Uniwersytet im. Adama Mickiewicza
w Poznaniu

BIBLIOTEKA 2024, NR 28 (37)
DOI: 10.14746/b.2024.28.10

Standardy oceny repozytoriów danych badawczych: przegląd dostępnych i stosowanych certyfikatów wiarygodności repozytoriów*

Standards for assessing research data repositories: an overview of available and applicable certification systems for trustworthy repositories

Agnieszka Adamiec
Szkoła Główna Gospodarstwa Wiejskiego w Warszawie, Biblioteka Główna
https://orcid.org/0000-0003-3372-258X
e-mail: agnieszka_adamiec@sggw.edu.pl

Abstract. Purpose/Thesis: The amount of digital research data is constantly growing worldwide, and the need to store and share it in a secure environment is becoming apparent. Online platforms called repositories are a widely recognized place to collect research results. From the point of view of the long-term security of the data deposited in them, it is important that repositories meet generally accepted standards, so that they can be counted among the 'trusted repositories'. In addition, providing open access to or at least storing research data in so-called trusted repositories is becoming one of the requirements for proper accounting of scientific research projects. The purpose of this article is to present the result of a review of tools for obtaining certification that confirms the trustworthiness of research data repositories. Certificates which formed the basis for the development of the 2010 *Memorandum of Understanding* were selected (including the necessary update). The number of institutions and their repositories with a current certificate awarded was also checked. **Approach/Methods:** The study applied the method of critical analysis of documentation using normative and informative materials found on the websites of entities that audit and certify digital repositories. **Results and conclusions:** Research has

* Tekst ten pierwotnie, w formie prezentacji, został przedstawiony na Ogólnopolskiej Konferencji Naukowej „Wyzwania w zarządzaniu dokumentacją, informacją i bazami danych" zorganizowanej przez Państwową Akademię Nauk Stosowanych we Włocławku w formie online 6 marca 2024 roku.

shown that, as of now, only about 4% of repositories registered with the international registry of research data repositories re3data.org have at least one current widely recognized certificate. Factors discouraging people from applying for a prestigious certificate may be its price and the lengthy process of evaluating and verifying an application.

Keywords: research data repository, standard for assessing repositories, certification of trustworthiness of digital repositories, ISO 16363, nestor Seal DIN31644, CoreTrustSeal.

Wstęp

Dane badawcze rozumiane jako zasoby cyfrowe, które trzeba odróżniać od publikacji naukowych (artykułów, książek), wytwarzane lub gromadzone w ramach aktywności badawczej oraz spełniające funkcję dowodów, także jako weryfikacja rzetelności badań[1], odgrywają niebagatelną rolę w komunikacji naukowej, co też wybrzmiewa w przytoczonej definicji. Znane są przypadki fałszowania badań[2], w związku z którymi uwidacznia się potrzeba zapewnienia możliwości szybszego wykrycia takich manipulacji dzięki otwartemu dostępowi do danych. Można zauważyć, że fałszowanie wyników nie stanowi problemu, trudno jednak zrobić to bez śladu. Publikowanie danych staje się z tego punktu widzenia sposobem na wykrycie ewentualnego oszustwa.

Najlepszym i najbezpieczniejszym miejscem do przechowywania i udostępniania danych są platformy zwane repozytoriami. Służą one do (samo)publikowania, (samo)archiwizacji i udostępniania bieżącej twórczości intelektualnej społeczności akademickiej. Już od lat 90. XX wieku wraz ze stworzeniem i rozwojem usługi World Wide Web (WWW) platformy te zyskiwały popularność. Najpierw służyły głównie do archiwizacji i udostępniania publikacji, ale z czasem zainteresowano się nimi z uwagi na ich niebagatelną rolę w zapewnieniu bezpieczeństwa danym badawczym.

W związku z rosnącą popularnością repozytoriów coraz ważniejsza stawała się potrzeba poświadczania o ich jakości, tak aby autorzy mogli być pewni, że

[1] Za: Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (wersja przekształcona), Dz.U.UE.L.2019.172.56, https://sip.lex.pl/akty-prawne/dzienniki-UE/dyrektywa-2019-1024-w-sprawie-otwartych-danych-i-ponownego-wykorzystywania-69198138 [dostęp: 23.03.2024]; Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, tekst jedn. Dz. U. 2021, poz. 1641, s. 1, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20210001641/U/D20211641Lj.pdf [dostęp: 23.03.2024].

[2] I. Oransky, A. Marcus, *There's far more scientific fraud than anyone wants to admit*, „The Guardian" 2023, 9 sierpnia, https://www.theguardian.com/commentisfree/2023/aug/09/scientific-misconduct-retraction-watch [dostęp: 25.03.2024].

ich dorobek naukowy przechowywany w wybranych repozytoriach jest rzeczywiście bezpieczny. W literaturze międzynarodowej zaczęły funkcjonować terminy *trusted digital repositories* i *trustworthy repositories*[3].

Co kryje się pod pojęciem „zaufane repozytorium"? Można spotkać się z różnymi definicjami. Zgodnie z dokumentem z 2002 roku zaufane repozytorium to takie, którego misją jest zapewnienie niezawodnego, długoterminowego dostępu do zarządzanych zasobów cyfrowych dla wybranej społeczności, aktualnie i w przyszłości[4].

W jeszcze innej definicji, którą podano w dokumencie stanowiącym przewodnik po programach europejskich 2021–2027[5], dokonano rozróżnienia zaufanych repozytoriów na trzy kategorie, z zastrzeżeniem, że kategorie te mogą się pokrywać:

1) repozytoria certyfikowane (np. CoreTrustSeal, nestor Seal DIN 31644, ISO 16363);
2) repozytoria dyscyplinarne lub dziedzinowe powszechnie używane i uznawane przez międzynarodowe społeczności badawcze;
3) repozytoria ogólnego przeznaczenia, repozytoria instytucjonalne lub inne repozytoria, które mają podstawowe cechy zaufanych repozytoriów, tj.:
   a) charakteryzują się szczególnymi cechami jakości organizacyjnej, technicznej i proceduralnej (na ich stronach internetowych zamieszczane są regulaminy i polityki, które określają ich usługi);
   b) zapewniają szeroki i otwarty dostęp do treści i przestrzegają obowiązujących ograniczeń prawnych i etycznych, w tym umożliwiają przypisanie stałych identyfikatorów (PID, np. DOI, handle i in.) do każdego zbioru danych czy publikacji oraz korzystają ze standardowych schematów metadanych (np. DataCite, Dublin Core i in.), co ułatwia wyszukiwanie, ponowne wykorzystywanie i cytowanie treści;
   c) spełniają ogólnie przyjęte międzynarodowe i krajowe kryteria bezpieczeństwa i ochrony zdeponowanych materiałów przed nieuprawnionym dostępem oraz mają różne poziomy zabezpieczeń w zależności od wrażliwości deponowanych danych.

---

[3] Np. wymienione w dalszej części artykułu dokumenty: *Trusted Digital Repositories: Attributes and Responsibilities*, *Trustworthy Repositories. Audit & Certification: Criteria and Checklist*, *Audit and Certification of Trustworthy Digital Repositories. Recommended practice*.

[4] RLG/OCLC Working Group on Digital Archive Attributes, *Trusted digital repositories: Attributes and responsibilities*, Mountain View 2002, s. 5, http://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf [dostęp: 26.03.2024].

[5] European Commission, *AGA — Annotated Grant Agreement: EU Funding Programmes 2021–2027*, [Brussels] 2023, s. 373–374, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/aga_en.pdf [dostęp: 1.05.2024].

W badaniach posłużono się metodą krytycznej analizy dokumentów. Wykorzystaną metodę należy odróżnić od metody analizy i krytyki piśmiennictwa, polegającej na badaniu publicznie dostępnej literatury fachowej i naukowej, czyli różnego typu opracowań, w celu stworzenia analityczno-syntetycznej relacji z dotychczasowego stanu wiedzy w danym zakresie[6]. Przedmiotem niniejszych badań była dokumentacja i materiały zamieszczone na stronach internetowych podmiotów przeprowadzających audyt i certyfikację repozytoriów cyfrowych, a w szczególności listy kontrolne czy szczegółowe kryteria oceny. Celem badań było zaprezentowanie przeglądu instrumentów pozwalających na uzyskanie certyfikatu potwierdzającego wiarygodność repozytoriów danych badawczych. Sprawdzono również aktualną liczbę repozytoriów, które pomyślnie przeszły proces certyfikacji. W wyniku badań z wykorzystaniem metody krytycznej analizy dokumentów zgromadzono opisowe i ilościowe informacje o badanym zjawisku, czyli narzędziach pozwalających na uzyskanie prestiżowego certyfikatu.

Zarys teoretyczno-historyczny standaryzacji oceny repozytoriów

W grudniu 1994 roku Commission on Preservation and Access (CPA) oraz Research Libraries Group (RLG) utworzyły Grupę Roboczą ds. Archiwizacji Cyfrowej (Task Force on Digital Archiving), w której skład weszli przedstawiciele archiwów narodowych i bibliotek, uniwersytetów, przemysłu, wydawnictw oraz innych organizacji rządowych i sektora prywatnego. Celem tej międzynarodowej grupy było przedstawienie raportu na temat sposobu, w jaki społeczeństwo powinno pracować nad dorobkiem kulturowym tworzonym w formie cyfrowej[7]. W 1996 roku Grupa Robocza ds. Archiwizacji Cyfrowej po raz pierwszy wyraziła potrzebę zainicjowania dialogu na temat standardów, kryteriów i mechanizmów potrzebnych do certyfikowania repozytoriów cyfrowych.

[6] S. Cisek, *Metoda analizy i krytyki piśmiennictwa w nauce o informacji i bibliotekoznawstwie w XXI wieku*, „Przegląd Biblioteczny" 2010, nr 3, s. 274–275.

[7] J. Garrett, D. Waters, *Preserving Digital Information. Report of the Task Force on Archiving of Digital Information*, 1 maja 1996, s. III, http://www.clir.org/pubs/reports/pub63watersgarrett.pdf [dostęp: 26.03.2024].

Open Archival Information System (OAIS)

Niejako w odpowiedzi na wspomniany apel wzywający do identyfikowania i opisywania standardów certyfikacji repozytoriów Consultative Committee for Space Data Systems (CCSDS) – organizacja składająca się z przedstawicieli wielu światowych agencji badań przestrzeni kosmicznej, w tym NASA – opracowała model referencyjny Reference Model for an Open Archival Information System (OAIS)[8]. Wersje robocze modelu referencyjnego zostały udostępnione do przeglądu w maju 1997 i 1999 roku, a opublikowano go w 2002 roku jako Blue Book, co według typologii dokumentów CCSDS oznacza zalecane standardy. W 2012 roku ukazała się druga wersja dokumentu, już jako Magenta Book, czyli zalecane praktyki. Model OAIS został zaakceptowany przez Międzynarodową Organizację Normalizacyjną (ISO) jako norma postępowania w zakresie długoterminowego przechowywania informacji, najpierw w 2003 roku – ISO 14721:2003, a po aktualizacji w 2012 roku – ISO 14721:2012[9]. W 2020 roku CCSDS przekazało ISO do przeglądu nową wersję modelu referencyjnego OAIS w formie Pink Book[10], czyli projektu zaleceń.

Audit and Certification of Trustworthy Digital Repositories: Recommended Practice (norma ISO 16363)

Standard OAIS stał się inspiracją do tworzenia kolejnych dokumentów mających pełnić funkcję instrumentów służących do pomiaru wiarygodności repozytoriów cyfrowych. W roku 2002 z inicjatywy Online Computer Library Center (OCLC) oraz Research Libraries Group (RLG) opublikowano dokument pt. *Trusted Digital Repositories: Attributes and Resposibilities*, w którym podano wymienioną we wstępie definicję repozytorium godnego zaufania. Wspomniane w tytule atrybuty godnych zaufania repozytoriów obejmują:

[8] Na grunt polskiego bibliotekarstwa problematykę standardu OAIS wprowadziła w 2005 roku Aneta Januszko-Szakiel – zob. eadem, *Open Archival Information System (OAIS) – standard w zakresie archiwizacji publikacji elektronicznych*, „Przegląd Biblioteczny" 2005, nr 3.

[9] B. Lavoie, *The Open Archival Information System (OAIS) Reference Model: Introductory Guide. DPC Technology Watch Report 14-02 October 2014 (2nd Edition)*, s. 6, https://www.dpconline.org/docs/technology-watch-reports/1359-dpctw14-02/file [dostęp: 26.03.2024].

[10] Consultative Committee for Space Data Systems, *Reference Model for an Open Archival Information System (OAIS). Draft Recommended Practice*, CCSDS 650.0-P-2.1, Pink Book, October 2020, https://public.ccsds.org/Lists/CCSDS%206500P21/650x0021.pdf [dostęp: 26.03.2024].

zgodność ze standardem OAIS; odpowiedzialność administracyjną; efektywność organizacyjną; stabilność finansową; adekwatność technologiczną i proceduralną; bezpieczeństwo systemu; rozliczalność proceduralną. Obowiązki podzielone są na dwa rodzaje: 1) organizacyjne i opiekuńcze wysokiego szczebla (definiowanie zakresu zbiorów; ochrona i zarządzanie materiałami cyfrowymi przez cały cykl ich życia; dbanie o różne grupy interesariuszy repozytoriów; własność materiałów i inne kwestie prawne; stałe zaangażowanie zasobów pieniężnych); 2) operacyjne (negocjacje z dostawcami treści; uzyskanie kontroli nad materiałami cyfrowymi i ich ochrona; określenie wyznaczonej społeczności użytkowników i dbałość o klarowność dostarczanych informacji; przestrzeganie udokumentowanych zasad i procedur; przestrzeganie dobrych praktyk w zakresie tworzenia zasobów cyfrowych)[11].

W 2007 roku opracowano dokument *Trustworthy Repositories. Audit & Certification: Criteria and Checklist* (TRAC) zawierający poszerzoną listę sprawdzającą wiarygodność repozytoriów na potrzeby ich certyfikacji (opartą na OAIS). Lista kontrolna została podzielona na trzy główne części: 1) ramy organizacyjne, 2) zarządzanie zasobami cyfrowymi oraz 3) technologie, infrastruktura techniczna i bezpieczeństwo[12], co będzie powtarzane w kolejnych dokumentach.

W 2011 roku, na podstawie listy kontrolnej TRAC, CCSDS wydał dokument *Audit and Certification of Trustworthy Digital Repositories. Recommended Practice*[13]. W 2012 roku jego treść została sformalizowana jako norma ISO 16363 (sprawdzona i potwierdzona w 2023 roku)[14].

Dokument *Audit and Certification of Trustworthy Digital Repositories. Recommended Practice*[15] jest podzielony na trzy obszary. Poszczególne kry-

[11] RLG/OCLC Working Group on Digital Archive Attributes, op. cit.

[12] RLG-National Archives and Records Administration Digital Repository Certification Task Force, *Trustworthy Repositories. Audit & Certification: Criteria and Checklist*, Version 1.0, luty 2007, https://www.crl.edu/sites/default/files/d6/attachments/pages/trac_0.pdf [dostęp: 26.03.2024].

[13] Consultative Committee for Space Data Systems, *Audit and Certification of Trustworthy Digital Repositories. Recommended Practice*, CCSDS 652.0-M-1, Magenta Book, September 2011, https://public.ccsds.org/Pubs/652x0m1.pdf [dostęp: 26.03.2024].

[14] W Polsce pierwszą próbę oceny krajowych kolekcji cyfrowych w kontekście kryteriów wiarygodności zaprezentowanych przez międzynarodową grupę roboczą RLG-NARA oraz grupę roboczą do spraw certyfikacji niemieckiego projektu NESTOR podjęto w 2016 roku. Zob. A. Januszko-Szakiel, W. Kowalewski, L. Szafrański, *Polskie biblioteki cyfrowe w kontekście kryteriów wiarygodności archiwów cyfrowych – próba ewaluacji*, w: *Inspiracje i innowacje: zarządzanie informacją w perspektywie bibliologii i informatologii*, red. S. Cisek, Kraków 2016.

[15] Ze względu na wysokie koszty autorka nie dotarła do wydania omawianego dokumentu w formie normy ISO 16363:2012 sprawdzonej i potwierdzonej w 2023 roku.

teria w pewnym stopniu pokrywają się i nie wszystkie mają zastosowanie do każdego typu repozytorium. Pierwszy obszar[16] to ramy organizacyjne, jest w nim mowa o:

1) zarządzaniu i sprawności organizacyjnej (repozytorium ma: misję, strategiczny plan ochrony zasobów cyfrowych, politykę gromadzenia zbiorów),
2) strukturze organizacyjnej i personelu (obowiązki w repozytorium wypełniane są przez odpowiednią liczbę pracowników o odpowiednich umiejętnościach i doświadczeniu),
3) odpowiedzialności proceduralnej i ramach polityki ochrony zasobów cyfrowych (w tym: repozytorium ma wyraźnie określoną docelową grupę użytkowników, repozytorium ma wypracowaną politykę ochrony zasobów cyfrowych, zarządzający repozytorium są zobowiązani do zachowania przejrzystości i rozliczania się ze wszystkich działań wspierających jego funkcjonowanie),
4) stabilności finansowej (w tym: zarządzający repozytorium stosują praktyki i procedury finansowe, które są przejrzyste oraz są kontrolowane przez zewnętrzne podmioty, zarządzający repozytorium są zobowiązani do bieżącego analizowania i raportowania ryzyka finansowego, korzyści, inwestycji i wydatków),
5) umowach, licencjach i zobowiązaniach (w sytuacji, gdy jest to wymagane, zarządzający repozytorium zawierają umowy z właścicielami praw autorskich, w których precyzowane są warunki procesów: przekazywania, przechowywania, udostępniania i wycofywania zasobów cyfrowych, repozytorium zarządza prawami oraz ograniczeniami dotyczącymi wykorzystania zawartości repozytorium).

Drugi obszar – zarządzanie zasobami cyfrowymi – jest podzielony na:

6) pozyskiwanie materiałów (w tym: zarządzający repozytorium określają zakres przechowywanych informacji, repozytorium weryfikuje przekazywane do repozytorium pakiety zasobów cyfrowych (SIP)[17] pod względem kompletności i poprawności),

[16] Szerzej wymienione kryteria i obszary zostały przedstawione w: A. Adamiec, *Model oceny akademickich repozytoriów instytucjonalnych w Polsce w kontekście otwartej nauki*, Warszawa 2023, s. 90–95.

[17] Dla zrozumienia pojęć używanych w tym dokumencie w nawiązaniu do modelu OAIS trzeba wyjaśnić kluczową terminologię przyjętą przez jego autorów: SIP (*submission information package*) – pakiety zasobów cyfrowych (obiekty cyfrowe i metadane opisowe) przekazywane do archiwum w celu dalszego przetworzenia; AIP (*archival information package*) – pakiety zasobów archiwalnych składające się z przechowywanej informacji (*content information*) i jej opisu (*preservation description information*, PDI); DIP (*dissemination information package*) – pakiety udostępniane użytkownikowi.

7) tworzenie pakietów zasobów archiwalnych (AIP) (w tym: zarządzający repozytorium kierują się wcześniej ustaloną instrukcją w procesie przekształcania SIP na AIP, repozytorium ma i stosuje wewnętrzny system, który generuje trwałe i niepowtarzalne identyfikatory dla wszystkich AIP, zarządzający repozytorium dbają, aby przechowywana informacja jako element AIP była zrozumiała dla użytkowników),
8) planowanie ochrony (w tym: w repozytorium stosowana jest udokumentowana, odpowiednia dla zbiorów strategia ich ochrony),
9) ochrona AIP (repozytorium ma dokumentację dotyczącą sposobu przechowywania AIP już na poziomie przed przekształceniem informacji w formę zrozumiałą dla użytkowników),
10) zarządzanie informacjami (w tym: repozytorium umożliwia użytkownikom odnalezienie materiałów będących przedmiotem ich zainteresowania; repozytorium pozyskuje lub tworzy minimalne informacje opisowe i zapewnia, że są one powiązane z AIP),
11) zarządzanie dostępem (zarządzający repozytorium przestrzegają zasad dostępu; pakiet udostępniony użytkownikowi (DIP) odzwierciedla zawartość AIP).

Trzeci obszar – zarządzanie infrastrukturą i ryzykiem bezpieczeństwa – obejmuje:

12) zarządzanie ryzykiem związanym z infrastrukturą techniczną (repozytorium identyfikuje zagrożenia dla swoich działań i celów w zakresie ochrony, związane z infrastrukturą systemu, i zarządza nimi; repozytorium zarządza liczbą i lokalizacją kopii wszystkich materiałów cyfrowych),
13) zarządzanie ryzykiem w zakresie bezpieczeństwa (zarządzający repozytorium prowadzą systematyczną analizę czynników ryzyka; repozytorium ma wdrożone mechanizmy kontrolne, które odpowiednio odnoszą się do każdego ze zdefiniowanych zagrożeń dla bezpieczeństwa; pracownicy repozytorium mają wyznaczone role, obowiązki i uprawnienia związane z wprowadzaniem zmian w systemie; repozytorium ma odpowiedni pisemny plan (oraz jego kopię) gotowości na wypadek awarii i potrzeby odzyskiwania danych, w tym co najmniej jedną kopię zapasową wszystkich zachowanych informacji poza siedzibą).

W *Memorandum of Understanding* uzgodnionym w 2010 roku w wyniku współpracy zarządu Data Seal of Approval (2008–2017; nazwa certyfikatu wydawanego przed opisanym w dalszej części artykułu certyfikatem CoreTrustSeal), CCSDS Repository Audit and Certification Working Group oraz DIN Working Group „Trustworthy Archives – Certification" zaproponowano trzy

poziomy oceny i certyfikacji repozytoriów cyfrowych. „Podstawowa certyfikacja" w ramach ówczesnego Data Seal of Approval oznaczała prostą samoocenę, „rozszerzona certyfikacja" to samoocena sprawdzona pod kątem wiarygodności, natomiast „formalna certyfikacja" to audyt przeprowadzany przez ekspertów zewnętrznych. Rozszerzona i formalna certyfikacja są poszerzonymi wersjami „podstawowej certyfikacji", które mogą być wydawane na podstawie ISO 16363 lub DIN 31644[18] (norma DIN 31644 zostanie omówiona w dalszej części artykułu).

PTAB (Primary Trustable Digital Repository Authorization Body) z siedzibą w Dorset w Wielkiej Brytanii zostało w 2017 roku pierwszą organizacją na świecie upoważnioną do przeprowadzania audytu według normy ISO 16363. Pierwszym repozytorium, które PTAB uhonorowało certyfikatem ISO 16363, było The National Cultural Audiovisual Archives (NCAA) prowadzone przez Indira Gandhi National Centre for the Arts Audio/Visual Repository. Na stronie internetowej PTAB jest obecnie zamieszczona informacja o dwóch repozytoriach z aktualnym certyfikatem ISO 16363 przyznanym przez tę organizację. Są to: od grudnia 2018 roku the U.S. Government Publishing Office oraz od lutego 2024 roku ETERNAL RDC-Arq Digital Repository (Brazylia) z numerem certyfikatu: PTAB-TDRMS 0003. Koszt audytu przeprowadzonego przez PTAB uzależniony jest od wielkości i złożoności repozytorium, a w przybliżeniu może wynieść 14 700 GBP[19]. Natomiast na stronie internetowej Center for Research Libraries (CRL) poświęconej certyfikacji i ocenie repozytoriów cyfrowych zamieszczona jest informacja o sześciu platformach internetowych, które pozytywnie przeszły proces certyfikacji przeprowadzony przez tę organizację w latach 2010–2018. Certyfikacja wykonywana przez CRL oparta jest głównie na wcześniejszej wersji normy ISO 16363: *Trustworthy Repositories. Audit & Certification: Criteria and Checklist* (TRAC)[20].

---

[18] C. Engelhardt, A. Recker, *Trust and the European Framework for Audit and Certification of Digital Repositories, DASISH Workshop on Trust and Certification*, 16–17 October 2014, https://cst.ku.dk/english/projects/closed-projects/dasish/dasishevents/wstrustcertification/2014_10_16_DASISH_trust-ws_Intro_trust_and_MoU-Framework_Recker_Engelhardt.pdf [dostęp: 13.11.2024].

[19] PTAB – Primary Trustworthy Digital Repository Authorisation Body, *Audit Costs*, 2024, http://www.iso16363.org/iso-certification/audit-costs/ [dostęp: 4.05.2024].

[20] Center for Research Libraries. Global Resources Network, *Certification and Assessment of Digital Repositories*, https://www.crl.edu/archiving-preservation/digital-archives/certification-assessment [dostęp: 4.05.2024].

Information und Dokumentation – Kriterien für vertrauenswürdige digitale Langzeitarchive (norma DIN 31644:2012-04)

W Niemczech w wyniku współpracy zespołu RLG-NARA (Research Libraries Group – National Archives and Records Administration) z grupą roboczą do spraw certyfikacji niemieckiego projektu NESTOR opublikowano w 2006 roku bardzo podobny dokument do *Trustworthy Repositories. Audit & Certification: Criteria and Checklist* (TRAC). Druga wersja tego dokumentu z 2008 roku pt. *Kriterienkatalog vertrauenswürdige digitale Langzeitarchive*[21] została sformalizowana w 2012 roku w postaci normy DIN 31644:2012-04 *Information und Dokumentation – Kriterien für vertrauenswürdige digitale Langzeitarchive* – niemieckiego odpowiednika międzynarodowego standardu ISO 16363[22].

Procedura certyfikacji NESTOR oparta na rozszerzonej samoocenie jest bardziej złożona, a jej wyniki oferują większą dokładność niż w przypadku zwykłej samooceny, ale jest prostsza i mniej dokładna niż intensywny audyt przeprowadzony przez zewnętrznych ekspertów w ramach formalnego procesu oceny. Instytucja, która chce uzyskać pieczęć NESTOR Seal, powiadamia NESTOR o swoich planach oceny i wyznacza dwie osoby do kontaktu. Musi również dokładnie określić przedmiot oceny, np. wybrane repozytorium danych badawczych. NESTOR potwierdza instytucji rozpoczęcie kontroli, wyznacza jedną osobę lub więcej osób odpowiedzialnych za kontrolę i ustala odpowiednie dla obu stron terminy. Cały audyt nie powinien trwać dłużej niż trzy miesiące. Narzędzia do samooceny obejmują formularz oceny oraz instrukcje i wyjaśnienia dotyczące poszczególnych kryteriów. W przypadku pytań można kontaktować się z wyznaczoną osobą. NESTOR aktualizuje wymagania w regularnych odstępach czasu. Po zakończeniu samooceny instytucja, która chce otrzymać pieczęć NESTOR Seal, przedstawia swoją dokumentację. Samoocena oraz przedłożone lub przywołane dokumenty muszą być sporządzone w języku niemieckim lub angielskim. Dokumenty zostaną następnie poddane kontroli wiarygodności przez recenzenta NESTOR.

Pieczęć jest ważna po wydaniu pozytywnej oceny, gdy repozytorium opublikuje raport z przeglądu, odpowiedzi na ocenę i wszystkie istotne dokumenty

[21] NESTOR-Arbeitsgruppe, *Kriterienkatalog vertrauenswürdige digitale Langzeitarchive*, Version 2, Frankfurt am Main, November 2008, s. 1–2, https://d-nb.info/1000083241/34 [dostęp: 26.03.2024].

[22] Wart odnotowania jest fakt, że w Polsce pierwszą próbę oceny krajowych kolekcji cyfrowych w kontekście kryteriów wiarygodności zaprezentowanych przez międzynarodową grupę roboczą RLG-NARA oraz grupę roboczą do spraw certyfikacji niemieckiego projektu NESTOR podjęto w 2016 roku. Zob. A. Januszko-Szakiel, W. Kowalewski, L. Szafrański, op. cit.

wraz z pieczęcią w łatwo dostępnym miejscu na swojej stronie internetowej i po dodaniu repozytorium do rejestru certyfikowanych repozytoriów. Pieczęć zawiera rok wydania. Formalnie jest ona ważna bezterminowo, jednak jej znaczenie prawdopodobnie zmniejszy się po kilku latach, chyba że zostanie przeprowadzony kolejny przegląd. Niemniej jednak nie ma wymogu powtarzania procedury[23]. Na stronie internetowej projektu NESTOR zamieszczona jest informacja o czterech repozytoriach, które otrzymały tę pieczęć od roku 2016 (repozytorium TIB – Technische Informationsbibliothek Hannover Leibniz-Informationszentrum Technik und Naturwissenschaften ma dwie takie pieczęcie: z 2017 i 2022 roku). Opłata administracyjna za przeprowadzenie kontroli składanego wniosku wynosi 500 EUR[24].

CoreTrustSeal

CoreTrustSeal jest międzynarodową, pozarządową organizacją non profit promującą zrównoważone i godne zaufania infrastruktury służące przechowywaniu i udostępnianiu danych.

CoreTrustSeal powstał w 2017 roku w wyniku połączenia dwóch podstawowych standardów certyfikacji – Data Seal of Approval (DSA) i World Data System (WDS). W 2013 roku w ramach Research Data Alliance (RDA) zaproponowano utworzenie grupy roboczej ds. audytu repozytoriów i certyfikacji DSA-WDS (Repository Audit and Certification DSA-WDS Partnership Working Group) z wizją zwiększenia wydajności, uproszczenia opcji oceny, stymulowania większej liczby certyfikacji i wzmocnienia wpływu na społeczność. W rezultacie prac grupy roboczej powstały wymagania Core Trustworthy Data Repositories i katalog wspólnych procedur, które stanowią podstawę standardu certyfikacji CoreTrustSeal[25].

CoreTrustSeal oferuje zainteresowanym podmiotom zarządzającym repozytorium danych certyfikację na poziomie podstawowym na bazie Core Trustworthy Data Repositories Requirements. Kryteria CoreTrustSeal zostały dostosowane do krajowych i międzynarodowych wytycznych dotyczących archiwizacji danych cyfrowych, takich jak NESTOR, TRAC i Digital Repository

[23] NESTOR Certification Working Group, *Explanatory notes on the nestor seal for trustworthy digital archives*, lipiec 2013, s. 3–6, https://d-nb.info/1047613859/34 [dostęp: 26.03.2024].

[24] NESTOR, *nestor-Siegel für vertrauenswürdige digitale Langzeitarchive*, https://www.langzeitarchivierung.de/Webs/nestor/DE/Zertifizierung/nestor_Siegel/siegel.html [dostęp: 4.05.2024].

[25] H. L'Hours, M. Kleemola, L. de Leeuw, *CoreTrustSeal. From academic collaboration to sustainable services*, „IASSIST Quarterly" 2019, t. 43 (1).

Audit Method Based on Risk Assessment (DRAMBORA)[26]. W trakcie opracowywania kryteriów został także wzięty pod uwagę dokument określający ramy polityki zarządzania różnymi rodzajami danych badawczych pt. *Stewardship of Digital Research Data: A Framework of Principles and Guidelines*[27], opublikowany przez Research Information Network w 2008 roku.

CoreTrustSeal w swoich kryteriach przyjmuje szeroką perspektywę z punktu widzenia całej organizacji. We wstępie, jeszcze przed częścią właściwą oceny, podana jest prośba o kontekst funkcjonowania badanego repozytorium (m.in. numer identyfikatora w rejestrze repozytoriów danych re3data.org; określenie typu repozytorium; przegląd kluczowych cech repozytorium, odzwierciedlający wybrany typ repozytorium; nazwanie docelowej grupy użytkowników; współpraca i outsourcing). Kolejne szesnaście kryteriów skupia się wokół trzech obszarów: infrastruktura organizacyjna (misja i zakres; zarządzanie prawami; ciągłość usług; kwestie prawne i etyczne; zarządzanie i zasoby; wiedza specjalistyczna i wskazówki), zarządzanie obiektami cyfrowymi (pochodzenie i autentyczność, deponowanie danych i ocena; plan ochrony; zapewnienie jakości; przepływy pracy; wyszukiwanie i identyfikacja; ponowne użycie) oraz technologia informacyjna i bezpieczeństwo (przechowywanie i spójność; infrastruktura techniczna; bezpieczeństwo)[28].

Podstawowy proces certyfikacji CoreTrustSeal nie obejmuje wizyty audytora – polega na samoocenie. Certyfikat traci ważność po trzech latach. Ciągłe dostosowywanie zaleceń i wymagań ma zapewnić, że certyfikat zachowuje aktualność w ciągle zmieniającym się środowisku cyfrowym. Za wydanie certyfikatu CoreTrustSeal pobierana jest opłata administracyjna, która 1 lutego 2024 roku wzrosła z 1 tys. EUR do 3 tys. EUR[29]. Z uwagi na cenę i rygorystyczny, długotrwały proces oceny na tę chwilę (maj 2024 roku) jedynie 118 repozytoriów danych badawczych na całym świecie może poszczycić się ważnym

[26] DRAMBORA to metoda kontroli repozytoriów cyfrowych oparta na szacowaniu ryzyka wyrażonego w kategoriach prawdopodobieństwa i potencjalnego wpływu. Narzędzie służące do określenia słabych i mocnych punktów repozytoriów zostało przygotowane przez Digital Curation Centre (DCC) oraz DigitalPreservationEurope (DPE). Na stronie internetowej DCC zamieszczono informację, że organizacja ta nie wspiera już narzędzia DRAMBORA – zob. DCC, *DRAMBORA*, https://www.dcc.ac.uk/tools/drambora [dostęp: 4.05.2024].

[27] Research Information Network, *Stewardship of Digital Research Data: A Framework of Principles and Guidelines*, London 2008, http://shapingthefuture.pbworks.com/f/Stewardship+of+digital+research+data+by+RIN.pdf [dostęp: 4.05.2024].

[28] CoreTrustSeal Standards and Certification Board, *CoreTrustSeal Trustworthy Digital Repositories Requirements 2023–2025. Extended Guidance*, V01.00, 2022, https://doi.org/10.5281/zenodo.7051095.

[29] CoreTrustSeal, *Administrative fee*, 2024, https://www.coretrustseal.org/apply/administrative-fee/ [dostęp: 23.03.2024].

certyfikatem CoreTrustSeal. Wśród nich znajdują się obecnie dwa polskie repozytoria danych badawczych: od października 2023 roku MOST Wiedzy Open Research Data Catalog i od marca 2024 roku Repozytorium Cyfrowe Instytutów Naukowych.

Omówione wcześniej normy ISO 16363 i DIN 31644 odnoszą się zarówno do repozytoriów publikacji, jak i do repozytoriów danych badawczych. CoreTrustSeal natomiast został opracowany z myślą o repozytoriach przechowujących i udostępniających dane.

Zakończenie

W latach 20. XXI wieku prawie każdy rezultat badań naukowych jest obiektem cyfrowym lub zostaje przekształcony w taki format. Zabezpieczanie obiektów elektronicznych wiąże się z szeregiem wyzwań – do istotniejszych należą szybkie starzenie się sprzętu i oprogramowania komputerowego czy problemy z odczytem łatwych do uszkodzenia nośników. Trzeba zauważyć, że zadanie długotrwałego przechowywania i udostępniania obiektów cyfrowych jest technicznie możliwe, ale złożone.

W związku ze wzrostem znaczenia repozytoriów coraz ważniejsza staje się konieczność potwierdzania ich jakości, aby budować zaufanie wśród autorów deponujących w nich swój dorobek naukowy. Dodatkowo jednym z wymogów właściwego rozliczania większości projektów jest udostępnienie lub przynajmniej przechowywanie danych badawczych w tzw. zaufanych repozytoriach. W przypadku Narodowego Centrum Nauki coraz częściej wspomina się o planach wprowadzenia obligatoryjności wybierania przez beneficjentów tej agencji finansującej naukę wyłącznie certyfikowanych repozytoriów. Niewątpliwie audyt i certyfikacja są najlepszym sposobem na poświadczenie jakości sprawdzanego repozytorium. Ciekawa i ważna może być jednak odpowiedź na pytanie o aktualny stan wykorzystania narzędzi do certyfikacji przez zarządzających repozytoriami.

W artykule zaprezentowano przegląd instrumentów pozwalających na uzyskanie certyfikacji potwierdzającej wiarygodność repozytoriów danych badawczych. Dodatkowo zwrócono uwagę na listę instytucji i ich repozytoriów, które mogą pochwalić się przynajmniej jednym z dostępnych i szeroko uznanych certyfikatów. Wyniki badania pokazały, że obecnie tylko 124 repozytoria na całym świecie mają przynajmniej jeden aktualny certyfikat. Dla porównania w rejestrze repozytoriów danych badawczych re3data.org zaindeksowanych zostało ponad 3200 systemów repozytoryjnych.

Jednym z czynników zniechęcających do ubiegania się o prestiżowy certyfikat może być jego cena. Spośród badanych instrumentów najbardziej

przystępna cenowo jest pieczęć NESTOR, certyfikat oparty na niemieckim odpowiedniku międzynarodowej normy ISO 16363. Jednak pomimo niezbyt wygórowanej ceny tylko cztery repozytoria mają ten certyfikat, w tym jedno holenderskie (DANS). Koszty wydania certyfikatu CoreTrustSeal wzrosły w 2024 roku do 3 tys. EUR, dodatkowo ważność tego certyfikatu kończy się już po trzech latach. Z wypowiedzi osób, których repozytoria przechodziły proces tej certyfikacji, wynika, że procedura oceny i weryfikacji CoreTrustSeal może się przeciągać nawet do ponad dwóch lat. W związku z tym trzeba przyznać, że w tym wypadku liczba 118 certyfikowanych repozytoriów na świecie i tak nie jest bardzo mała. Trzeci z instrumentów certyfikacji, który umożliwia formalny, czyli pełny audyt, jest najdroższy – ok. 14 700 GBP. Certyfikat ISO również przestaje być ważny po trzech latach, a dodatkowo istnieje wymóg corocznych audytów nadzoru. Warto przypomnieć, że aktualnie tylko dwa repozytoria mogą poszczycić się tym certyfikatem, przy czym od 2017 roku, od czasu upoważnienia PTAB do przeprowadzania audytu według normy ISO 16363, tylko trzy repozytoria uzyskały ten certyfikat.

Warto w tym miejscu powtórzyć, że CoreTrustSeal służy do certyfikacji repozytoriów danych badawczych, natomiast normy ISO 16363 i DIN 31644 stanowią instrumenty oceny każdego typu repozytorium, także publikacji.

Do pełnego obrazu stanu wykorzystania przez zarządzających repozytoriami narzędzi do certyfikacji brakuje informacji o liczbie zgłoszeń, które nie przeszły procesu oceny z pozytywnym wynikiem – to wprawdzie nie należało do zakresu tego artykułu, ale niewątpliwie może stanowić punkt wyjścia dalszych badań. Pozostaje wątpliwość, czy mała liczba certyfikowanych repozytoriów związana jest z równie niewielką liczbą zgłoszeń do procesu certyfikacji, czy jednak większą liczbą negatywnie ocenionych systemów repozytoryjnych.

Niewątpliwie wymóg deponowania danych tylko w repozytoriach z powszechnie uznanym certyfikatem mógłby podnieść liczbę podmiotów ubiegających się o taki certyfikat. Wydaje się jednak, że środowisko naukowe nie jest jeszcze na to gotowe, ponieważ taki krok znacznie zawęziłby liczbę możliwych do wyboru repozytoriów i mógłby wprowadzić zamieszanie wśród naukowców, już teraz często mających problem ze znalezieniem zaufanego repozytorium. Warto też zwrócić uwagę na to, że definicja zaufanego repozytorium wciąż obejmuje wiele zróżnicowanych repozytoriów, a nie koncentruje się tylko na tych z przyznanym certyfikatem.

Bibliografia – References

Adamiec A., *Model oceny akademickich repozytoriów instytucjonalnych w Polsce w kontekście otwartej nauki*, Warszawa: Szkoła Główna Gospodarstwa Wiejskiego 2023.

Center for Research Libraries. Global Resources Network, *Certification and Assessment of Digital Repositories*, https://www.crl.edu/archiving-preservation/digital-archives/certification-assessment [dostęp: 4.05.2024].

Cisek S., *Metoda analizy i krytyki piśmiennictwa w nauce o informacji i bibliotekoznawstwie w XXI wieku*, „Przegląd Biblioteczny" 2010, nr 3, s. 274–275. DOI: https://doi.org/10.36702/pb.411

Consultative Committee for Space Data Systems, *Audit and Certification of Trustworthy Digital Repositories. Recommended Practice*, CCSDS 652.0-M-1, Magenta Book, September 2011, https://public.ccsds.org/Pubs/652x0m1.pdf [dostęp: 26.03.2024].

Consultative Committee for Space Data Systems, *Reference Model for an Open Archival Information System (OAIS). Draft Recommended Practice*, CCSDS 650.0-P-2.1, Pink Book, October 2020, https://public.ccsds.org/Lists/CCSDS%206500P21/650x0021.pdf [dostęp: 26.03.2024].

CoreTrustSeal, *Administrative fee*, 2024, https://www.coretrustseal.org/apply/administrative-fee/ [dostęp: 23.03.2024].

CoreTrustSeal Standards and Certification Board, *CoreTrustSeal Trustworthy Digital Repositories Requirements 2023–2025. Extended Guidance*, V01.00, 2022. DOI: https://doi.org/10.5281/zenodo.7051095

DCC, *DRAMBORA*, https://www.dcc.ac.uk/tools/drambora [dostęp: 4.05.2024].

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (wersja przekształcona), Dz.U.UE.L.2019.172.56, https://sip.lex.pl/akty-prawne/dzienniki-UE/dyrektywa-2019-1024-w-sprawie-otwartych-danych-i-ponownego-wykorzystywania-69198138 [dostęp: 23.03.2024].

Engelhardt C., Recker A., *Trust and the European Framework for Audit and Certification of Digital Repositories, DASISH Workshop on Trust and Certification*, 16–17 October 2014, https://cst.ku.dk/english/projects/closed-projects/dasish/dasishevents/wstrustcertification/2014_10_16_DASISH_trust-ws_Intro_trust_and_MoU-Framework_Recker_Engelhardt.pdf [dostęp: 13.11.2024].

European Commission, *AGA — Annotated Grant Agreement: EU Funding Programmes 2021–2027*, [Brussels] 2023, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/aga_en.pdf [dostęp: 26.03.2024].

Garrett J., Waters D., *Preserving Digital Information. Report of the Task Force on Archiving of Digital Information*, 1 maja 1996, s. III, http://www.clir.org/pubs/reports/pub63watersgarrett.pdf [dostęp: 26.03.2024].

Januszko-Szakiel A., *Open Archival Information System (OAIS) – standard w zakresie archiwizacji publikacji elektronicznych*, „Przegląd Biblioteczny" 2005, nr 3, s. 341–358, https://pliki.sbp.pl/ac/259_pb2005z3.pdf#page=68 [dostęp: 2.05.2024].

Januszko-Szakiel A., Kowalewski W., Szafrański L., *Polskie biblioteki cyfrowe w kontekście kryteriów wiarygodności archiwów cyfrowych – próba ewaluacji*, w: *Inspiracje i innowacje: zarządzanie informacją w perspektywie bibliologii i informatologii*, red. S. Cisek, Kraków: Biblioteka Jagiellońska 2016, s. 189–224, https://ruj.uj.edu.pl/server/api/core/bitstreams/e56c80d8-c320-41d2-a6c1-959c3bb25f1e/content [dostęp: 15.07.2024].

Lavoie B., *The Open Archival Information System (OAIS) Reference Model: Introductory Guide. DPC Technology Watch Report 14-02 October 2014 (2nd Edition)*, s. 6, https://www.dpconline.org/docs/technology-watch-reports/1359-dpctw14-02/file [dostęp: 26.03.2024].

L'Hours H., Kleemola M., de Leeuw L., *CoreTrustSeal: From academic collaboration to sustainable services*, „IASSIST Quarterly" 2019, t. 43 (1), s. 1–17. DOI: https://doi.org/10.29173/iq936

NESTOR-Arbeitsgruppe, *Kriterienkatalog vertrauenswürdige digitale Langzeitarchive*, Version 2, Frankfurt am Main, November 2008, https://d-nb.info/1000083241/34 [dostęp: 26.03.2024].

NESTOR Certification Working Group, *Explanatory notes on the nestor seal for trustworthy digital archives*, lipiec 2013, s. 3–6, https://d-nb.info/1047613859/34 [dostęp: 26.03.2024].

NESTOR, *nestor-Siegel für vertrauenswürdige digitale Langzeitarchive*, https://www.langzeitarchivierung.de/Webs/nestor/DE/Zertifizierung/nestor_Siegel/siegel.html [dostęp: 4.05.2024].

Oransky I., Marcus A., *There's far more scientific fraud than anyone wants to admit*, „The Guardian" 2023, 9 sierpnia, https://www.theguardian.com/commentisfree/2023/aug/09/scientific-misconduct-retraction-watch [dostęp: 25.03.2024].

PTAB – Primary Trustworthy Digital Repository Authorisation Body, *Audit Costs*, 2024, http://www.iso16363.org/iso-certification/audit-costs/ [dostęp: 4.05.2024].

Research Information Network, *Stewardship of Digital Research Data: A Framework of Principles and Guidelines*, London 2008, http://shapingthefuture.pbworks.com/f/Stewardship+of+digital+research+data+by+RIN.pdf [dostęp: 4.05.2024].

RLG-National Archives and Records Administration Digital Repository Certification Task Force, *Trustworthy Repositories. Audit & Certification: Criteria and Checklist*, Version 1.0, luty 2007, https://www.crl.edu/sites/default/files/d6/attachments/pages/trac_0.pdf [dostęp: 26.03.2024].

RLG/OCLC Working Group on Digital Archive Attributes, *Trusted digital repositories: Attributes and responsibilities*, Mountain View 2002, http://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf [dostęp: 26.03.2024].

Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (tekst jedn. Dz. U. 2021 poz. 1641), https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20210001641/U/D20211641Lj.pdf [dostęp: 23.03.2024].

Agnieszka Adamiec

Standardy oceny repozytoriów danych badawczych: przegląd dostępnych i stosowanych certyfikatów wiarygodności repozytoriów

Streszczenie. Na świecie nieustannie rośnie liczba cyfrowych danych badawczych, co wywołuje potrzebę ich przechowywania i udostępniania w bezpiecznym środowisku. Platformy internetowe nazywane repozytoriami są powszechnie uznanym miejscem gromadzenia wyników badań naukowych. Z punktu widzenia długotrwałego bezpieczeństwa deponowanych w nich danych ważne jest, by repozytoria spełniały ogólnie przyjęte standardy, dzięki czemu można wliczać je w poczet „zaufanych repozytoriów". Dodatkowo coraz częściej udostępnienie lub przynajmniej przechowywanie danych badawczych w tzw. zaufanych repozytoriach staje się jednym z wymogów właściwego rozliczania projektów naukowo-badawczych. **Celem** autorki jest zaprezentowanie wyniku przeglądu narzędzi pozwalających na uzyskanie certyfikacji potwierdzającej wiarygodność repozytoriów danych badawczych. Wybrano certyfikaty, które stały się podstawą opracowania *Memorandum of Understanding* uzgodnionego w 2010 roku (z uwzględnieniem koniecznej aktualizacji). Sprawdzono również liczbę instytucji i ich repozytoriów z przyznanym aktualnym certyfikatem. W badaniu zastosowano **metodę** krytycznej analizy dokumentów z wykorzystaniem materiałów o charakterze normatywnym i informacyjnym znajdujących się na stronach internetowych podmiotów przeprowadzających audyt i certyfikację repozytoriów cyfrowych. **Rezultaty:** badania wykazały, że na chwilę obecną tylko ok. 4% repozytoriów zarejestrowanych w międzynarodowym rejestrze repozytoriów danych badawczych re3data.org ma przynajmniej jeden aktualny szeroko uznany certyfikat. Czynnikami zniechęcającymi do starania się o prestiżowy certyfikat mogą być jego cena oraz długotrwały proces oceny i weryfikacji zgłoszenia.

Słowa kluczowe: repozytorium danych badawczych, standard oceny repozytoriów, certyfikacja wiarygodności repozytoriów cyfrowych, ISO 16363, nestor Seal DIN31644, CoreTrustSeal.

Tekst wpłynął do Redakcji 29 maja 2024 roku.

Agnieszka Adamiec – dr, absolwentka dwóch kierunków studiów: informacji naukowej i bibliotekoznawstwa oraz filologii polskiej na Uniwersytecie Jana Kochanowskiego w Kielcach. W 2022 roku obroniła z wyróżnieniem doktorat na Uniwersytecie Warszawskim (temat rozprawy: *Model oceny akademickich repozytoriów instytucjonalnych w Polsce w kontekście otwartej nauki*). Od 2015 roku pracuje w Bibliotece Głównej Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie, w której od 2023 roku jest kierownikiem Oddziału Otwartych Zasobów Nauki. Jej zainteresowania naukowe skupiają się wokół zagadnień zarządzania wiedzą i informacją, otwartości w nauce, wyszukiwania informacji, oceny jakości systemów i zasobów informacyjnych.