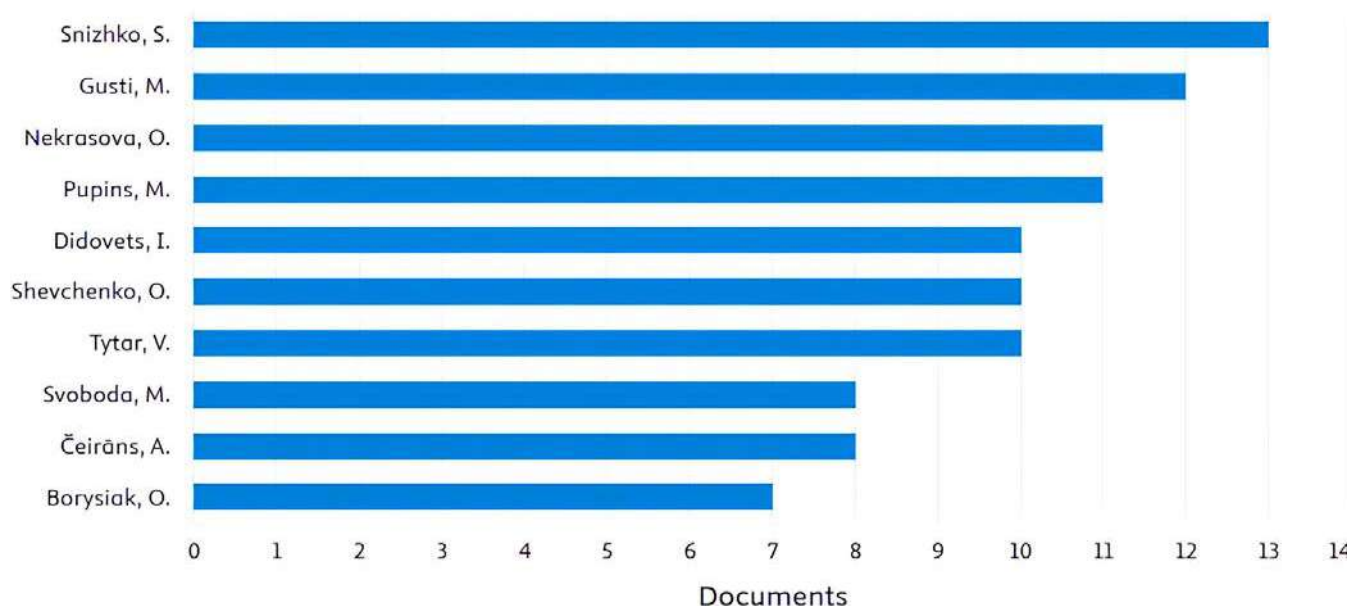


Fig. 3. Documents by authors

to quantity in research can highlight institutions that are actively engaged in climate research and attract significant funding. Additionally, the level of their collaboration with other institutions, such as international universities or non-governmental organizations, can also be assessed.

Identifying leading researchers and institutions has great practical significance. It helps in building scientific consortia for addressing global challenges together. For example, if a group of researchers working on climate change adaptation is identified, cooperation can be initiated between them and institutions involved in developing technologies for reducing greenhouse gas emissions. This approach allows for the integration of expertise from different fields, creating interdisciplinary platforms for innovation.

Moreover, identifying leading scientists contributes to the search for potential mentors for young researchers and strengthens the human resources capacity in the field of climate research. For example, young scientists can collaborate with leaders, learn from their experience and methodologies, which will help foster the development of new generations of climate experts.

In our case, however, researchers from institutions of the National Academy of Sciences

of Ukraine often affiliate themselves with the Academy as a whole rather than with specific research institutions. This presents a challenge for analysis, as it becomes difficult to accurately identify the contributions of individual institutions within the Academy. Many researchers in Ukraine are more likely to emphasize their affiliation with the broader Academy rather than specifying their particular institution, which may lead to a lack of detailed data for scientometric analysis at the institutional level.

This situation complicates the process of identifying leading institutions, as the contributions of individual research centers may be masked by the general affiliation with the Academy. As a result, we may face challenges in tracking collaborative networks, funding sources, and research outputs linked to specific institutions. Additionally, it may hinder the ability to assess the impact of certain institutions on the development of climate research, as the data may not fully reflect the institutional differences within the broader structure of the National Academy of Sciences. This issue highlights the need for more granular data collection and clearer institutional affiliations in order to better understand the contributions of specific re-

Compare the document counts for up to 15 affiliations.

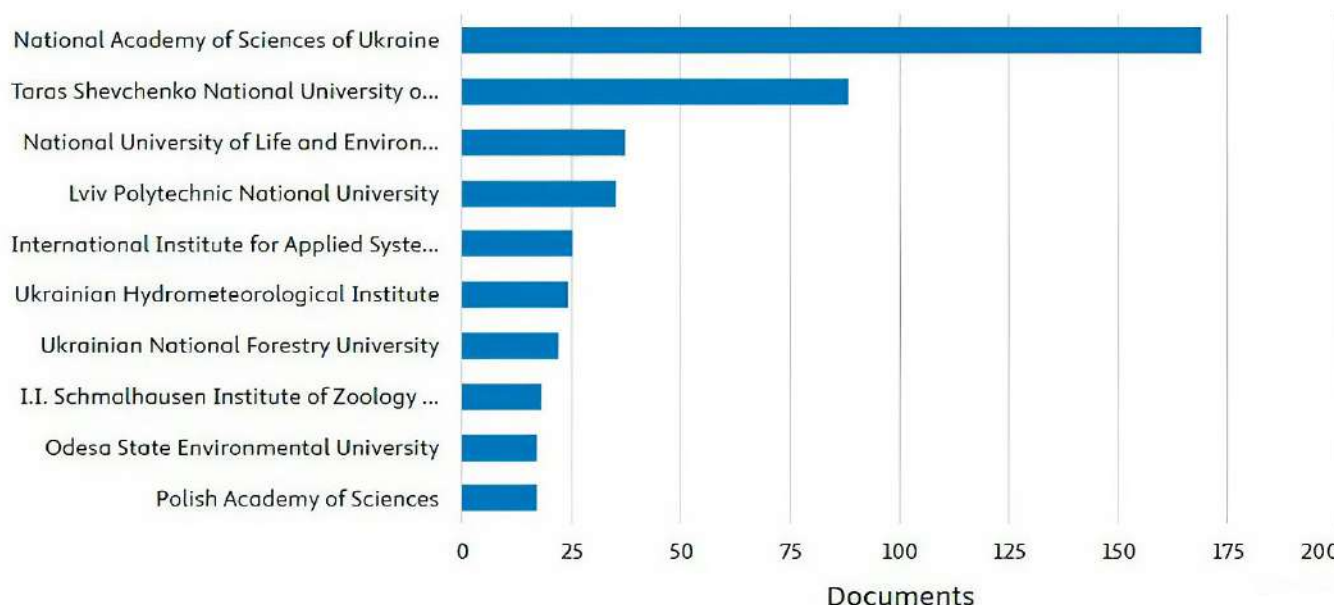


Fig. 4. Documents by affiliations

search institutions to climate change studies in Ukraine.

Another important aspect is the evaluation of the geographical distribution of leading researchers and institutions. Scientometrics allows for the identification of which countries or regions are leaders in climate change research. This is crucial for identifying gaps in global scientific collaboration. For example, the analysis may reveal that some countries with high levels of climate change risk are underrepresented in international research consortia. In such cases, strategies can be developed to involve their scientists and institutions in global initiatives.

Ultimately, identifying leaders in climate change research not only facilitates the formation of partnerships but also creates the conditions for effectively implementing research findings in practical applications. This enables the development of policies and innovations that address the challenges of climate change and have a significant socio-economic impact.

An analysis of the funding for climate change research can offer valuable insights into the global landscape of efforts to tackle this critical issue. By examining the sources and amounts

of financial support directed towards climate-related research, we can identify the leading institutions, countries, and regions involved in this field. Such an analysis also helps uncover disparities in the distribution of funding, shedding light on areas that may require additional resources or support (Fig. 5).

For instance, the European Commission emerges as the largest contributor, with 42 instances of funding, reflecting Europe's strong commitment to addressing climate change. Similarly, the Ministry of Education and Science of Ukraine, with 28 instances, signals the importance of governmental involvement in climate research in Ukraine. This indicates a significant effort on the part of Ukrainian authorities to engage in global climate change initiatives.

The National Science Foundation of the United States (16 instances) and the Horizon 2020 Framework Programme (15 instances) are other notable sources of funding, demonstrating substantial investments from both the U.S. and the European Union in advancing climate research. These contributions highlight the active role played by large international funding bodies in fostering scientific advancements related to climate change.

Compare the document counts for up to 15 funding sponsors.

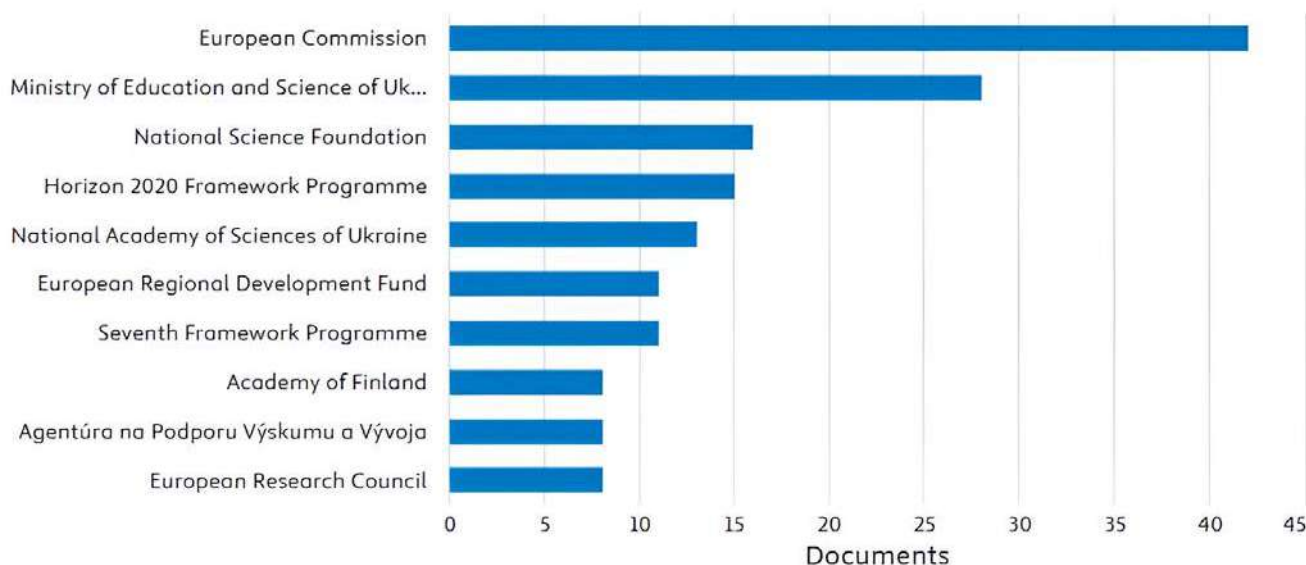


Fig. 5. Documents by funding

Moreover, international funding organizations such as the European Research Council (8 instances) and the National Natural Science Foundation of China (8 instances) emphasize the global nature of the climate research effort. These organizations are crucial in ensuring that both developed and developing nations contribute to and benefit from climate change research, which is essential for achieving a unified global response to climate challenges.

The funding landscape also includes a diverse range of contributors, such as the Bill and Melinda Gates Foundation, NASA, and the National Geographic Society, further illustrating the broad interest in addressing climate change from various sectors, including philanthropy, space agencies, and scientific organizations. This diverse funding ecosystem is critical for driving innovation and collaborative efforts in climate change research.

By analyzing the distribution of funding sources, we gain a clearer understanding of which regions and institutions are currently leading the charge in climate change research. It also helps identify potential gaps in funding or areas where additional resources may be needed. For example, countries at high risk from climate change that are underrepresented in the funding data could be targeted for increased research collabora-

tion and financial support. Overall, such an analysis provides valuable insights into the current state of global climate change research and helps shape future strategies for international cooperation and funding allocation.

Policy impact research is a vital component of scientometric analysis, enabling the evaluation of how scientific results are integrated into the policymaking process addressing climate change. Such analysis is based on the study of citations of scientific works in policy documents, official reports, strategies, government resolutions, and other regulatory acts related to climate change.

Citations of scientific publications in policy documents serve as a direct indicator of how research influences policymaking, particularly in the context of climate adaptation and greenhouse gas emissions reduction. Scientometric analysis, in particular, allows for identifying which scientific works have laid the foundation for developing government strategies, how they were utilized to justify specific policy decisions, and the extent to which they contributed to formulating concrete actions at international, national, or regional levels.

One critical aspect of this analysis is assessing how relevant scientific findings were incorporated into decision-making within a specific

timeframe. This helps reveal the responsiveness of policymakers to new scientific data, reflecting the level of collaboration between scientific and political institutions. The faster scientific results are reflected in policy decisions, the more effective climate adaptation efforts become.

For instance, the analysis can identify which scientific articles, reports, studies, or projects underpinned international climate agreements, such as the Paris Agreement, or national climate strategies. For example, if a scientific publication on climate adaptation strategies served as the basis for developing a national program to strengthen infrastructure or manage water resources, it represents a significant indicator of science's influence on policy.

It is also crucial to consider the type of policy documents citing scientific research. For example, if scientific works are extensively cited in international reports on global climate change, this indicates that the research is internationally recognized and used to shape global policies. Conversely, citations in national reports or strategies may point to more localized integration of scientific findings into policy practices.

This type of analysis also helps identify which academic schools, research institutions, or individual scientists contribute most significantly to shaping climate policy. By examining citations of their works, one can determine who the key drivers of new ideas and concepts influencing state strategies are. These strategies may include cutting-edge technologies for emissions reduction, adaptation strategies for agriculture, or ecosystem management under changing climate conditions.

Policy impact assessment through scientometric methods also highlights potential gaps in scientific research that have yet to be reflected in policy decisions. For example, if certain aspects of climate change, such as impacts on health or biodiversity conservation, receive insufficient attention in policy documents, this may indicate the need for further research and publications to address these gaps.

Scientific influence on climate policy can be measured not only by the number of citations but also by the quality of these citations—that is,

whether scientific research is used to substantiate critical policy steps. This includes evaluating whether scientific works support decisions with long-term effects, such as in the fields of energy, construction, or transport infrastructure.

Thus, scientometric analysis of citations in policy documents is a powerful tool for examining how science shapes climate-related policies and how research findings contribute to effective decision-making, ensuring sustainable development and mitigating the impacts of climate change.

For instance, the Kyoto Protocol served as a catalyst for Ukraine's environmental research and policy development. While the implementation of its mechanisms faced criticism, the Protocol's influence on the scientific community was undeniably positive. The increased volume of research outputs reflects the growing acknowledgment of science as a cornerstone for effective climate action in Ukraine. The alignment of Ukraine's climate commitments with the global scientific agenda created opportunities for international collaboration. Ukrainian scientists contributed to joint research projects, particularly within the frameworks of EU programs, and gained access to funding and expertise through partnerships with foreign institutions. This collaborative approach not only enhanced the quantity of scientific publications but also improved their quality and relevance in addressing global challenges.

The analysis of innovative impact is a key aspect of scientometric research, enabling the evaluation of how scientific studies in the field of climate change are translated into specific technological solutions and innovations for sustainable development. This analysis involves studying patents derived from scientific works and examining their connections to publications to understand how scientific knowledge and research are applied practically in engineering, technology, and industry.

Patents related to climate change often emerge as the result of innovative scientific ideas developed during research. For instance, these could include new water treatment technologies, the development of alternative energy

sources, methods for reducing greenhouse gas emissions, or advancements in eco-friendly materials and products. The innovative impact of scientometric analysis lies in its ability to not only examine patents but also trace their links to scientific publications, thereby identifying the research that leads to the creation of new technologies.

The connection between scientific publications and patents is of great importance since publications often represent the initial stage in the development of innovative ideas. Researchers publish their findings, which can serve as a foundation for subsequent technological advancements. Engineers, technologists, and entrepreneurs can use these publications to create new products and processes that align with the goals of sustainable development and reduced environmental impact.

Patent analysis in the context of climate change helps identify specific technologies that have the greatest impact on addressing climate challenges. For example, patents related to wind and solar power technologies demonstrate how energy research contributes to the development of renewable energy sources. Studying such patents not only provides insights into the volume of innovations but also assesses their practical application in industry and markets.

Through scientometric analysis, it is possible to evaluate the level of innovative activity arising from scientific research. This allows an understanding of whether there is progress in the commercialization of scientific developments and which technologies are most widely adopted in combating climate change. Scientometric approaches also help identify the countries or institutions leading the development of innovations for sustainable development and study the global dissemination of these technologies.

Innovative impact can be assessed not only by the number of patents but also by their social and economic effects. For example, technologies that reduce energy consumption or environmental pollution can foster the creation of new markets, generate jobs, and improve quality of life. Scientometric analysis explores how such innovations are integrated into industry or daily life.

Moreover, analyzing patents in the context of climate change helps identify key institutions actively working on technologies for sustainable development, as well as determining which scientific fields hold the greatest potential for innovation. This analysis also reveals the influence of scientific research on economic and political decisions, as patents can form the basis for new legislative initiatives or innovation support programs aimed at environmental preservation.

Thus, scientometric analysis of the innovative impact of climate change research serves as an important tool for understanding how scientific studies lay the groundwork for technological solutions capable of addressing climate challenges. It enables the evaluation of how scientific ideas are transformed into real innovations with the potential to improve quality of life and ensure sustainable development in the face of climate change.

Contributing to Sustainable Development Goal (SDG) 13, which focuses on combating climate change, is a vital aspect of analyzing scientific research, and scientometric tools provide valuable opportunities to assess this contribution. Through scientometric data, it is possible to identify which studies contribute to solving climate-related challenges and how these studies integrate into the broader context of sustainable development. This approach reveals how scientific efforts in specific areas, such as energy, ecology, technology, and social sciences, help achieve not only SDG 13 but also other interconnected sustainability goals.

Scientometric tools enable the analysis of scientific publications addressing climate change issues and assess their contributions to global initiatives aimed at resolving these challenges. For example, citation analysis can uncover which studies have formed the basis for political strategies or technological developments directly impacting climate change mitigation. Integrating such research into global initiatives or national programs is a key aspect of evaluating their contributions to SDG 13.

Furthermore, scientometric analysis provides insights into how studies from various scientific domains—such as environmental sciences, energy,

urban planning, agriculture, engineering, and social sciences—integrate into broader sustainable development strategies. For instance, scientometric analysis can demonstrate how ecological studies supporting climate adaptation strategies interact with research aimed at improving carbon emission reduction technologies or biodiversity conservation.

Additionally, scientometric methods allow for the assessment of collaboration levels among countries, research institutions, and other stakeholders, which is crucial for achieving global climate goals. These insights can identify key regions or institutions actively working on solutions contributing to SDG 13 and evaluate their influence on policy development, international agreements, or scientific initiatives.

Lastly, analyzing how climate change research aligns with other SDGs—such as SDG 7 (Affordable and Clean Energy), SDG 11 (Sustainable Cities and Communities), or SDG 12 (Responsible Consumption and Production) — is another important aspect. Scientometric data can reveal how climate change studies impact addressing these challenges, highlighting the interconnection between various aspects of sustainable development.

In conclusion, scientometric analysis of contributions to SDG 13 enables the identification of scientific studies with the greatest impact on developing solutions and policies addressing climate change. It also reveals how these studies influence the broader picture of global sustainable development. This tool is indispensable for evaluating the effectiveness of scientific efforts in achieving global goals, ensuring greater transparency, and adopting a strategic approach to solving climate change challenges.

Geographic analysis in scientometrics is a powerful tool for studying territorial features and global patterns of scientific research, particularly those related to climate change. Scientometric analysis allows researchers to trace how scientific work is distributed across different regions of the world, identify zones of high activity, and pinpoint areas where climate change research needs significant intensification. This approach provides a clearer understanding of global trends

and enables targeted intervention by the scientific community, governments, and international organizations to address climate-related challenges.

The analysis of scientometric data makes it possible to determine which regions or countries concentrate the majority of climate change research. It is crucial to identify scientific centers and institutions actively working in this field and to examine the research published in these regions. This analysis reveals regions with high levels of scientific activity and achievements in climate change studies, as well as areas where there is a lack of research in this field. Such insights are especially important to understand where global efforts to combat climate change are underrepresented or need reinforcement.

One of the key advantages of geographic analysis is its ability to highlight regions that are at high risk of climate change impacts but lack sufficient research or development in this area. These may include countries or regions experiencing instability, such as those affected by economic or political crises, or those with limited access to funding for scientific research. In such cases, scientometric analysis can identify the need for intensified scientific initiatives to assess and mitigate climate threats in these areas.

On the other hand, geographic analysis also helps identify countries or regions that are leaders in climate change research. These are places where scientific articles are actively published, new methodologies are developed, or international projects are initiated. Such countries often have advanced scientific infrastructures, numerous universities and research institutions, and strong participation in international scientific collaborations. Identifying these leaders facilitates the exchange of experiences, intellectual resources, and best practices among countries and research institutions.

Regional analysis also uncovers geographic patterns and trends in publications related to specific aspects of climate change, such as temperature fluctuations, sea-level rise, land degradation, or the increasing frequency of extreme weather events. For example, studying publications on climate change in low-lying coastal

areas may reveal a growing body of research on sea-level rise and its impact on ecosystems and populations. Meanwhile, in mountainous regions, researchers may focus on adaptation strategies to changes in precipitation or temperature regimes.

The analysis also identifies key regions that require greater attention from the scientific community, particularly in industrializing countries or rural areas where climate change could have severe socio-economic consequences. These are often territories where the effects of climate change are insufficiently studied or where there is no solid foundation for developing effective adaptation policies.

In conclusion, geographic analysis of scientometric data on climate change opens up critical pathways for further scientific research and practical initiatives. It enables more precise alignment of scientific efforts aimed at addressing specific problems in various parts of the world, facilitates more targeted international collaboration, and optimizes resources for effectively combating climate change on a global scale.

CONCLUSIONS

The bibliometric analysis of scientific research trends related to climate change provides valuable insights into the evolution of research interests and the identification of emerging topics. By tracking the number of publications, citations, authors, and institutions, bibliometrics allows for a comprehensive understanding of the dynamics of scientific activity in the field of climate change. The data reveal key patterns in research, showing how interest in climate change has grown significantly, particularly since 2010, as global awareness and technological advances have driven new methodologies and areas of focus.

The analysis highlights several core areas of research, such as Environmental Science, Earth and Planetary Sciences, and Agricultural and Biological Sciences, which are central to understanding climate change impacts on ecosystems, agriculture, and biodiversity. Other important areas, including Engineering, Social Sciences, and Economics, emphasize the inter-

disciplinary nature of climate change research, highlighting the need for integrated solutions that address both scientific and socio-economic challenges. Furthermore, the presence of research in less-explored fields such as health and veterinary sciences indicates a growing recognition of the broader implications of climate change on human and animal health.

One of the significant advantages of scientometrics is its ability to identify emerging research «hotspots» and knowledge gaps. Areas such as climate scenario modeling, renewable energy, and the socio-economic impacts of climate change are growing rapidly in terms of publication output and citation frequency. At the same time, the identification of under-researched regions or topics enables the strategic allocation of resources and funding to address urgent and underexplored issues in climate change science.

The interdisciplinary approach is essential for solving the complex challenges posed by climate change. Scientometric tools facilitate the identification of collaborative efforts between different scientific fields, such as the intersection of ecology and economics or engineering and social sciences, and measure the impact of such interdisciplinary research on both academic and policy-making circles. This integrated approach is vital for developing innovative solutions that consider both the technical and socio-economic dimensions of climate change.

Furthermore, the identification of leading researchers and institutions plays a critical role in fostering collaboration and global cooperation. By analyzing performance indicators such as publication counts, citation indices, and institutional collaborations, scientometrics helps to identify key players in climate change research, promoting the creation of scientific consortia and partnerships. These collaborations are essential for addressing the global challenges of climate change and for ensuring the effective application of research findings.

The analysis of scientific research trends related to climate change, through the use of bibliometrics, reveals important insights into the development of this critical field. The identification of key areas of focus, such as the growing

attention to environmental science, Earth and planetary sciences, and agriculture, highlights the multifaceted approach required to tackle climate change. It is clear that addressing climate change requires an interdisciplinary effort that spans across different scientific domains, integrating knowledge from environmental sciences, engineering, economics, and social sciences. The growing number of publications in these fields shows an increasing recognition of the complexity of climate challenges.

However, the study also reveals several challenges related to the lack of granularity in institutional data, especially in the context of Ukraine. Many researchers affiliated with the National Academy of Sciences of Ukraine tend to identify with the Academy as a whole rather than with specific institutions. This makes it difficult to accurately track contributions from individual research centers, hindering the ability to evaluate their roles in advancing climate change research. Therefore, improving the collection and reporting of data on institutional affiliations will be critical to refining scientometric analysis and understanding institutional contributions to climate change science in Ukraine.

The analysis of funding sources highlights the central role of international organizations, such as the European Commission and the National Science Foundation of the United States, in supporting climate change research. However, it also reveals potential disparities in the global funding landscape, with certain regions, particularly those most affected by climate change, being underrepresented. Targeted efforts to increase funding for these regions and facilitate international collaborations are necessary to ensure a more equitable global research effort.

Furthermore, the policy impact of scientific research is a crucial element in bridging the gap between scientific discovery and practical application. By evaluating the incorporation of scientific findings into climate policies, it is possible to assess the extent to which research influences decision-making at both national and international levels. Identifying key researchers and institutions whose work shapes climate policy can guide future collaborations and ensure that scientific knowledge is effectively translated into actionable climate strategies.

REFERENCES

1. Bator, A., & Borek, A. (2021). Adaptation to Climate Change under Climate Change Treaties. *International Community Law Review*, 23(2-3), 158-167. <https://doi.org/10.1163/18719732-12341467>
2. Adedeji, O. et al. (2014). Global Climate Change. *Journal of Geoscience and Environment Protection*, 2, 114-122. <http://dx.doi.org/10.4236/gep.2014.22016>
3. Emilio Laino, Roberta Paranunzio, Gregorio Iglesias, Scientometric review on multiple climate-related hazards indices, *Science of The Total Environment*, Volume 945, 2024, 174004, ISSN 0048-9697, <https://doi.org/10.1016/j.scitotenv.2024.174004>.
4. Emilio Laino, Gregorio Iglesias, Scientometric review of climate-change extreme impacts on coastal cities, *Ocean & Coastal Management*, Volume 242, 2023, 106709, ISSN 0964-5691, <https://doi.org/10.1016/j.ocecoaman.2023.106709>.
5. Shivappa Lingappa Sangam, Savitha K S, Climate change and global warming : A scientometric study, June 2019, *Collnet Journal of Scientometrics and Information Management* 13, DOI:10.1080/09737766.2019.1598001, https://www.researchgate.net/publication/332394859_Climate_change_and_global_warming_A_scientometric_study
6. Iancu, T., Tudor, V. C., Dumitru, E. A., Sterie, C. M., Micu, M. M., Smedescu, D., Marcuta, L., Tonea, E., Stoicea, P., Vintu, C., Jitareanu, A. F., & Costuleanu, L. C. (2022). A Scientometric Analysis of Climate Change Adaptation Studies. *Sustainability*, 14(19), 12945. <https://doi.org/10.3390/su141912945>

НАУКОМЕТРИЧНИЙ АНАЛІЗ ПРОБЛЕМ ЗМІНИ КЛІМАТУ: ПРИКЛАД УКРАЇНИ

Анотація. Дослідження зміни клімату має критично важливе значення через її широкомасштабний вплив на екосистеми, економіку та соціальні структури. Зміна клімату, включно з підвищенням температури, підняттям рівня моря, екстремальними погодними явищами та посухами, уже завдає значної шкоди людям, біорізноманіттю та довкіллю, що підкреслює необхідність проведення досліджень для розроблення стратегій адаптації та пом'якшення наслідків. Крім того, розуміння базових механізмів кліматичних процесів є необхідним для прогнозування майбутніх наслідків та створення ефективних політик і технологій. Такі зусилля є ключовими для скорочення викидів парникових газів, переходу до відновлюваних джерел енергії та запобігання природним катастрофам.

Окрім цього, дослідження зміни клімату відіграє важливу роль у глобальних наукових і політичних дискусіях, впливаючи на формування міжнародних угод і законодавства, що підтримують сталий розвиток та охорону довкілля. Наукові знання сприяють ухваленню обґрунтованих рішень на міжнародному, національному та місцевому рівнях, зокрема у створенні стратегій соціальної підтримки для вразливих груп населення, таких як бідні регіони та малі острівні держави.

У цьому дослідженні застосовано бібліометричний аналіз для вивчення наукового ландшафту досліджень зі зміни клімату, зокрема для виокремлення ключових напрямів, визначення прогалів у знаннях і визначення пріоритетних сфер для подальших досліджень. Бібліометрія також допомагає оцінити міждисциплінарний характер досліджень у цій галузі, що охоплює широкий спектр дисциплін — від екології до соціальних наук, — та надає уявлення про внесок наукових досліджень у досягнення Цілей сталого розвитку. Такий підхід сприяє кращому розумінню географічних аспектів досліджень зі зміни клімату, формуванню наукових пріоритетів і підвищенню впливу досліджень на розв'язання практичних проблем.

Для аналізу використано дані платформи Scopus щодо публікацій, присвячених адаптації до зміни клімату, зменшенню ризику стихійних лих, сталим сільськогосподарським практикам і циркулярній економіці. Усього ідентифіковано 1 689 документів за період з 1991 по 2024 рік, за якими проведено описову статистику. У дослідженні застосовано методи структурної наукометрії, включно з аналізом бібліометричних зв'язків, співавторства та спільного цитування, а також картуванням когнітивних структур, що забезпечує комплексне бачення еволюції досліджень зі зміни клімату. Результати показали, що науковий інтерес до цієї тематики суттєво зріс після 2010 року, що стало переломним моментом у глобальному усвідомленні та дослідницькій активності.

Ключові слова: наукометричний аналіз, зміна клімату, Україна.

INFORMATION ABOUT THE AUTHORS

Balanchuk Iryna — Head of the Department, State scientific institution “Ukrainian Institute of Scientific and Technical Expertise and Information” (UkrI STEI), 180, Antonovycha Str., Kyiv, Ukraine, 031507; +38 (044) 521-09-81; e-mail: slavira218@gmail.com, ORCID: 0000-0002-5179-7350

Ihnatsevych Sergiy — Candidate of Economic Sciences, Senior Researcher, State scientific institution “Ukrainian Institute for Scientific Technical Expertise and Information” (UkrI STEI), 180, Antonovycha Str, Kyiv, Ukraine, 031507; e-mail: ignatsevichserg@ukrintei.ua; ORCID: 0000-0002-0401-4325

ІНФОРМАЦІЯ ПРО АВТОРІВ

Баланчук Ірина — зав. відділу міжнародного науково-технічного співробітництва та трансферу технологій, Державна наукова установа «Український інститут науково-технічної експертизи та інформації» (УкрІНТЕІ), вул. Антоновича, 180, м. Київ, Україна, 031507; +38 (044) 521-09-81; e-mail: slavira218@gmail.com, ORCID: 0000-0002-5179-7350

Ігнацевич Сергій — к.е.н., с.н.с. відділу міжнародного науково-технічного співробітництва та трансферу технологій, Державна наукова установа «Український інститут науково-технічної експертизи та інформації» (УкрІНТЕІ), вул. Антоновича, 180, м. Київ, Україна, 031507; e-mail: ignatsevichserg@ukrintei.ua; ORCID: 0000-0002-0401-4325

ЦИФРОВА ТРАНСФОРМАЦІЯ НАУКИ

Алла Жарінова,

докт. екон. наук, проф., в.о. директора ДНТБ України

РЕЦЕНЗІЯ на книгу Наукова комунікація в цифрову епоху: наук.-практ. монографія /Т. Ярошенко, О. Ярошенко, С. Чуканова; за заг.ред. Т. Ярошенко. — Київ: Видавничий дім «Києво-Могилянська академія», 2024. — 463 с.



Монографія «*Наукова комунікація в цифрову епоху*» авторського колективу Тетяни Ярошенко, Олександри Ярошенко та Світлани Чуканової є вчасною та надзвичайно актуальною науково-практичною працею, яка присвячена трансформаціям, що відбуваються у сфері наукової комунікації під впливом цифрових технологій, відкритої науки та інформаційного суспільства.

Авторки пропонують не просто огляд цифрових інструментів, а цілісну аналітичну рамку для осмислення змін у науковому середовищі. У центрі уваги — еволюція практик наукового спілкування, доступу до знань, зберігання та поширення результатів досліджень, з урахуванням принципів відкритості, прозорості, інноваційності та етичної відповідальності. Монографія охоплює широкий спектр тем: від історії наукової комунікації та організації досліджень до сучасних циф-

рових сервісів, наукометрії, академічної доброчесності, відкритих даних і публікацій. Значна увага приділена також практичному виміру — книзі властивий посібниковий підхід, із вправами, прикладами та рекомендаціями, що робить її корисною не лише для дослідників, а й для адміністраторів науки, бібліотекарів, видавців, рецензентів.

Особливої ваги надає роботі те, що вона базується на багаторічному викладацькому та тренінговому досвіді авторок, зокрема в межах курсу «Цифрова наука» в НаУКМА та онлайн-курсу на платформі Prometheus. Такий практичний бекграунд дозволяє подати матеріал структуровано, у доступній формі, не втрачаючи при цьому наукової глибини. У контексті розвитку відкритої науки (Open Science) монографія слугує дороговказом для тих, хто прагне не просто користуватися цифровими інструментами, а й інтегрувати

принципи відкритості у свої дослідницькі практики. Вона також реагує на виклики сучасності: глобалізацію наукового простору, потребу у швидкому та справедливому доступі до знань, вплив COVID-19 на відкритість наукової інформації, а також — етичні дилеми, пов'язані з наукометрією, комерціалізацією видавничого процесу, нерівним доступом до публікацій. Книга відповідає на запит суспільства на більш зрозумілу, доступну та прозору науку. Вона не лише інформує, а

й формує нову дослідницьку культуру, засновану на відкритості, співпраці, цифровій грамотності та сталому доступі до знань.

Книга «*Наукова комунікація в цифрову епоху*» є вагомим внеском у науково-освітній дискурс цифрової трансформації науки. Вона має практичну цінність, наукову новизну та високу прикладну значущість і цілком заслуговує на широку читацьку аудиторію серед науковців, аспірантів, викладачів та управлінців у сфері науки.

*Придбати книжку (друкований чи електронний варіант) можна у Видавничому домі «Києво-Могилянська академія»
(<http://publish-ukma.kiev.ua/ua/>)*