



Proaktywne zarządzanie ryzykiem w archiwach cyfrowych w świetle zmian modelu referencyjnego Open Archival Information System (OAIS) z 2024 r.

Aneta Januszko-Szakiel

Uniwersytet Jagielloński / Jagiellonian University (Poland)
aneta.januszko-szakiel@uj.edu.pl, ORCID 0000-0002-9309-8136

STRESZCZENIE

Niniejszy artykuł stanowi analizę i charakterystykę trzeciej edycji modelu referencyjnego Open Archival Information System OAIS z 2024 r. (CCSDS 650.0-M-3). Celem opracowania jest zwrócenie uwagi na paradygmatyczne przesunięcie procesów długoterminowej archiwizacji od pasywnego składowania danych w stronę proaktywnego, mierzalnego i opartego na dowodach zarządzania zasobem cyfrowym, ze szczególnym uwzględnieniem zarządzania ryzykiem. Zastosowanie metody jakościowej analizy treści, pomocniczo również metody analizy i krytyki piśmiennictwa, umożliwiło wskazanie kluczowych zmian w modelu OAIS 2024, które mają przełożenie na praktykę archiwizacji cyfrowej. Nowa edycja modelu skłania środowisko kuratorów cyfrowych do zmiany myślenia o zadaniach archiwizacji cyfrowej oraz do działań na rzecz modernizacji archiwów cyfrowych.

SŁOWA KLUCZOWE

archiwizacja
cyfrowa, model
referencyjny OAIS
2024, proaktywne
zarządzanie
ryzykiem
w archiwach
cyfrowych

Proactive risk management in digital archives in the Light of the 2024 revisions to the Open Archival Information System (OAIS) Reference Model

ABSTRACT

This article presents an analysis and characterization of the third edition of the Open Archival Information System (OAIS) reference model, released in 2024 (CCSDS 650.0-M-3). The study aims to delineate a paradigmatic shift in long-term preservation – moving from passive data storage toward proactive, measurable, and evidence-based management of digital assets, with a particular emphasis on risk management. Utilizing qualitative content analysis alongside literature review and critique, the author identifies pivotal changes in the OAIS 2024 model that impact digital archiving practices. This new edition encourages digital curators to re-evaluate digital preservation tasks and modernize digital archives.

KEYWORDS

digital archiving,
OAIS 2024
reference model,
proactive risk
management in
digital archives

Wprowadzenie

W dobie cyfrowej transformacji, powszechności cyfryzacji zasobów i automatyzacji procesów zarządzanie ryzykiem przestaje być zadaniem pobocznym, a staje się osią, wokół której należy orientować konkretne działania i funkcje systemów zarządzania obiektami cyfrowymi. Poszukiwanie przedmiotowych wzorców, rozwiązań i dobrych praktyk staje się ważnym zadaniem instytucji i organizacji działających na rzecz trwałej ochrony narodowych dóbr kultury i nauki. Przyjęto zatem założenie, że adekwatnym źródłem rekomendacji dla archiwistów cyfrowych w dobie zmian może okazać się model Open Archival Information System (dalej: OAIS) w jego najnowszej odsłonie z 2024 r.

Celem artykułu jest analiza i charakterystyka trzeciej wersji modelu referencyjnego. Szczególną uwagę zwrócono na kontekst zarządzania ryzykiem w archiwach cyfrowych. Na podstawie jakościowej analizy treści modelu referencyjnego oraz – pomocniczo – analizy i krytyki piśmiennictwa zauważono paradygmatyczne przesunięcie procesów długoterminowej archiwizacji od pasywnego składowania danych i reaktywnego reagowania na zagrożenia w archiwach cyfrowych do proaktywnego, mierzalnego i opartego na dowodach zarządzania przyjętymi celami i ryzykiem. Zmiana ta zdecydowanie niesie za sobą określone implikacje dla instytucji i organizacji działających na rzecz ochrony dziedzictwa cyfrowego. Aktualizacja modelu wydaje się stanowić w Polsce temat otwarty badawczo, a zarazem szczególnie obiecujący dla studiów nad kuratorstwem cyfrowym.

OAIS jako model długoterminowej archiwizacji zasobów cyfrowych – geneza i ewolucja

Analizowany model referencyjny, usankcjonowany międzynarodową normą ISO 14721, stanowi od ponad dwóch dekad fundament teorii i praktyki długoterminowej archiwizacji zasobów cyfrowych¹. Od wersji pierwszej z 2002 r.²,

¹ ISO 14721:2012 *Space data and information transfer systems – Open archival information system (OAIS) – Reference model*; A. Januszko-Szakiel, *Open Archival Information System – standard w zakresie archiwizacji publikacji elektronicznych*, „Przegląd Biblioteczny” 2005, r. 73, z. 3, s. 341–358; eadem, *Archiwistyka cyfrowa. Długoterminowa ochrona dziedzictwa nauki i kultury*, Warszawa 2017, s. 39–47.

² Consultative Committee for Space Data Systems, *Historical Document. Recommendation for Space Data System Standards. Reference Model for an Open Archival Information System (OAIS) CCSDS 650.0-B-1*, 2002, <https://ccsds.org/Pubs/650x0b1s.pdf> [dostęp: 30.04.2026].

poprzez aktualizację w 2012 r.³, OAIS ewoluował, reagując na zmieniający się krajobraz technologiczny, rosnącą złożoność obiektów cyfrowych oraz dynamikę społeczności użytkowników archiwów cyfrowych. Rok 2024 przyniósł publikację trzeciej edycji standardu (*Consultative Committee for Space Data Systems, CCSDS 650.0-M-3*), która rok później została oficjalnie przyjęta przez Międzynarodową Organizację Normalizacyjną jako ISO 14721:2025⁴. Wersja z 2024 r. to efekt wieloletnich międzynarodowych dyskusji i konsultacji mających na celu dostosowanie modelu do ery wielkich zbiorów danych, chmur obliczeniowych i rosnącej potrzeby automatyzacji procesów kuratorstwa cyfrowego.

Zgodnie z modelem OAIS długoterminowa archiwizacja „oznacza nie tylko gromadzenie i przechowanie materiału cyfrowego w długim czasie, ale przede wszystkim zapewnienie jego długoterminowej użyteczności, rozumianej jako dostępność, możliwość odczytania i prezentacji jego treści w formie zrozumiałej dla użytkownika, zarówno obecnie, jak i w najbardziej odległej przyszłości”⁵. Jej celem jest zabezpieczenie istotnych cech dokumentów cyfrowych, w tym autentyczności, integralności i poufności, a także zachowanie informacji kontekstowych, czyli metadanych archiwizowanych dokumentów. Koncentruje się przede wszystkim na utrzymaniu dostępności, kompletności oraz wiarygodności tych zasobów w możliwie długim czasie. Archiwizacja cyfrowa przyczynia się do pełniejszego zaspokajania potrzeb użytkowników w zakresie identyfikacji, wyszukania, odczytu i interpretacji interesujących ich zasobów zapisanych w formie cyfrowej. Musi też spełnić wymagania deponentów, którym zależy na długoterminowej użyteczności przekazanych w depozyt dokumentów⁶.

Model OAIS powstał wprawdzie z inicjatywy środowisk zajmujących się badaniami przestrzeni kosmicznej, i głównie na potrzeby archiwizacji danych i informacji pochodzących z ich przedsięwzięć badawczych, jednak z czasem został uznany za uniwersalny model organizowania i funkcjonowania archiwów cyfro-

³ Consultative Committee for Space Data Systems, *Recommendation for Space Data System Practices. Reference Model for an Open Archival Information System (OAIS). Recommended practice CCSDS 650.0-M-2*, 2012, https://digital.library.unt.edu/ark:/67531/metadc123535/m2/1/high_res_d/650x0m2.pdf [dostęp: 30.04.2026].

⁴ Consultative Committee for Space Data Systems, *Recommendation for Space Data System Practices. Reference Model for an Open Archival Information System (OAIS). Recommended practice CCSDS 650.0-M-3*, 2024, <https://ccsds.org/Pubs/650x0m3.pdf> [dostęp: 30.04.2026]; ISO 14721:2025 *Space Data System Practices – Reference model for an open archival information system (OAIS)*.

⁵ A. Januszko-Szakiel, *Archiwistyka cyfrowa...*, s. 10–11.

⁶ Ibidem.

wych, stosowany do gromadzenia, przechowywania oraz udostępniania różnych typów dokumentów cyfrowych. Znalazł zastosowanie w wielu światowych bibliotekach, archiwach i muzeach, także repozytoriach danych badawczych, w których realizowane są projekty długoterminowej archiwizacji zbiorów cyfrowych⁷. Cechą charakterystyczną modelu jest jego niezależność od konkretnych implementacji technicznych, co pozwala na porównywanie różnych architektur systemowych przy użyciu wspólnego katalogu pojęciowego. Przez dostarczanie zunifikowanego i powszechnie stosowanego nazewnictwa, OAIS ułatwia międzynarodową dyskusję, wymianę poglądów oraz doświadczeń w środowiskach zainteresowanych problematyką długoterminowej archiwizacji zasobów cyfrowych⁸.

Archiwum cyfrowe OAIS to nie tylko system informatyczny, ale organizacja składająca się z osób i narzędzi ich pracy, działająca według określonych procesów i polityk, która przyjmuje odpowiedzialność za długoterminową ochronę zbiorów. Wszystkie działania archiwum koncentrują się wokół zabezpieczenia i udostępniania Obiektu Informacyjnego (*Information Object*) Wyznaczonej Grupie Użytkowników (*Designated Community*)⁹. Wyraz „open” w nazwie modelu wskazuje na otwartość inicjatywy, to znaczy, że rekomendacje OAIS są opracowywane w otwartych strukturach, a nie że dostęp do archiwum jest nieograniczony. Długoterminowość natomiast należy rozumieć jako przechowywanie obiektów cyfrowych w horyzoncie czasowym na tyle długim, by mogły przetrwać zmiany technologiczne oraz zmieniające się preferencje i zasoby wiedzy użytkowników¹⁰.

Model OAIS 2024 utrzymuje klasyczną strukturę sześciu jednostek funkcjonalnych (*Ingest, Archival Storage, Data Management, Administration, Preservation Planning, Access*) (rys.1), skoncentrowanych na „obsłudze” Obiektu Informacyjnego.

Pierwsza jednostka funkcjonalna Wprowadzanie (*Ingest*) odpowiada za przyjmowanie obiektów cyfrowych od producentów (dostawców, wydawców) w formie Zgłoszeniowych Pakietów Informacyjnych (*Submission Information Package, SIP*) i ich przekształcanie w Pakiety Archiwizacyjne (*Archival Information Package, AIP*). Tradycyjne podejście wymagało, aby każdy pakiet trafiający do archiwum był w momencie wpływu kompletny pod względem metadanych, co często opóźniało proces zabezpieczania bitów i narażało dane na utratę. W wersji OAIS 2024

⁷ Ibidem, s. 40.

⁸ Ibidem, s. 46.

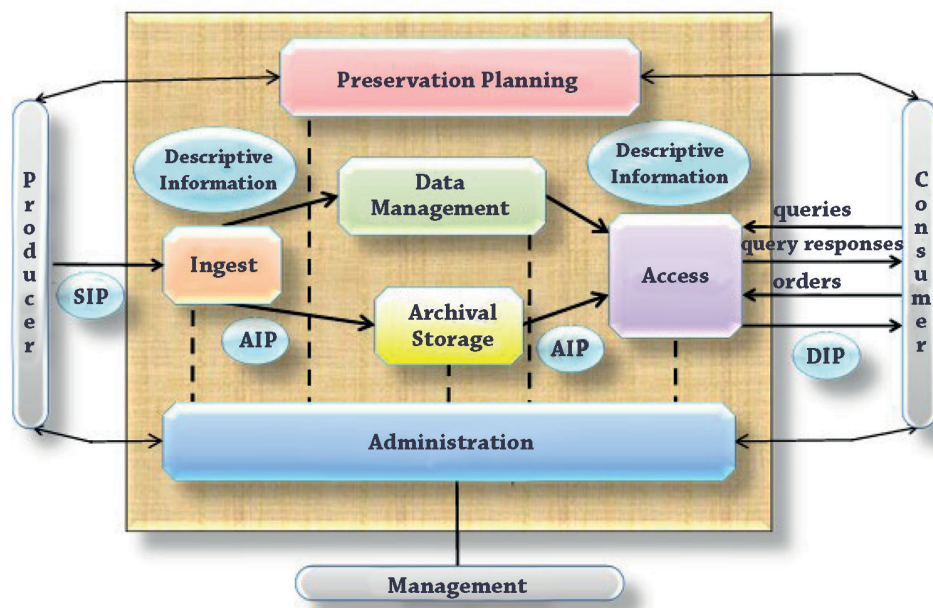
⁹ Consultative Committee for Space Data Systems, *Recommendation for Space Data System Practices...*, 2024.

¹⁰ Ibidem; A. Januszko-Szakiel, *Archiwistyka cyfrowa...*, s. 19–20.

jednostka ta zyskała większą elastyczność sprzyjającą podejściu „ingest first, describe later”¹¹ (najpierw przyjmij, później opisz), co pozwala na natychmiastowe zabezpieczenie Obiektu Informacyjnego przed utratą nośnika, nawet jeśli pełna dokumentacja (kompletne metadane) nie jest jeszcze gotowa.

Pakiet Informacyjny może składać się z jednego lub więcej opcjonalnych Obiektów Informacyjnych. System może formalnie utworzyć i przyjąć pakiet, który zawiera same bity danych, a metadane kontekstowe, proveniencyjne czy techniczne mogą być dodawane iteracyjnie w późniejszym czasie. OAIS 2024 wspiera proces tzw. dynamicznego wzbogacania metadanych. Autorzy zmiany uznają tym samym, że ochrona to proces ciągły.

Rysunek. 1. Jednostki funkcjonalne modelu OAIS



Źródło: Consultative Committee for Space Data Systems, *Recommendation for Space Data System Practices. Reference Model for an Open Archival Information System (OAIS). Recommended practice CCSDS 650.0-M-3*, 2024, <https://ccsds.org/Pubs/650x0m3.pdf>, s. 4-1 [dostęp: 30.04.2026].

¹¹ J. O'Sullivan, *What you need to know about the recent updates in OAIS v3*, Preservica (blog), 3.04.2025, <https://preservica.com/resources/blogs-and-news/what-you-need-to-know-about-the-most-recent-oais-revision> [dostęp: 30.04.2026].

Jednostka druga, Przechowywanie Archiwalne (*Archival Storage*), odpowiada za fizyczne bezpieczeństwo bitów stanowiących Obiekt Danych. Zarządza replikacją, sprawdzaniem sum kontrolnych oraz migracją do nowych formatów i nośników. Kolejna, Zarządzanie Danymi (*Data Management*), zapewnia usługi i funkcje służące do zasiedlania (doładowywania/wypełniania), utrzymywania oraz udostępniania: a) Informacji Opisowych (*Descriptive Information*), które identyfikują i dokumentują zasoby archiwum, co umożliwia użytkownikom wyszukanie i zamawianie tych zasobów; b) Danych Administracyjnych (*Administrative Data*), stosowanych w procesach zarządzania archiwum. Funkcje Zarządzania Danymi obejmują zatem administrowanie bazami danych archiwum, wykonywanie ich aktualizacji, realizację zapytań, generowanie odpowiedzi na te zapytania oraz sporządzanie raportów na podstawie uzyskanych odpowiedzi.

Czwarta jednostka funkcjonalna OAIS, Planowanie Ochrony (*Preservation Planning*), monitoruje otoczenie archiwum. Dzięki wzmocnieniu, poprzez formalne dodanie do niej funkcji Monitoring Ochrony (*Preservation Watch*), proaktywnie wykrywa zagrożenia dla Obiektu Informacyjnego (np. przestarzałość formatu) i opracowuje strategie jego aktualizacji (migracji), aby pozostał zrozumiały dla przyszłych użytkowników. Następna, Administracja (*Administration*), nadzoruje ogólne działanie systemu, zarządza politykami i negocjuje umowy dotyczące przyjmowania nowych Obiektów Informacyjnych.

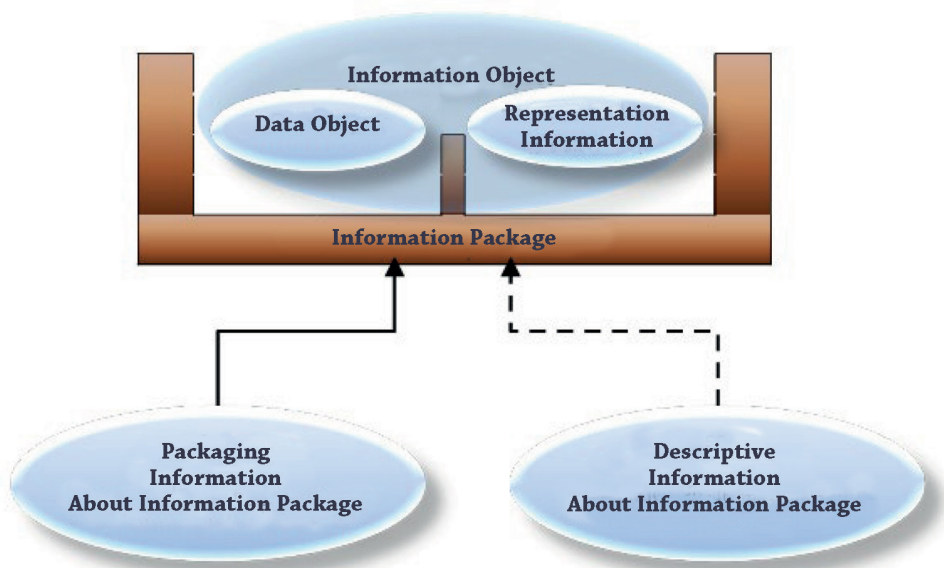
Ostatnia jednostka funkcjonalna w OAIS to Dostęp (*Access*). Umożliwia ona użytkownikom odnalezienie i pobranie informacji. Przetwarza też Obiekt Informacyjny (*Information Object*) w Pakiet Udostępniany (*Dissemination Information Package*, DIP) w formie dostosowanej do Bazy Wiedzy (*Knowledge Base*), a więc możliwości technicznych i kompetencji użytkowników¹². Wymienione jednostki funkcjonalne OAIS współpracują ze sobą, aby zarządzać cyklem życia Obiektu Informacyjnego, utrzymując jego długoterminową dostępność i użyteczność oraz chroniąc przed degradacją.

Obiekt Informacyjny (zgodnie z rys. 2) stanowi połączenie dwóch elementów: 1) Obiektu Danych (*Data Object*), będącego albo sekwencją bitów (w przypadku obiektów cyfrowych), albo fizycznym artefaktem, który archiwum zamierza chronić, oraz 2) Informacji o Reprezentacji (*Representation Information*). Ten drugi element należy postrzegać jako klucz interpretacyjny, techniczną metodę przed-

¹² Consultative Committee for Space Data Systems, *Recommendation for Space Data System Practices...*, 2024, s. 4-1-4-19 [dostęp: 30.04.2026].

stawienia danych i nadawania im znaczenia. Umożliwia on pełną interpretację danych tworzących Obiekt Danych, ich przekształcenie w zrozumiałe informacje. Informacja o Reprezentacji towarzysząca Obiektowi Danych nie tylko opisuje go z zewnątrz (jak typowe metadane), ale przede wszystkim stanowi instrukcję mapowania bitów na pojęcia, powszechnie rozpoznawalne typy danych, takie jak znak, liczba, tym samym umożliwia ich interpretację zgodnie z określonymi Celami Ochrony (*Preservation Objectives*)¹³.

Rysunek. 2. Pakiet informacyjny jako „kontener” obiektu informacyjnego (danych i metadanych)



Źródło: Consultative Committee for Space Data Systems, *Recommendation for Space Data System Practices. Reference Model for an Open Archival Information System (OAIS). Recommended practice CCSDS 650.0-M-3*, 2024, <https://ccsds.org/Pubs/650x0m3.pdf>, s. 2-6 [dostęp: 30.04.2026].

W modelu OAIS Informacja o Reprezentacji obejmuje trzy typy. Są to:

1) Informacja o Reprezentacji Struktury (*Structure Representation Information*) dotycząca układu i organizacji elementów Obiektu Danych. Jej zadaniem jest konwersja ciągów bitów na powszechnie rozpoznawane typy komputerowe, takie

¹³ Ibidem, s. 4-23-4-24.

jak znaki, liczby czy piksele, oraz ich agregacje (np. tablice). W praktyce jest to określenie formatu obiektu cyfrowego (formatu pliku);

2) Informacja o Reprezentacji Semantyki (*Semantic Representation Information*) uszczegóławiająca znaczenie Obiektu Danych oraz jego elementów, wykraczająca poza sam opis strukturalny. Ten typ Informacji o Reprezentacji pozwala przypisać zdekodowanym bitom konkretny sens/kontekst, np. informację, że dana liczba to pomiar temperatury w stopniach Celsjusza. W przypadku tekstu obejmuje ona wiedzę o języku naturalnym, w którym został wyrażony, wskazując adekwatne słowniki i gramatykę;

3) Informacja o Reprezentacji Innych Komponentów Obiektu Danych (*Other Representation Information*) obejmująca pozostałe elementy Obiektu Danych, trudne do sklasyfikowania jako struktura lub semantyka, np. takie jak oprogramowanie potrzebne do przetwarzania zawartości bazy danych, algorytmy, szyfrowanie, instrukcje. Według OAIS Informacja o Reprezentacji Innych Komponentów Obiektu Danych mogłaby przykładowo dotyczyć powiązań Informacji o Reprezentacji Struktury i Informacji o Reprezentacji Semantyki¹⁴.

Konkludując, bez Informacji o Reprezentacji Obiekt Danych – zwłaszcza cyfrowy – pozostaje jedynie nieczytelnym ciągiem bitów¹⁵. Relacja między tymi dwoma elementami jest dynamiczna. Archiwum musi monitorować Bazę Wiedzy Wyznaczonej Grupy Użytkowników i w razie potrzeby aktualizować Informację o Reprezentacji, aby zapewnić długoterminową zrozumiałość i użyteczność zasobów¹⁶.

Kluczowym wymogiem w modelu OAIS jest to, aby Obiekt Informacyjny był „niezależnie zrozumiały” (*independently understandable*) dla Wyznaczonej Grupy Użytkowników. OAIS definiuje „niezależną zrozumiałość” jako cechę informacji, która jest wystarczająco kompletna, aby mogła zostać zrozumiana przez społeczność użytkowników bez konieczności odwoływania się do specjalnych zasobów, ekspertów czy źródeł, które nie są powszechnie dostępne tej społeczności. Oznacza to, że Informacje o Reprezentacji muszą być na tyle zasobne, aby użytkownicy mogli odczytać i zrozumieć archiwizowany obiekt bez pomocy twórcy lub ekspertów zewnętrznych. Autorzy wersji OAIS z 2024 r. kładą nacisk na Cele Ochrony, które służą jako mierzalne kryteria sprawdzające czy Obiekt Informacyjny

¹⁴ Ibidem, s. 4-25.

¹⁵ Ibidem, s. 4-24; A. Januszko-Szakiel, *Archiwistyka cyfrowa...*, s. 41.

¹⁶ Consultative Committee for Space Data Systems, *Recommendation for Space Data System Practices...*, 2024, s. 4-25–4-26.

rzeczywiście pozostaje zrozumiały dla społeczności użytkowników o określonym poziomie wiedzy¹⁷.

Oprócz Informacji o Reprezentacji, która umożliwia odczyt i interpretację treści archiwizowanego obiektu, ważnym komponentem weryfikacji autentyczności, wiarygodności i użyteczności archiwizowanego obiektu jest pakiet Opisu Przechowywania (*Preservation Description Information*, PDI). Ujmuje on pięć elementów, tj. 1) Dane Identyfikujące (*Reference*) czyli unikalne identyfikatory obiektu (np. DOI, sygnatury), które pozwalają na jego jednoznaczne wskazanie wewnątrz i na zewnątrz archiwum, co zapewnia stabilność odniesień identyfikacyjnych; 2) Pochodzenie (*Provenance*), które dokumentuje historię obiektu, w tym informacje o jego twórcy, procesie przekazania do archiwum oraz wszelkich zmianach (np. migracjach formatów), jakim został poddany, i służy zachowaniu historii i autentyczności obiektu; 3) Kontekst (*Context*), który opisuje relacje obiektu archiwizowanego z innymi zasobami (np. innymi częściami serii, powiązanymi załącznikami) oraz powody jego powstania, tym samym chroni obiekt przed utratą znaczenia; 4) Integralność (*Fixity*), która zawiera mechanizmy (np. sumy kontrolne, podpisy cyfrowe) pozwalające udowodnić, że Obiekt Danych nie został w nieuprawniony sposób zmieniony, wspierające wykrywanie zmian; 5) Prawa Dostępu (*Access Rights*), które określają warunki prawne, licencje oraz ograniczenia techniczne dotyczące udostępniania obiektu użytkownikom i umożliwiają kontrolę zgodności dostępu¹⁸. W kontekście zarządzania ryzykiem Opis Przechowywania można traktować jako zestaw mechanizmów redukujących ryzyko utraty wiarygodności i użyteczności pojedynczego zasobu.

Porównanie wersji modelu OAIS z 2012 i 2024 r. wskazuje na zmianę myślenia o ochronie cyfrowej. Archiwum powinno koncentrować się już nie tyle na precyzyjnym definiowaniu, czym jest chroniony obiekt i jego metadane, co przede wszystkim na tym, jak system powinien operować w nieustannie zmieniającej się rzeczywistości. Kluczowe zmiany to przejście:

1) od statyki do dynamiki, tj. od sztywnych pakietów danych do elastycznych struktur, czego ewidentnym przykładem jest umożliwienie priorytetyzacji ochrony bitów i odroczenia etapu uzupełnienia informacji kontekstowych („ingest first, describe later”)¹⁹. Strategia ta umożliwia archiwum natychmiastowe zabezpieczenie zagrożonych danych (np. zagrożenie zidentyfikowane jeszcze u pro-

¹⁷ Ibidem, s. 2-3-2-4.

¹⁸ Ibidem, s. 2-6-2-7, 4-35-4-37.

¹⁹ J. O’Sullivan, *What you need to know...*

ducenta/wytwórcy obiektu cyfrowego), przy jednoczesnym odłożeniu w czasie szczegółowego opisywania tego obiektu (wzbogacenie o metadane i inne zasoby tzw. informacji reprezentującej). Takie podejście bezpośrednio mityguje ryzyko fizycznej degradacji nośnika poprzez szybkie zabezpieczenie bitów, odkładając szczegółowe opisywanie i tworzenie pełnej struktury pakietu AIP na później. Jest to odpowiedź na wyzwania skali i tempa współczesnego przyrostu danych;

2) od reaktywności do proaktywności, tj. wprowadzenie funkcji Monitoring Ochrony, która czyni z monitorowania otoczenia archiwum centralny punkt strategii ochrony, redukując ryzyko utraty dostępu do zasobów archiwalnych z powodu nagłej zmiany w dowolnym obszarze cyfrowego środowiska archiwum;

3) od subiektywności do obiektywnej mierzalności, tj. uczynienia z funkcji Cele Ochrony narzędzia obiektywnego pomiaru efektów zabiegów archiwalnych, co wzmacnia zaufanie do archiwów.

Dla profesjonalistów zajmujących się ochroną zasobów cyfrowych w długim czasie model OAIS z 2024 r. nie jest jedynie aktualizacją terminologiczną, lecz wezwaniem i zestawem rekomendacji do budowania systemów archiwizacji bardziej odpornych, lepiej zintegrowanych z otoczeniem i przede wszystkim zdolnych do ciągłej ewolucji wraz ze swoimi użytkownikami i technologiami. Najnowszą odsłoną model ten potwierdza swoją pozycję jako niekwestionowany standard archiwizacji cyfrowej w skali globalnej. Oferuje on przy tym ramy, które są jednocześnie rygorystyczne pod względem zasad i elastyczne pod względem implementacji w nowoczesnych infrastrukturach archiwów cyfrowych.

Model OAIS jako rama dla proaktywnego zarządzania ryzykiem w archiwach cyfrowych

W ujęciu ogólnym ryzyko jest definiowane jako wpływ niepewności na cele organizacji lub działania, co w standardach zarządzania ryzykiem (np. ISO 31000) przekłada się na możliwość odchylenia od zamierzonych rezultatów wskutek działania czynników niepewnych, zarówno negatywnych, jak i pozytywnych²⁰.

²⁰ Ryzyko [w:] *Słownik Języka Polskiego PWN*, <https://sjp.pwn.pl/slowniki/ryzyko.html> [dostęp: 30.04.2026]; Ryzyko [w:] *Encyklopedia Zarządzania*, <https://mfiles.pl/pl/index.php/Ryzyko> [dostęp: 30.04.2026]; E. Młodzik, *Zakres odpowiedzialności w procesie zarządzania ryzykiem w organizacji*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Finanse, Rynki Finansowe, Ubez-

Zarządzanie ryzykiem oznacza natomiast skoordynowane działania odnoszące się do identyfikacji, analizy, oceny i monitorowania ryzyka w powiązaniu z celami organizacji²¹.

Ryzyko w archiwach cyfrowych ma charakter szczególnie złożony. Organizatorzy archiwów cyfrowych muszą liczyć się z ryzykiem technologicznym, obejmującym awarie nośników, dezaktualizację formatów, zanikanie środowisk programowych czy zależność od określonych dostawców systemów. Pojawia się także ryzyko informacyjne i epistemiczne, polegające na utracie kontekstu, autentyczności, integralności albo zrozumiałości zasobu dla przyszłych użytkowników. Kolejna kategoria to ryzyka organizacyjne i strategiczne, związane z niedoborem zasobów, niewłaściwymi politykami, brakiem odpowiedzialności lub niewystarczającym planowaniem działań ochronnych. Bardzo ważna kategoria to także ryzyko prawne i dostępowe, dotyczące ograniczeń dostępu, błędnej autoryzacji, naruszenia poufności lub nieskutecznej kontroli praw do informacji. Archiwum cyfrowe funkcjonuje zatem w przestrzeni wieloaspektowej niepewności, w której skuteczna ochrona wymaga zarówno środków technicznych, jak i świadomego zarządzania²².

Analizowany model od początku zawierał „ukrytą” logikę „risk-based”. Archiwum zgodne z OAIS zawsze musiało przewidywać ewentualną utratę zrozumiałości, integralności, autentyczności i dostępności informacji, a następnie organizować swoje działania tak, aby te zagrożenia redukować. Ryzyko dotyczy zarówno obiektu cyfrowego, jak i całej struktury instytucjonalnej odpowiedzialnej za jego ochronę. W wersji OAIS z 2024 r. logika ta jest bardziej eksponowana. Autorzy

pieczenia” 2014, nr 65, s. 689–698, http://wneiz.pl/nauka_wneiz/frfu/65-2014/FRFU-65-689.pdf [dostęp: 30.04.2026]; M. Młynczak, T. Nowakowski, D. Vališ, *Jak zarządzać ryzykiem? Podejście normatywne*, „Problemy eksploatacji” 2011, nr 1, s. 137–147, <https://share.google/fQ-3PE6dUKQ0iqq4sf> [dostęp: 30.04.2026].

²¹ ISO 31000:2018 *Risk management – Guidelines*; ISOQUAR, ISO 31000 Zarządzanie ryzykiem – Wytyczne, <https://www.isoqar.pl/pl/aktualnosci/zloty-standard/iso-31000-zarzadzanie-ryzykiem-wytyczne> [dostęp: 30.04.2026]; R.D. Frank, *Risk in trustworthy digital repository audit and certification*, „Archival Science” 2021, nr 22(1), s. 43–73, <https://doi.org/10.1007/s10502-021-09366-z> [dostęp: 30.04.2026].

²² R.D. Frank, *Risk in trustworthy...*, s. 43–73; A. Januszko-Szakiel, L. Szafrński, *Długoterminowa archiwizacja cyfrowych danych badawczych: zagadnienia wybrane* [w:] *Horyzonty informacji*, red. P. Korycińska, Kraków 2024, s. 23–36, <https://ruj.uj.edu.pl/entities/publication/26bbe4b4-7498-48d7-85ab-a12aff5fdd5e> [dostęp: 30.04.2026]; A. Januszko-Szakiel, P. Korycińska, *Zarządzanie ryzykiem w cyfrowych repozytoriach danych badawczych* [w:] *Biblioteka 5.0. Transformacja procesów i usług w środowisku inteligentnych technologii*, red. M. Kowalska-Chrzanowska, Warszawa 2026, s. 123–148.

modelu dodali funkcje pozwalające lepiej formułować cele ochrony i monitorować otoczenie, w którym archiwum funkcjonuje. Te dodatkowe funkcje można interpretować jako zmianę w podejściu do zarządzania ryzykiem z reaktywnego na proaktywne, czyli takie, które koncentruje się nie na reagowaniu na zaistniały już problem, lecz na świadomym wcześniejszym rozpoznaniu, oszacowaniu i ograniczeniu ewentualnego problemu. W logice proaktywnej kluczowe znaczenie mają: monitorowanie otoczenia, bieżąca identyfikacja słabych sygnałów zagrożenia, analiza scenariuszy, definiowanie akceptowalnego poziomu ryzyka oraz wdrażanie środków zapobiegawczych zanim dojdzie do realnej straty²³. W odniesieniu do archiwów cyfrowych oznacza to przejście od modelu, w którym działania konserwatorskie uruchamia się dopiero po wystąpieniu awarii i utraci czytelności treści obiektu cyfrowego do modelu, w którym zmiany technologiczne, potrzeby użytkowników i słabości systemu są stale obserwowane i oceniane. Odzwierciedleniem takiego podejścia w OAIS z 2024 r. jest przede wszystkim jednostka funkcjonalna Planowanie Ochrony wraz z funkcją Monitoring Ochrony oraz idea Cele Ochrony²⁴.

Planowanie Ochrony to jednostka funkcjonalna odpowiedzialna za monitorowanie otoczenia systemu archiwalnego OAIS oraz dostarczanie rekomendacji i planów działania, które zapewnią, że zasoby pozostaną dostępne, zrozumiałe i użyteczne dla Wyznaczonej Grupy Użytkowników (*Designated Community*) w długim czasie. Do jej głównych zadań należy okresowe ocenianie zawartości archiwum, opracowywanie strategii migracji, rozwijanie standardów i polityk archiwalnych oraz dostarczanie raportów z analizy ryzyka, jak też projektowanie szablonów pakietów informacji (SIP i AIP) oraz opracowanie szczegółowych planów i oprogramowania prototypowego dla realizacji przyjętych celów ochrony²⁵.

W strukturze Planowanie Ochrony formalnie wydzielono funkcję Monitoring Ochrony, którą można definiować jako narzędzie ciągłego monitorowania zagrożeń lub system wczesnego ostrzegania zestawiający (konfrontujący) dane z monitoringu technologii z danymi (zmieniającymi się/aktualizowanymi na bieżąco) w Bazie Wiedzy o Wyznaczonej Grupie Użytkowników (preferencje, dostępne narzędzia, zasób kompetencji). Dzięki temu archiwum przekształca się z pasyw-

²³ Consultative Committee for Space Data Systems, *Recommendation for Space Data System Practices...*, 2024.

²⁴ Ibidem, s. 1-14; 4-2-4-3; 4-15-4-17.

²⁵ Ibidem, s. 4-15-4-21.

nego magazynu w dynamiczny system, który podejmuje terminowe interwencje (*timely interventions*)²⁶, zanim ryzyko (np. obsolescencji formatu) uniemożliwi odczyt danych i przerodzi się w nieodwracalną utratę informacji. Monitoring Ochrony formalizuje zatem obowiązek ciągłego monitorowania wewnętrznego i zewnętrznego środowiska archiwum i gromadzenia informacji dotyczących trzech krytycznych obszarów, tj. 1) postępu technologii – śledzenie cyklu życia formatów plików, systemów operacyjnych i sprzętu, w celu identyfikacji momentów, w których np. format PDF/A-1b zaczyna tracić wsparcie ze strony kluczowych dostawców oprogramowania, co stwarza ryzyko utraty dostępu do treści; 2) zmieniających się potrzeb i kompetencji Wyznaczonej Grupy Użytkowników – śledzenie Bazy Wiedzy użytkowników w celu identyfikacji zmian kompetencji technicznych grupy odbiorców (np. młodzi historycy nie potrafią już obsłużyć relacyjnych baz danych) i sygnalizowania potrzeby dodania nowych Informacji o Reprezentacji obiektu archiwizowanego; 3) integralności zasobów (kontrolowanie kondycji nośników obiektów cyfrowych) oraz skuteczności procedur administracyjnych wewnątrz archiwum. Dzięki Monitoringowi Ochrony model OAIS zmienia paradygmat ochrony z działań jednorazowych lub okresowych na proces ciągły, zapobiegając sytuacjom, w których obiekty cyfrowe stają się nieczytelne z powodu zbagatelizowania faktu zmian technologicznych lub za późnej reakcji wobec faktu przestarzałości technologii.

Należy podkreślić, że w wersji OAIS z 2012 r. monitorowanie otoczenia technologicznego było wpisane w ogólne ramy planowania działań archiwizacyjnych. Autorzy nowej wersji sformalizowali ten proces, nadając mu status odrębnej, krytycznej funkcji systemowej. Monitoring Ochrony jest zatem aktywnym generatorem wyzwalaczy (*triggers*), które inicjują działania w pozostałych częściach Planowania Ochrony, takich jak opracowywanie konkretnych planów ochrony czy aktualizowanie pakietów informacyjnych w magazynie archiwalnym. Taka integracja pozwala na budowanie systemów zdolnych do automatycznego reagowania na zmiany, co jest kluczowe dla skalowalności operacji w nowoczesnych i rozwijających się organizacjach²⁷. Planowanie Ochrony pozwala analizować scenariusze

²⁶ J. O'Sullivan. *What you need to know...*

²⁷ Consultative Committee for Space Data Systems, *Recommendation for Space Data System Practices...*, 2024, s. 4-15-4-17; J. O'Sullivan, *What you need to know...*; A. Potter, *The Standard That Outgrew Space. OAIS v3, PREMIS, and the New Metadata Ecosystem*, Substack (blog), 17.04.2024, <https://metaarchivist.substack.com/p/the-standard-that-outgrew-space> [dostęp: 30.04.2026].

zmian, oceniać strategie ochrony i rekomendować działania, natomiast Monitoring Ochrony dostarcza informacje o zmianach, które mogą zagrozić realizacji celów archiwum, co daje impuls do wprowadzenia modyfikacji²⁸. Razem tworzą mechanizm cykliczny: monitorowanie, analiza, decyzja, wdrożenie, ponowny monitoring. Jest to odpowiednik procesu proaktywnego zarządzania ryzykiem w obrębie modelu OAIS.

Cele Ochrony z kolei można interpretować jako ideę i zarazem narzędzie oceny wykonalności przyjętych przez archiwum celów, także pomiaru poziomu skuteczności ochrony. W świetle OAIS z 2024 r. cele archiwizacji obiektów cyfrowych przestają mieć charakter subiektywny, tym samym utrudniający jednoznaczną ocenę, czy i w jakim zakresie archiwum wywiązuje się ze swoich zadań, z przyjętych zobowiązań. Zamiast ogólnej deklaracji o „zachowaniu dokumentu”, archiwum definiuje precyzyjne parametry ochrony, określa cele specyficzne, osiągalne i mierzalne (dokładne cechy obiektu archiwizowanego, które mają zostać zachowane, np. wierność kolorystyczna obrazu, funkcjonalność skryptów w bazach danych). Wprowadzenie rygoru w Celach Ochrony pozwala na przejście od intuicyjnego zarządzania ryzykiem do „inżynierii ochrony danych”, gdzie każde działanie konserwatorskie jest testowane pod kątem zgodności z przyjętymi celami. Jest to także ważna zmiana pozwalająca na obiektywny audyt skuteczności ochrony, co jest kluczowe dla uzyskania certyfikacji zgodnie z nowym standardem ISO 16363:2025. Ponadto Cele Ochrony umożliwiają testowanie poziomu cechy „niezależnej zrozumiałości” informacji²⁹. Przykładowe testy obejmują sprawdzenie czy teksty lub obrazy są renderowane w sposób wystarczająco zbliżony do oryginału lub czy zestaw danych może być poprawnie przetworzony przez narzędzia analityczne w celu uzyskania oczekiwanych wyników. Inna ważna funkcja Celów Ochrony uwidacznia się na etapie wprowadzania danych do archiwum. Umożliwia ona archiwum podejmowanie świadomych decyzji dotyczących akceptowalnego poziomu zmian lub utraty informacji podczas zabiegów konserwatorskich, np. zmiany formatu. Archiwum cyfrowe OAIS zakłada potrzebę analizy ryzyka i świadomego przyjmowania kompromisów dotyczących rozbieżności (ilościowych, jakościowych) pomiędzy przyjętymi Celami Ochrony a efektami zabiegów konserwatorskich. W OAIS za ocenę ryzyka jest odpowiedzialna funkcja Opracowywanie Strategii i Standardów Ochrony (*Develop*

²⁸ Consultative Committee for Space Data Systems, *Recommendation for Space Data System Practices...*, 2024, s. 4-1-4-15.

²⁹ Ibidem, s. 1-12, 2-8, 3-4.

Preservation Strategies and Standards)³⁰. Podstawowym założeniem tej funkcji jest właśnie umożliwienie archiwum dokonywania świadomych kompromisów podczas ustanawiania standardów, określania polityk i zarządzania infrastrukturą systemową³¹. Takie podejście jest w OAIS podstawą do postrzegania zarządzania ryzykiem jako metodologii zapewniającej równowagę między potrzebami a możliwymi do zastosowania środkami, także między doraźnymi działaniami a długoterminowymi celami archiwizacji³².

Podsumowanie

Analiza modelu OAIS z 2024 r. jest podstawą do wysnucia wniosku, że archiwa cyfrowe przestają funkcjonować jako systemy „bezpiecznego składowania” danych i wchodzi w etap „aktywnego zarządzania zrozumiałością” obiektów archiwalnych. Najważniejszą zmianą jest przejście od modelu reaktywnego do proaktywnego, w którym bieżące monitorowanie otoczenia archiwum za pomocą funkcji Monitoring Ochrony staje się centralnym punktem strategii archiwizacji. Archiwum cyfrowe przekształca się z pasywnego magazynu w dynamiczny system podejmujący terminowe interwencje na rzecz zachowania użyteczności obiektów cyfrowych w długim czasie. W kontekście zarządzania ryzykiem istotne zmiany wniesione do długoterminowej archiwizacji zasobów cyfrowych przez OAIS z 2024 r. to: 1) mierzalność – Cele Ochrony dostarczają obiektywnych narzędzi weryfikacji skuteczności działań konserwatorskich; 2) elastyczność – możliwe stało się natychmiastowe przyjęcie do systemu archiwalnego i zabezpieczenie zagrożonych danych, bez konieczności kompletowania pełnego obiektu informacyjnego na wejściu; 3) rozwój – Informacja o Reprezentacji musi ewoluować wraz ze zmianami bazy wiedzy społeczności użytkowników docelowych, co chroni zasoby przed przeistoczeniem się w nieczytelny ciąg bitów.

³⁰ Ibidem, s. 4-16.

³¹ Ibidem, s. 2-8; 4-13 – 4-17.

³² Ibidem, s. 4-16.

Bibliografia

- Consultative Committee for Space Data Systems, *Historical Document. Recommendation for Space Data System Standards. Reference Model for an Open Archival Information System (OAIS)* CCSDS 650.0-B-1, 2002, <https://ccsds.org/Pubs/650x0b1s.pdf> [dostęp: 30.04.2026].
- Consultative Committee for Space Data Systems, *Recommendation for Space Data System Practices. Reference Model for an Open Archival Information System (OAIS). Recommended practice* CCSDS 650.0-M-2, 2012, https://digital.library.unt.edu/ark:/67531/metadc123535/m2/1/high_res_d/650x0m2.pdf [dostęp: 30.04.2026].
- Consultative Committee for Space Data Systems, *Recommendation for Space Data System Practices. Reference Model for an Open Archival Information System (OAIS). Recommended practice* CCSDS 650.0-M-3, 2024, <https://ccsds.org/Pubs/650x0m3.pdf> [dostęp: 30.04.2026].
- ISO 14721:2012 *Space data and information transfer systems – Open archival information system (OAIS) – Reference model*.
- ISO 14721:2025 *Space Data System Practices – Reference model for an open archival information system (OAIS)*.
- ISO 31000:2018 *Risk management – Guidelines*.
- ISOQUAR, ISO 31000 Zarządzanie ryzykiem – Wytyczne, <https://www.isoqar.pl/pl/aktualnosci/zloty-standard/iso-31000-zarzadzanie-ryzykiem-wytyczne> [dostęp: 30.04.2026].
- Frank R.D., *Risk in trustworthy digital repository audit and certification*, „Archival Science” 2021, nr 22(1), s. 43–73, <https://doi.org/10.1007/s10502-021-09366-z> [dostęp: 30.04.2026].
- Januszko-Szakiel A., *Archiwistyka cyfrowa. Długoterminowa ochrona dziedzictwa nauki i kultury*, Warszawa 2017.
- Januszko-Szakiel A., *Open Archival Information System – standard w zakresie archiwizacji publikacji elektronicznych*, „Przegląd Biblioteczny” 2005, r. 73, z. 3, s. 341–358.
- Januszko-Szakiel A., Korycińska P., *Zarządzanie ryzykiem w cyfrowych repozytoriach danych badawczych* [w:] *Biblioteka 5.0. Transformacja procesów i usług w środowisku inteligentnych technologii*, red. M. Kowalska-Chrzanowska, Warszawa 2026, s. 123–148.
- Januszko-Szakiel A., Szafrąński L., *Długoterminowa archiwizacja cyfrowych danych badawczych: zagadnienia wybrane* [w:] *Horyzonty informacji*, red. P. Korycińska, Kraków 2024, s. 23–36, <https://ruj.uj.edu.pl/entities/publication/26bbe4b4-7498-48d7-85ab-a12aff5fdd5e> [dostęp: 30.04.2026].
- Młodzik E., *Zakres odpowiedzialności w procesie zarządzania ryzykiem w organizacji*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Finanse, Rynki Finansowe, Ubezpieczenia” 2014, nr 65, s. 689–698, http://wneiz.pl/nauka_wneiz/frfu/65-2014/FRFU-65-689.pdf [dostęp: 30.04.2026].

- Młyńczak M., Nowakowski T., Vališ D., *Jak zarządzać ryzykiem? Podejście normatywne*. „Problemy eksploatacji” 2011, nr 1, s. 137–147, <https://share.google/fQ3PE6dUKQ0iqq4sf> [dostęp: 30.04.2026].
- O’Sullivan J., *What you need to know about the recent updates in OAIS v3*, Preservica (blog), 3.04.2025, <https://preservica.com/resources/blogs-and-news/what-you-need-to-know-about-the-most-recent-oais-revision> [dostęp: 30.04.2026].
- Potter A., *The Standard That Outgrew Space. OAIS v3, PREMIS, and the New Metadata Ecosystem*, Substack (blog), 17.04.2026, <https://metaarchivist.substack.com/p/the-standard-that-outgrew-space> [dostęp: 30.04.2026].
- Ryzyko [w:] *Słownik Języka Polskiego PWN*, <https://sjp.pwn.pl/slowniki/ryzyko.html> [dostęp: 30.04.2026].
- Ryzyko [w:] *Encyklopedia Zarządzania*, <https://mfiles.pl/pl/index.php/Ryzyko> [dostęp: 30.04.2026].