PRZEGLĄD BIBLIOTECZNY 2009 z. 3
PL ISSN 0033-202X

ANETA JANUSZKO-SZAKIEL
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
e-mail: ajanuszko-szakiel@afm.edu.pl

WIARYGODNOŚĆ ARCHIWÓW CYFROWYCH

Aneta Januszko-Szakiel jest absolwentką Instytutu Bibliotekoznawstwa i Informacji Naukowej UJ. Wykłada w Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego. Jej zainteresowania naukowe skupiają się wokół organizacji i funkcjonowania cyfrowych repozytoriów, w szczególności dotyczą długoterminowej archiwizacji zasobów cyfrowych. Ważniejsze publikacje: Open Archival Information System – standard w zakresie archiwizacji publikacji elektronicznych (*Przegląd Biblioteczny,* 2005), Dysertacje via Internet (*Przegląd Biblioteczny,* 2006).

SŁOWA KLUCZOWE: Archiwa cyfrowe. Repozytoria cyfrowe. Wiarygodne archiwa cyfrowe. Certyfikacja archiwów cyfrowych. Audyt archiwów cyfrowych.

ABSTRAKT: W artykule dokonano przeglądu definicji pojęcia *archiwum cyfrowe* oraz przedstawiono typologię funkcjonujących archiwów cyfrowych. Zwrócono uwagę na odmienność archiwów instytucji pamięci i archiwów sektora biznesu bądź administracji. Szczegółowo omówiono problematykę oceny wiarygodności archiwów cyfrowych i wymieniono cechy identyfikacyjne, zapewniające im status serwisów wiarygodnych. Artykuł ma charakter dokumentacji dotychczasowych ustaleń w zakresie procesów organizacji, funkcjonowania, audytu i certyfikacji wiarygodnych archiwów cyfrowych. Ustalenia te są efektem międzynarodowej współpracy takich organizacji i instytucji, jak: DCC – Digital Curation Centre, OCLC – Online Computer Library Center, RLG – Research Library Group, NARA – National Archives and Records Administration, NESTOR – Network of Expertise in Long-term Storage of Digital Resources oraz CRL – U.S. Center for Research Libraries. Są one dostępne w dwóch wersjach językowych; angielskiej: *Trustworthy Repositories Audit & Certification. Criteria and Checklist* (TRAC), oraz niemieckiej: *Kriterienkatalog vertrauenswürdige digitale Langzeitarchive.*

WSTĘP

W obliczu popularności tworzenia rozmaitych typów archiwów cyfrowych, określanych także jako repozytoria cyfrowe, warto ustalić, co te pojęcia oznaczają oraz zastanowić się nad takimi założeniami ich organizacji i funkcjonowania, które zapewniłyby deponentów i użytkowników o ich wiarygodności i niezawodności. Wieloletnie dyskusje i prace szeregu instytucji i organizacji z różnych krajów świata przyniosły efekty, na których podstawie możliwe jest rozeznanie, jakie rozwiązania organizacyjne, techniczne, prawne oraz ekonomiczne należy przyjąć w procesach planowania, organizacji i funkcjonowania archiwów cyfrowych, aby zapewnić ciągłość bezpieczeństwa i dostępności deponowanych w nich materiałów. Z uwagi na to, że obok przechowywanego materiału cyfrowego, istotnym ogniwem archiwów cyfrowych

są użytkownicy wraz z ich oczekiwaniami, trwają intensywne prace nad metodyką oceniania funkcjonujących systemów archiwalnych, właśnie pod względem stopnia spełniania przez nie oczekiwań użytkowników i deponentów.

W artykule przedstawiono obecny stan wiedzy z zakresu organizacji i funkcjonowania wiarygodnych, długoterminowych archiwów cyfrowych. Wiedza ta wynika z międzynarodowej współpracy licznych organizacji i instytucji bibliotecznych, archiwalnych, muzealnych, etc., wśród których najważniejsze to:

– Research Library Group (RLG) to amerykańska organizacja bibliotek naukowych, powołana w 1974 r. jako wspólne przedsięwzięcie biblioteki publicznej Nowego Yorku oraz uniwersytetów Columbii, Harvardu oraz Yale. Głównym celem przedsięwzięcia było prowadzenie wspólnej polityki w zakresie gromadzenia oraz udostępniania zbiorów. Od momentu fuzji RLG z OCLC w 2006 r. mówi się o programie RLG-OCLC obejmującym ponad 140 bibliotek, archiwów, muzeów oraz innych instytucji pamięci, którego celem jest tworzenie zasobów dla nauki i edukacji, a także zapewnienie ich długoterminowej i wiarygodnej archiwizacji[1]. RLG jest jedną z pierwszych organizacji na świecie zajmujących się tematyką audytu i certyfikacji repozytoriów cyfrowych. Rozpoznania grupy RLG oraz współpracujących z nią ściśle organizacji OCLC i NARA stanowią podstawę dla wszelkich późniejszych inicjatyw z tego zakresu tematycznego.

– Online Computer Library Center (OCLC) to amerykańska organizacja o charakterze badawczym i usługowym, powstała w 1967 r., pierwotnie pod nazwą Ohio College Library Center. Jej zadaniem jest przede wszystkim wspieranie procesów automatyzacji, a następnie także cyfryzacji bibliotek, obecnie w zakresie bibliotekarstwa cyfrowego w szczególności zajmuje się poprawą dostępu do zasobów informacyjnych oraz obniżaniem kosztów wynikających z ich użytkowania. W 2006 r. miało miejsce połączenie OCLC i RLG[2], jednak już wcześniej obie instytucje współpracowały, głównie w zakresie charakterystyki stabilnych, wiarygodnych archiwów cyfrowych, budowanych na podstawie modelu referencyjnego OAIS.

– National Archives and Records Administration (NARA) jest narodowym archiwum Stanów Zjednoczonych, które zostało założone w 1934 r. w celu ujednolicenia polityki ochrony stanowych zasobów archiwalnych. W 2003 r. NARA i RLG zainicjowały utworzenie międzynarodowej grupy roboczej do spraw certyfikacji archiwów cyfrowych[3].

– NESTOR – Network of Expertise in Long-term Storage of Digital Resources (niem. Kompetenznetzwerk Langzeitarchivierung) to niemiecka organizacja utworzona w 2003 r. przez siedem niemieckich instytucji bibliotecznych, archiwalnych oraz muzealnych w celu wymiany doświadczeń w zakresie długoterminowej archiwizacji zasobów cyfrowych. Nestor aktywnie działa w pracach międzynarodowej grupy założonej przez RLG i NARA i jest autorem niemieckojęzycznej wersji, prezentowanego w niniejszym artykule katalogu kryteriów oceny wiarygodności archiwów cyfrowych[4].

[1] Dodatkowe informacje na temat programu RLG-OCLC są dostępne w serwisie WWW pod adresem: <http://www.oclc.org/programs/default.htm> [dostęp: 12.12.2008].

[2] Szczegółowe informacje o działalności OCLC dostępne są na stronie WWW, pod adresem: <http://www.oclc.org/about/default.htm> [dostęp: 15.12.2008].

[3] Więcej informacji o założeniach grupy roboczej oraz wykaz instytucji członkowskich jest dostępny na stronie WWW: <http://worldcat.org/arcviewer/1/OCC/2007/08/08/0000070511/viewer/file2588.html> [dostęp: 15.12.2008].

[4] Działalność grupy NESTOR jest szczegółowo przedstawiona na stronie WWW pod adresem: <http://www.langzeitarchivierung.de/index.php> [dostęp: 15.12.2008].

– U.S. Center for Research Libraries (CRL) zostało założone w 1949 r. jako Midwest Inter-Library Center (MILC) przez amerykańskie uczelnie oraz biblioteki, w celu utworzenia wspólnej depozytowej biblioteki gromadzącej i archiwizującej różnego typu zasoby potrzebne w procesach badawczych i edukacyjnych. Obecnie CRL skupia ponad dwieście instytucji partnerskich, które merytorycznie wspiera w ich bieżącej działalności oraz rozwoju. Na podstawie doświadczeń pochodzących z licznych prac badawczych, analiz i testów dotyczących funkcjonowania archiwów cyfrowych CRL pełni funkcję doradcy w wielu inicjatywach związanych z archiwizacją cyfrowych dokumentów[5].

– Digital Curation Center (DCC) to konsorcjum czterech brytyjskich instytucji partnerkich (University of Edinburgh, University of Glasgow, University of Bath, Science and Technology Facilities Council). Zostało powołane w 2004 r. w celu merytorycznego wsparcia brytyjskich instytucji naukowych, badawczych, edukacyjnych, etc., generujących i przechowujących cyfrowe zasoby. DCC ma doradzać w zakresie metod i narzędzi długoterminowego i stabilnego zarządzania zasobami cyfrowymi[6]. DCC bardzo aktywnie działa w międzynarodowej grupie do spraw audytu i certyfikacji archiwów cyfrowych. Obecnie DCC wspiera prace w zakresie standaryzacji procesów audytu i certyfikacji wiarygodnych archiwów cyfrowych. DCC ściśle współpracuje z Digital Preservation Coalition[7].

Ustalenia stanowiące efekt prac przedstawionych organizacji i ściśle z nimi współpracujących instytucji zaprezentowano w dalszej części artykułu.

ARCHIWA ELEKTRONICZNE – DEFINICJA I TYPOLOGIA

Z przeglądu definicji dostępnych w piśmiennictwie przedmiotu (Reitz, 2004, p. 216; *Kriterienkatalog*..., 2006, S. 2) wynika, że pod pojęciem *archiwum elektroniczne*, bądź *archiwum cyfrowe* należy rozumieć organizację ludzi oraz narzędzi lub system złożony z osób oraz przyjętych rozwiązań organizacyjnych i technicznych, powołany w celu zgromadzenia, przechowania oraz zapewnienia długoterminowego dostępu i użyteczności cyfrowego materiału. Działania archiwum koncentrują się na pracach związanych z przeprowadzeniem cyfrowych dokumentów przez kolejne etapy rozwoju technologicznego i przy użyciu najróżniejszych narzędzi i metod archiwizacji, między innymi migracji oraz emulacji. Docelowo archiwum ma zapewnić obecnym oraz przyszłym użytkownikom możliwość odczytu i interpretacji autentycznych, integralnych, wiarygodnych dokumentów cyfrowych (*Eine kleine Enzyklopädie*..., 2008, S. 116). W wypowiedziach na temat archiwów cyfrowych autorzy często odwołują się do standardu archiwizacji publikacji elektronicznych OAIS (*Reference Model*..., 1999, zob. też Januszko-Szakiel, 2005, s. 342), w którym, oprócz już wymienionych cech, uwzględnia się dążenie archiwum cyfrowego do stałej obserwacji i zabezpieczenia zmieniających się potrzeb docelowej grupy użytkowników, nazywanych niekiedy klientami, czy

[5] Historia powstania oraz obecna działalność CRL jest opisana na stronie WWW pod adresem: <http://www.crl.edu/content.asp?l1=1> [dostęp: 15.12.2008].

[6] Na podstawie informacji zamieszczonych w witrynie WWW organizacji pod adresem: <http://www.dcc.ac.uk/about/> [dostęp: 15.12.2008].

[7] Udział organizacji Digital Preservation Coalition w projektach dotyczących długoterminowej ochrony zasobów cyfrowych jest przedstawiony na stronie WWW pod adresem: <http://www.dpconline.org/graphics/about/> [dostęp: 15.12.2008].

też odbiorcami usług archiwum. Synonimicznie archiwum elektroniczne określane bywa terminem *repozytorium cyfrowe* (Reitz, 2004, p. 216; *Trusted Digital Repositories*..., 2002).

Spektrum funkcjonujących oraz wciąż powstających archiwów cyfrowych jest bardzo szerokie. W jednym z opracowań przedmiotu proponuje się następującą ich typologię (*Kriterienkatalog*..., 2006, S. 3):

– elektroniczne archiwa bibliotek narodowych, realizujące zadania gromadzenia oraz zabezpieczenia cyfrowych produktów wydawniczych, naukowych zasobów sieciowych, także wyników projektów dygitalizacyjnych; docelową grupą ich użytkowników jest ogół społeczeństwa;

– elektroniczne archiwa bibliotek uczelnianych, gromadzące i zarządzające cyfrowymi publikacjami, głównie wydawnictw naukowych, ale dodatkowo kolekcjonujące media dla procesów zdalnego nauczania, cyfrowe wersje rozpraw naukowych, również rozmaite opracowania pracowników dydaktycznych i naukowych, np. reprinty; docelową grupę użytkowników takich archiwów stanowią głównie studenci oraz pracownicy uczelni;

– elektroniczne archiwa centrów i instytutów badawczych, działające w celu gromadzenia i zabezpieczenia danych, powstających w wyniku ich badawczej działalności; klientami archiwów tego typu są zazwyczaj specjaliści dziedzinowi, którzy łączą swą wiedzę z danymi wynikowymi instytucji badawczych, interpretują je i ewentualnie dostarczają nowe wnioski i opracowania przedmiotu;

– elektroniczne archiwa sektora administracji, zarządzania, biznesu, powstające na mocy przepisów obligujących instytucje do stosownego zarządzania oraz przechowania przez określony czas elektronicznych dokumentów powstających i przydatnych w toku ich działalności; w zależności od typu dokumentu, docelową grupą użytkowników może być ogół społeczeństwa bądź pracownicy samej instytucji dla potrzeb wykonywanych przez nich zadań. Od archiwów instytucji pamięci, sektora nauki i kultury, odróżnia je okres przechowywania zbiorów: Nie chodzi w nich o zachowanie długoterminowe, w sensie jak najodleglejszego w przyszłości, lecz o dostępność dokumentów podyktowaną rozmaitymi przepisami prawnymi (niekiedy prawo nakazuje zniszczenie dokumentu, ogranicza bądź zabrania jego użytkowania);

– elektroniczne archiwa muzealne, w których przechowuje się i zarządza cyfrowymi obiektami muzealnymi oraz dygitalizatami obiektów analogowych; mogą być użytkowane przez całe społeczeństwo, głównie jednak przeznaczone są dla osób zawodowo związanych ze światem sztuki i nauki;

– elektroniczne archiwa, organizowane przez zewnętrznych usługodawców, przyjmujące zlecenia archiwizacji zasobów cyfrowych rozmaitych instytucji zarówno tych z sektora biznesu i administracji, jak i nauki oraz kultury; odpowiedzialność za gromadzenie i przekazanie zasobów do archiwum ponoszą instytucje zlecające, natomiast usługodawcy przyjmują obowiązek zabezpieczenia ich dostępności i użyteczności w określonym czasie.

Każde z wymieniowych powyżej typów archiwów można by ogólnie określić jako zbiór dokumentów elektronicznych, zgromadzonych i przechowywanych w określonym miejscu, przez określony czas i dla określonych celów. Dyskusyjny jednak mógłby okazać się fakt stosowania jednakowego określenia w odniesieniu do archiwum elektronicznych materiałów bibliotecznych oraz archiwum elektronicznych dokumentów bankowych, podatkowych, administracyjnych, itp. Należy zwrócić uwagę na odmienność wyobrażeń o systemach archiwalnych instytucji pamięci narodowej i systemach sektora

biznesu lub administracji. Zasadnicza różnica pomiędzy powyższymi systemami tkwi w założeniach dotyczących okresu przechowywania dokumentów. Otóż archiwalne systemy biznesowe, w zależności od rodzaju przechowywanych dokumentów, realizowanych zadań oraz procedur prawnych mają zapewnić dostępność i użyteczność deponowanych materiałów w zakresie od trzech do pięćdziesięciu lat (Sasin, 2004, passim), natomiast systemy archiwalne instytucji pamięci powinny gwarantować utrzymanie użyteczności zbiorów przez okres stu i więcej lat (Borghoff, 2005, S. 31). Wiąże się to z innymi założeniami organizacyjnymi oraz rozwiązaniami technicznymi dla funkcjonowania tychże systemów. Ponadto – na co zwraca uwagę A. Radwański (Radwański, 2005, s.101) – elektroniczne systemy archiwalne w ujęciu biznesowym operują dokumentami prymarnymi, tj. stworzonymi od początku jako dokumenty cyfrowe, natomiast systemy archiwalno-biblioteczne dotyczą dodatkowo dokumentów wtórnych, tj. cyfrowych surogatów dokumentów papierowych. Skutkuje to innymi oczekiwaniami i nakłada na system archiwalny dodatkowe powinności. Zdaniem A. Radwańskiego elektroniczne archiwum, czyli zbiór dokumentów cyfrowych w sensie archiwalno-bibliotecznym musi sprostać zasadniczym problemom, tj. długotrwałemu przechowywaniu dokumentów cyfrowych, zarządzaniu wielką liczbą dokumentów elektronicznych oraz umożliwić ich sprawne indeksowanie, wyszukiwanie i udostępnianie użytkownikom.

Istotę funkcjonowania systemów archiwalnych, głównie tych organizowanych w bibliotekach, przybliżają wypowiedzi specjalistów[8], z których wynika, że działanie bibliotecznych archiwów elektronicznych wymaga dwóch zasadniczych elementów składowych, tj. serwera, na którym jest posadowiony system biblioteczny (realizujący zadania bieżącej obsługi biblioteki i jej użytkowników), oraz systemu depozytowego, stanowiącego jądro archiwum, którego zadaniem jest długoterminowa archiwizacja materiału cyfrowego. Rozróżnienie to ma ogromne znaczenie z uwagi na brak zgodności fachowców co do tego, czy archiwum elektroniczne powinno posiadać dwa odrębne zasoby, z których jeden byłby kompletnym zbiorem dokumentów elektronicznych, natomiast drugi tworzyłby wyselekcjonowaną kolekcję publikacji stanowiących dziedzictwo nauki i kultury, deponowanych długoterminowo z myślą – tylko i wyłącznie – o przyszłych użytkownikach (model rozłączny zasobów wewnątrz archiwum bibliotecznego), czy też wszystkie biblioteczne zasoby cyfrowe powinny być przechowywane długoterminowo w systemie depozytowym i stąd pobierane również przez system biblioteczny w celu bieżącego udostępniania użytkownikom (model zasobów połączonych wewnątrz archiwum bibliotecznego).

Argumentem przemawiającym za rozłącznością zasobów „depozytowego" oraz „bieżącego" jest ich odmienny charakter; otóż – w myśl niektórych opinii – zasoby archiwizowane w systemie depozytowym powinny być starannie dobraną, reprezentatywną kolekcją dóbr nauki i kultury, nikłe są bowiem możliwości zachowania dla przyszłych użytkowników wszystkich dokumentów publikowanych w wersji elektronicznej. Wydaje się wielce prawdopodobne, że nawet biblioteki narodowe, ustawowo zobowiązane do zachowania kompletnego dziedzictwa nauki i kultury będą zmuszone do wyboru spośród

[8] Na podstawie opinii fachowców głoszonych podczas cyklu warsztatów organizowanych w latach 2002-2004 w Bibliotece Niemieckiej DDB: *Workshop des Kompetenznetzwerkes Neue Dienste, Standards und Metadaten*, oraz rozmów z pracownikami Biblioteki podczas hospitacji w dniach 01-08.10.2003 r. w dziale IT DDB, zajmującymi się opracowywaniem długoterminowej strategii postępowania z niemieckimi publikacjami elektronicznymi.

kompletnej oferty wydawniczej tych dokumentów, które z racji swej treści i formy zasługują na długoterminową archiwizację. Jednocześnie biblioteki muszą brać pod uwagę fakt, iż obecni użytkownicy mają prawo do bieżącego korzystania z wszelkich publikowanych materiałów, bez względu na to, czy stanowią one dziedzictwo narodowe, czy też nie. Zatem konieczne jest gromadzenie i udostępnianie kompletu wydawniczej oferty. Stąd pomysł, aby z myślą o obecnych użytkownikach, system biblioteczny gromadził i udostępniał na bieżąco wszystkie publikowane dokumenty, natomiast system depozytowy przejął zadania długoterminowej archiwizacji wyselekcjonowanej kolekcji dokumentów stanowiących dziedzictwo nauki i kultury, zabezpieczając tym samym potrzeby przyszłych użytkowników.

Kolejny punkt polemiki, dotyczący organizacji i funkcjonowania archiwów elektronicznych, wywoływany jest przez różne podejścia fachowców do problemu częstotliwości użytkowania zbiorów. Jedni twierdzą, że użytkowanie publikacji elektronicznych, zwłaszcza tych z systemu depozytowego, i to jak najczęstsze, jest wielce pożądane. Wraz z realizacją procesów użytkowania wzrasta prawdopodobieństwo wykrycia ewentualnych utrudnień odczytu i prezentacji dokumentów cyfrowych, tym samym minimalizuje się ryzyko bezpowrotnej utraty dokumentu, na przykład z racji niezauważonych zmian technologicznych i wywołanych przez nie braków w otoczeniu sprzętowym lub programowym. Bieżące udostępnianie zbiorów cyfrowych jest – ich zdaniem – sposobem obserwacji zmian technologicznych, tym samym zwiększeniem szans na podjęcie stosownych działań we właściwym czasie. W bieżącym udostępnianiu zbiorów archiwalnych widzą oni strategię długoterminowego utrzymania ich użyteczności. Takie podejście wywodzi się prawdopodobnie z doświadczeń uzyskanych podczas funkcjonowania komputerowych systemów zarządzających archiwaliami tradycyjnymi, w których moduł „konserwacja" umożliwia przejście do pliku zawierającego wykaz archiwalnych jednostek, które powinny zostać poddane zabiegom konserwatorskim. Jednostki wymagające konserwacji są „wychwytywane" właśnie w procesie udostępniania archiwaliów. Wykrycie dokumentu wymagającego prac konserwatorskich wiąże się z poczynieniem w module „konserwacja" stosownej adnotacji o jego stanie (Pest, 2007, s. 15-23)[9].

Z kolei zwolennicy rozdzielnego modelu zasobów archiwum elektronicznego bronią przekonania, iż bieżące udostępnianie zbiorów z systemu depozytowego może okazać się zgubne w skutkach. W procesach ich częstego użytkowania i w wyniku ewentualnych niepożądanych działań użytkowników zbiory te są narażone na ryzyko naruszenia ich integralności i autentyczności. Dodatkowo udostępnianie i użytkowanie dokumentów z depozytu może utrudniać prace charakterystyczne dla procesu ich długoterminowej archiwizacji. Stąd uważa się, że archiwalne zbiory depozytowe należałoby oddzielić od zbiorów użytku bieżącego, udostępniać je wyłącznie osobom upoważnionym do prac konserwatorskich, przewidzianych w strategii ich długoterminowej archiwizacji.

Chociaż w obu przedstawionych podejściach występują elementy racjonalnego postępowania ze zbiorami cyfrowymi, bardziej przekonujący wydaje się pogląd o bieżącym użytkowaniu zasobów archiwalnych. Przy obecnych

[9] Wspomniany moduł „konserwacja" istnieje i podobnie funkcjonuje w wielu rozmaitych programach obsługi archiwów i bibliotek. Podany przykład pochodzi z publikacji Czesława Pesta pt.: Zastosowanie programu TABULARIUM do kompleksowej obsługi archiwum i biblioteki. *Archiwista Polski*, nr 1(45)/2007, s. 15-23.

możliwościach technicznych oraz starannie przemyślanej taktyce działania specjaliści są w stanie ochronić autentyczność i integralność materiału cyfrowego. Ponadto argumentem przemawiającym przeciwko rozdzielności zasobów jest fakt stałego wzrostu liczby nowopowstających dokumentów i idącej za tym ich łącznej objętości. Podwajanie nawet najmniejszych objętościowo zasobów wiąże się z dodatkowymi kosztami ich utrzymania oraz zwiększonymi wymaganiami technicznymi stawianymi przed systemami opartymi na zdublowanych zbiorach.

Abstrahując od wymienionych wcześniej argumentów, prawdopodobne wydaje się, że zarówno model rozłączenia zasobów, jak i model zasobów połączonych przyniósłby pożądany efekt końcowy. Oba modele archiwizacji są w stanie zapewnić dostępność i użyteczność cyfrowego materiału w długim czasie. Jednak, aby miały szansę sprawdzić się w praktyce, musiałyby zostać wbudowane w sprecyzowaną, kompleksową strategię długoterminowej archiwizacji zbiorów cyfrowych. Pomimo wysiłków wielu instytucji na świecie takie strategie należą wciąż do rzadkości, a nawet jeśli powstają, nie są popularyzowane i rekomendowane, ponieważ zwykle są rozwiązaniami tymczasowymi, modyfikowanymi, dostosowywanymi do zmieniających się potrzeb i okoliczności, a przede wszystkim są to rozwiązania niesprawdzone. Ich efektywność można sprawdzić i ocenić jedynie w dłuższym czasie i w obliczu zachodzących zmian technologicznych.

Z dyskusji fachowców wynika, że istnieje duże zapotrzebowanie na wszelkie hipotetyczne scenariusze organizacji i działania archiwów elektronicznych. Należy jednak koncentrować się na tworzeniu rozwiązań kompleksowych, wielozadaniowych, elastycznych, umożliwiających ewentualną reorganizację wstępnych założeń.

PROBLEM WIARYGODNOŚCI ARCHIWUM CYFROWEGO

W literaturze przedmiotu mocno akcentowane są starania, aby wszelkie funkcjonujące i planowane archiwa cyfrowe, zwłaszcza te przechowujące cyfrowe dziedzictwo nauki i kultury, zasłużyły na miano instytucji wiarygodnych, autentycznych, stabilnych i niezawodnych (ang. *trusted digital repository, trustworthy digital repositories,* niem. *vertrauenswürdiges digitales Langzeitarchiv*) (*Trusted Digital Repositories...*, 2002, p. 8, *Kriterienkatalog...*, 2006, S. 9, *Trustworthy Repositories...*, 2007, p. 3). Wciąż jednak trwają prace nad identyfikacją cech, których posiadanie zapewni archiwom cyfrowym taki status.

Obecnie charakteryzowaniem repozytoriów elektronicznych zajmują się najintensywniej RLG wraz z OCLC i NARA oraz współpracująca z nimi niemiecka grupa Nestor.

Pierwsze efekty prac RLG z tego zakresu znane są z raportów opublikowanych w 2001 i 2002 r. (*Trusted Digital Repositories...*, 2000, *Attributes of a Trusted...*, 2001). Raporty te zawierają ustalenia specjalnej grupy roboczej, powołanej ze struktur RLG oraz OCLC, odnośnie właściwości archiwów cyfrowych budowanych na podstawie modelu referencyjnego OAIS, tworzonych dla potrzeb instytucji pamięci odpowiedzialnych za długoterminową archiwizację dokumentów cyfrowych. Celem grupy roboczej było określenie cech wiarygodnych i stabilnych archiwów, powstających w instytucjach sektora nauki i kultury, w celu gromadzenia i przechowywania różnorodnych pu-

blikacji elektronicznych. RLG oraz OCLC zajmują się między innymi rozwojem procedur certyfikacji wiarygodnych archiwów cyfrowych, prowadzą badania oraz tworzą narzędzia identyfikacji cech materiałów, które powinny podlegać długookresowemu przechowaniu, pracują nad rozwojem modelu sieci współpracujących archiwów, rozwijają system jednoznacznej, stabilnej identyfikacji obiektów cyfrowych, prowadzą badania i rozpowszechniają informacje dotyczące związku pomiędzy elektroniczną archiwizacją dokumentów oraz ochroną praw autorskich. Ponadto grupa RLG/OCLC pracuje nad określeniem technicznych strategii gwarantujących permanentną dostępność archiwizowanych obiektów cyfrowych, definiuje minimalny poziom metadanych koniecznych w procesie długoterminowego zarządzania nimi oraz działa w zakresie rozwoju narzędzi do ich automatycznego generowania.

Z ustaleń zamieszczonych we wspomnianych raportach wynika, że wiarygodne archiwum elektroniczne to takie, które gwarantuje dostępność przechowywanych i zarządzanych w nim dokumentów elektronicznych obecnie i w odległej przyszłości, przyjmuje odpowiedzialność za przeprowadzanie stosownych prac konserwatorskich w imieniu swoich deponentów oraz na rzecz potrzeb obecnych i przyszłych użytkowników. Projekt takiego archiwum powinien uwzględnić powszechnie przyjęte umowy i standardy w zakresie zapewnienia ciągłości zarządzania bezpieczeństwem i dostępności deponowanego w nim materiału cyfrowego. Ponadto potrzebne jest wypracowanie metod oceniania systemu pod względem spełniania oczekiwań użytkowników odnośnie jego wiarygodności. W celu odróżniania wiarygodnych archiwów od tych, które nie gwarantują niezawodności w zakresie utrzymania dostępu do zdeponowanego materiału cyfrowego, niezbędne jest zidentyfikowanie atrybutów systemu, które są w stanie przekonać użytkowników o jego zdolności do długoterminowego i stabilnego zarządzania dokumentami cyfrowymi. Zdaniem specjalistów, działania oraz wydajność i efektywność systemów archiwizacji powinny podlegać okresowym pomiarom i kontroli, a zatem być sprawdzalne i mierzalne (*Trusted Digital Repositories*..., 2002, *Attributes of a Trusted*..., 2001, passim). Dodatkowo archiwum cyfrowe powinno posiadać sprecyzowaną politykę sporządzania i kontroli kopii zapasowych archiwizowanych obiektów, dysponować narzędziami wykrywania i odzysku utraconych lub uszkodzonych dokumentów, dbać o kontakty z wydawcami, zapewniać jawność informacji o tym, co i w jaki sposób jest archiwizowane. W raportach zwraca się też uwagę na równowagę kosztów i korzyści, to znaczy na to, że należy starannie rozważyć, czy cyfrowy obiekt jest wart kosztów ponoszonych w procesie jego archiwizacji. W podsumowującym zestawieniu atrybuty archiwum cyfrowego zakwalifikowano do czterech następujących grup: odpowiedzialność administracyjna, wykonalność organizacyjna, równowaga ekonomiczna, podstawy proceduralne (*Attributes of a Trusted*..., 2001, p. 11).

Omawiane raporty, o charakterze ustaleń wstępnych i ogólnym zarysie wiedzy na temat wiarygodnych archiwów cyfrowych, okazały się bazą dla dalszych prac nad identyfikowaniem wiarygodności archiwów, nie tylko w strukturach RLG, ale także w ramach innych organizacji.

W 2003 r. RLG wraz z NARA utworzyły grupę roboczą, której działania dedykowano stricte certyfikacji archiwów cyfrowych (RLG-NARA Digital Repository Certification Task Force). Głównym celem grupy było ustalenie katalogu kryteriów identyfikacyjnych dla wiarygodnych, stabilnych, długoterminowych archiwów cyfrowych, na podstawie których możliwe byłoby opra-

cowanie potencjalnego modelu audytu i certyfikacji archiwów cyfrowych. Po dwóch latach pracy, grupa opublikowała propozycję rejestru atrybutów, umożliwiających rozpoznanie wiarygodnych archiwów cyfrowych – *An Audit Checklist for the Certification of Trusted Digital Repositories. Draft for Public Comment* (*An Audit Checklist...*, 2005). Dokument, jak tytuł wskazuje, miał stanowić podstawę konstruktywnej dyskusji przedmiotu i tak też został odebrany. Do dyskusji i prac przyłączyło się wiele instytucji i organizacji (*Trustworthy Repositories...*, 2007, p. 3), m.in. niemiecka grupa robocza NESTOR.

W ramach przedsięwzięcia „Wiarygodne archiwa – certyfikacja" grupa NESTOR stara się, podobnie jak amerykańska grupa RLG-NARA, identyfikować kryteria umożliwiające oszacowanie wiarygodności cyfrowego archiwum, głównie pod względem organizacyjnych oraz technicznych parametrów. Praca grupy odbywa się na forum otwartym przy współpracy instytucji archiwizujących (przedstawicieli bibliotek, archiwów, muzeów, centrów badawczych) oraz twórców publikacji cyfrowych (wydawców), z udziałem specjalistów ściśle powiązanych z tematyką (przedstawiciele branży IT oraz znawcy zagadnień związanych z certyfikacją), także osób zainteresowanych i chętnych do pracy w tym zakresie. Otwartość działań i szerokie spektrum uczestników ma być podstawą do rozwiązań możliwie ogólnego zastosowania i wysoce przydatnych w praktyce, także powszechnie akceptowanych. Swoje działania NESTOR postrzega jako wsparcie dla prac innych grup, np. RLG-NARA i udział w ustaleniu międzynarodowych standardów tworzenia wiarygodnych archiwów cyfrowych (*Kriterienkatalog...*, 2006, passim).

W efekcie dotychczasowych prac zespołów RLG-NARA oraz NESTOR powstały dwa, bardzo podobne w swej treści rejestry atrybutów wiarygodnych archiwów cyfrowych – angielskojęzyczny: *Trustworthy Repositories Audit & Certification. Criteria and Checklist* (*Trustworthy Repositories...*, 2007) oraz niemieckojęzyczny: *Kriterienkatalog vertrauenswürdige digitale Langzeitarchive. Version 1. Entwurf zur öffentlichen Kommentierung* (*Kriterienkatalog...*, 2006).

Oba zaproponowane katalogi kryteriów wiarygodnych archiwów cyfrowych mają charakter vademecum. Zawierają wskazówki dotyczące prac koncepcyjnych, planowania oraz organizacji, w późniejszej fazie także kontroli funkcjonowania wiarygodnych długoterminowych archiwów cyfrowych. Są pomyślane jako podręcznik dla wszelkich instytucji, które podejmują zadania archiwizacji zasobów cyfrowych, także dla komercyjnych usługodawców w zakresie cyfrowej archiwistyki. W pracach nad charakterystyką wiarygodnych archiwów cyfrowych, za punkt wyjściowy obie grupy przyjęły referencyjny model OAIS. Posługują się więc standaryzowanym nazewnictwem procesów zachodzących w archiwach cyfrowych, akceptują normatywny sposób organizacji i funkcjonowania obiektów cyfrowych w archiwach.

W obu katalogach obok kryteriów oceny wiarygodności archiwów cyfrowych wymieniono cztery zasady ich wprowadzania do archiwów (*Kriterienkatalog...*, 2006, S. 4, *Trustworthy Repositories...*, 2007, p. 6):

1. Dokumentacja: wszelkie pomysły, plany, wdrożenia, zastosowane normy jakościowe i normy bezpieczeństwa dotyczące archiwum cyfrowego, powinny być skrupulatnie dokumentowane i poddawane ocenie wewnętrznej oraz zewnętrznej. Cenne mogą okazać się wszelkie spostrzeżenia i wskazówki zarówno ze strony pracowników instytucji inicjującej działania, jak i opinii publicznej. Możliwie wczesna ocena jest środkiem zapobiegawczym przed

popełnieniem ewentualnych błędów. Ponadto stosowne, konsekwentne dokumentowanie wszystkich obszarów i etapów prac umożliwia kompleksową ocenę spójności i poprawności pracy archiwum.

2. Przejrzystość: działania związane z tworzeniem archiwum cyfrowego, jak i jego późniejsze funkcjonowanie powinny być transparentne, zarówno wewnątrz organizacji jak i na zewnątrz. W celu osiągnięcia przejrzystości zewnętrznej zaleca się podawanie do ogólnej wiadomości, jaki jest stan zaawansowania prac. Permanentne publikowanie tworzonych raportów i dokumentacji, tym samym informowanie deponentów oraz użytkowników o wszystkim, co dotyczy archiwum, umożliwia im samodzielną ocenę stopnia jego wiarygodności. Twórcom[10] dodatkowo pozwala przekonać się o tym, czy archiwum jest w stanie zapewnić ich produktom stosowną ochronę. Przejrzystość wewnętrzna natomiast jest przydatna osobom czynnie zaangażowanym w prace nad tworzeniem i funkcjonowaniem archiwum. Poprzez bieżące, wzajemne informowanie o wykonywanych i planowanych czynnościach we wszystkich obszarach działań, menedżerowie oraz wykonawcy zadań mają możliwość stwierdzenia, czy archiwum osiąga zakładany stan rozwoju i jakości. Ponadto umożliwia osobom skupionym nad poszczególnymi fragmentami prac i zadań archiwum, objąć je i zrozumieć ich znaczenie w działaniu jednego systemu. W przypadku fragmentów dokumentacji, zawierających informacje tajne, kieruje się je tylko do wiadomości osób upoważnionych. Mówi się wówczas o przejrzystości zawężonej.

3. Adekwatność: przy tworzeniu archiwów cyfrowych zaleca się przyjęcie zasady adekwatności, w myśl której mało realne, a nawet niemożliwe jest stworzenie rozwiązań absolutnie standardowych. Wszelkie proponowane metody, sposoby, tudzież formy postępowania na rzecz ochrony zasobów cyfrowych wymagają oszacowania za każdym razem ich przydatności w realizacji zadań określonej instytucji archiwizującej. Rozwiązania z powodzeniem sprawdzające się w jednym archiwum mogą tylko częściowo albo w ogóle nie znaleźć zastosowania w innym. Należy uwzględnić obowiązujące przepisy prawne, zasoby personalne oraz finansowe, także ewentualnie istniejące już struktury organizacyjne oraz stopień zaawansowania prac na rzecz opracowania instytucjonalnej, lokalnej albo narodowej strategii długoterminowej archiwizacji zasobów cyfrowych.

4. Ewaluacja: w przypadku oceny wiarygodności archiwum cyfrowego – postrzeganej szczególnie jako jego zdolność do ochrony długoterminowej – nie wymieniono dotychczas atrybutów dających się obiektywnie i jednoznacznie oszacować, zmierzyć. Wciąż trwają prace nad utworzeniem ostatecznego wykazu wskaźników reprezentujących wiarygodność archiwum. Wszelkie propozycje wskaźników powinny zostać podane do powszechnej wiadomości, raz z racji uzyskania komentarzy i opinii o nich, dwa jako element działań na rzecz zapewnienia przejrzystości archiwum.

Wiarygodność archiwów cyfrowych – zdaniem przedstawicieli grupy Nestor – nie powinna być postrzegana jak pojęcie absolutne, lecz odnoszące się każdorazowo do indywidualnych założeń, zadań i celów poszczególnych archiwów. Każde archiwum powinno opublikować swoje cele i, w myśl zasady adekwatności, wybrać spośród istniejących rozwiązań te, które umożliwią ich realizację. Proces ewaluacji wiarygodności archiwum powinien polegać

[10] Pod pojęciem *twórcy* w omawianym opracowaniu rozumie się wszystkie osoby (autora, informatyka, wydawcę, dostawcę), którzy mają swój udział w opublikowaniu i dostarczeniu do archiwum dokumentu cyfrowego w jego ostatecznej treści i formie.

właśnie na obserwacji transparentnych poczynań archiwum i opiniowaniu przez obserwatorów, głównie deponentów i użytkowników, w jaki sposób radzi sobie ono z realizacją wytyczonych celów (*Kriterienkatalog*..., 2006, s. 7). Dodatkowo grupa NESTOR zaznacza, że wiarygodność archiwów cyfrowych jest ściśle powiązana ze stabilnością techniczną, zapewnianą przez specjalistów branży IT (*Kriterienkatalog*..., 2006, s. 3).

KRYTERIA OCENY WIARYGODNOŚCI ARCHIWUM CYFROWEGO

Poniżej przedstawione jest zestawienie zbiorcze kryteriów identyfikacji wiarygodnego długoterminowego archiwum cyfrowego, które wyróżnione zostały w omawianych katalogach i zgrupowane w trzech klasach (*Kriterienkatalog*..., 2006, S. 7-29, *Trustworthy Repositories*..., 2007, pp. 10-49):

A – RAMY ORGANIZACYJNE

Archiwum cyfrowe działa w organizacyjnych ramach, wynikających ze zdefiniowanych celów archiwum, uwarunkowań prawnych, a także zasobów kadrowych i finansowych.

1. Definiowanie celu działalności archiwum cyfrowego. Archiwum cyfrowe określa swoje założenia, obowiązki, zadania do wykonania oraz zasady, którymi kieruje się w ich wykonywaniu. Cele archiwum cyfrowego są transparentne, publikowane w formie tzw. „policy" (*Eine kleine Enzyklopädie*..., 2008, s. 49)[11].

1.1. Opracowanie kryteriów gromadzenia obiektów cyfrowych. Archiwum cyfrowe możliwie jednoznacznie wskazuje cechy obiektów cyfrowych podlegających długoterminowej ochronie. Niekiedy przyjęcie do kolekcji archiwalnej obiektu cyfrowego może być podyktowane odrębnymi przepisami prawnymi, którym instytucja archiwizująca powinna podporządkować się w swej działalności. Oprócz procedur selekcji i oceny archiwum cyfrowe określa zasady przekazania obiektu cyfrowego do archiwum.

1.2. Przyjęcie odpowiedzialności za długoterminową ochronę obiektów cyfrowych. Archiwum cyfrowe oświadcza, iż przyjmuje odpowiedzialność za długoterminowe zabezpieczenie dostępności oraz użyteczności zasobów cyfrowych, zgromadzonych na podstawie ustaleń wynikających z punktu 1.1.

1.3. Definiowanie grupy użytkowników docelowych archiwum cyfrowego. Archiwum cyfrowe określa grupę(y) użytkowników, dla których potrzeb działa, rozpoznaje specyfikę ich oczekiwań i na tej podstawie dobiera odpowiednie narzędzia i metody pracy. Ponadto archiwum przyjmuje obowiązek stałego monitorowania wymogów użytkowników i dostosowywania do nich swych usług.

[11] Najogólniej pod pojęciem „Presevation Policy" należy rozumieć zbiór dokumentów (o charakterze ustaw, postanowień, umów, rozporządzeń, wytycznych, etc.) regulujących procesy długoterminowej archiwizacji zasobów cyfrowych. W odróżnieniu od strategii archiwizacji, która określa sposób ochrony materiału cyfrowego, *preservation policy* wskazuje co, dlaczego, gdzie i jak długo powinno podlegać ochronie. *Preservation Policy* jest niezbędną podstawą dla strategii archiwizacji. Na podstawie: Nestor Handbuch: *Eine kleine Enzyklopädie der digitalen Langzeitarchivierung*. Version 1.2, Juni 2008, S. 49. [online]. [dostęp: 28.09.2008]. Dostępny w World Wide Web: <http://nestor.sub.uni-goettingen.de/handbuch/nestor-handbuch.pdf>.

2. Tworzenie możliwości użytkowania archiwalnych zasobów cyfrowych. Archiwum cyfrowe przyjmuje za podstawowe zadanie stworzenie swym obecnym i przyszłym klientom możliwości użytkowania, czyli odczytu i interpretacji treści reprezentowanych przez chronione obiekty archiwalne. Zakres użytkowania może być różny, w zależności od ewentualnych obostrzeń prawnych lub niepowodzenia w zachowaniu pewnych atrybutów oryginału. W przypadkach tego typu niepowodzeń, czy też poważniejszych zagrożeń utraty zasobów archiwalnych wykorzystywane są zasoby tzw. ciemnych archiwów (nieoficjalnych, drugiego obiegu), których założeniem jest ochrona zasobów, jednak bez możliwości ich tradycyjnego użytkowania. Są pomyślane jako forma zastępstwa dla archiwów cyfrowych w sytuacjach szczególnie kryzysowych.

2.1. Organizacja dostępu użytkowników do archiwalnych zasobów cyfrowych. Archiwum cyfrowe gwarantuje uprawnionym użytkownikom dostęp do obiektów cyfrowych, stwarzając przy tym stosowne narzędzia ich wyszukiwania. Ustala jasne zasady organizacyjne korzystania z zasobów oraz informuje o ewentualnych kosztach np. wydruku, zapisu na nośniku, wysłania pocztą mailową.

2.2. Zapewnienie użytkownikom możliwości interpretacji treści cyfrowych obiektów. Archiwum cyfrowe podejmuje działania na rzecz zagwarantowania użytkownikom możliwości odczytu i interpretacji dokumentów cyfrowych, zarówno ich treści, jak i metadanych. W tym celu wymagane jest wiele zabiegów natury technicznej, m.in. okresowa kontrola odczytu i interpretacji obiektów. Archiwa stosują również tzw. formularz zwrotny, dzięki któremu użytkownicy mogą zgłaszać ewentualne trudności odczytu i interpretacji.

3. Respektowanie przepisów prawnych i umownych. Archiwa cyfrowe działają na bazie określonych regulacji ustawowych oraz umownych. Dotyczą one w szczególności sposobu pozyskiwania zasobów archiwalnych, ich ochrony oraz udostępniania. Archiwa starają się uwzględniać zarówno interesy twórców publikacji, jak i potrzeby użytkowników.

3.1. Prawne uregulowanie współpracy archiwum cyfrowego z twórcami publikacji. W celu działania planowego oraz zgodnego z prawem archiwa cyfrowe zawierają formalne porozumienia z wydawcami publikacji, w których precyzowane są warunki procesów: przekazania publikacji do archiwum, archiwizacji, użytkowania. Pewne obowiązki i zadania zarówno archiwów, jak i wydawców mogą wynikać z obowiązujących aktów prawnych; dodatkowe porozumienia i umowy określają sposób realizacji tychże zadań.

3.2. Respektowanie przepisów prawnych dotyczących procesów długoterminowej ochrony obiektów cyfrowych. Archiwa cyfrowe regulują stosownymi zapisami procesy związane z archiwizacją obiektów cyfrowych, np. prawo dostępu, w celu przeprowadzania prac konserwatorskich na obiektach. Ponadto przestrzegania wymagają zapisy ustawy o prawie autorskim związane z ewentualnymi zmianami treści i formy dokumentu.

3.3. Respektowanie przepisów prawnych dotyczących procesów użytkowania zasobów cyfrowych. Archiwa cyfrowe dbają o to, aby użytkowanie deponowanych zasobów cyfrowych odbywało się z poszanowaniem przepisów prawnych. Przestrzegania wymagają przede wszystkim ustawy o prawie autorskim oraz o ochronie danych, także na przykład przepisy regulujące okres przechowywania dokumentów w archiwach. Wszelkie ograniczenia i bariery uniemożliwiające użytkowanie zasobów powinny być dokumentowane wraz z uzasadnieniem ich podstaw.

4. Dostosowanie formy organizacyjnej archiwum cyfrowego do realizowanych w nim celów. W zależności od założeń archiwa cyfrowe mogą działać i zapewniać ochronę krótko-, średnio- lub długoterminową zdeponowanych zasobów cyfrowych. Wydajność oraz trwałość archiwum cyfrowego to parametry podlegające ocenie deponentów oraz użytkowników i wpływające na jego wiarygodność. Podstawy tej oceny są wymienione w kolejnych podpunktach:

4.1. Zabezpieczenie finansowania działalności archiwum cyfrowego. Archiwum cyfrowe zapewnia swych klientów o finansowym zabezpieczeniu swojej działalności. Zarówno archiwa państwowe, jak i prywatne – w szczególności długoterminowe – powinny wskazać prawną podstawę oraz źródła finansowania. Archiwa państwowe są zazwyczaj finansowane z budżetu państwa i to państwo jest gwarantem ich finansowej stabilności. Natomiast archiwa prywatne świadczą usługi odpłatnie, ich finansowa kondycja jest wynikiem powodzenia na rynku, wewnętrznej gospodarki finansowej, finansowego planowania. Aktualna sytuacja i polityka finansowa archiwum cyfrowego przekłada się na ocenę jego wiarygodności.

4.2. Dyspozycyjność personelu o odpowiednich kwalifikacjach. Archiwum cyfrowe zatrudnia stosowną ilość kadry z odpowiednimi kwalifikacjami. Dla zapewnienia długoterminowej skuteczności konieczny jest stały rozwój kadry, w sensie dostosowywania kwalifikacji do zmieniających się okoliczności funkcjonowania archiwum. Archiwum dba o ilość i jakość personelu tak, aby wszystkie czynności związane z jego funkcjonowaniem były wykonywane zgodnie z założeniami ilościowymi, jakościowymi oraz terminowymi. W zasadzie wszystkie archiwa cyfrowe, w szczególności jednak te z planem funkcjonowania długoterminowego, muszą w swych planach organizacyjnych i finansowych, uwzględnić procesy dokształcania kadry. Zapewnione powinny być czas i pieniądze na udział personelu w specjalistycznych kursach, szkoleniach, krajowych oraz międzynarodowych konferencjach. Należy także uwzględnić potrzebę dostępu do fachowej literatury, etc. Świadectwa obecności personelu we wszelkich formach podnoszenia kwalifikacji wpływają na ocenę jego wiarygodności.

4.3. Powoływanie stosownych struktur organizacyjnych. Struktura organizacyjna archiwum cyfrowego powinna być ściśle dostosowana do jego założeń, realizowanych celów, zadań. Procesom zachodzącym w archiwach należy przyporządkować stosowne zasoby personalne oraz materialne, umożliwiające realizację założonych celów.

4.4. Sporządzanie planów długoterminowych. Archiwa cyfrowe sporządzają plany działania, w których uwzględniane są wszelkie zadania do wykonania obecnie i w przyszłości, wraz z określeniem terminów. Dla zapewnienia ich długoterminowego działania prowadzą też tzw. zapobiegawcze planowanie strategiczne, polegające na stałej obserwacji pewnych zjawisk, przewidywaniu ewentualnych zmian i wytyczaniu w związku z nimi nowych zadań. Monitorują głównie zmiany technologiczne (w modelu OAIS określane jako *Monitor Technology*) oraz zmiany oczekiwań i potrzeb użytkowników (za OAIS *Monitor Designated Community*). Mogą się zmieniać również podstawy prawne oraz finansowe działania archiwów cyfrowych. Elementem planowania jest zabezpieczenie potrzebnych zasobów.

4.5. Kontynuacja ochrony zasobów archiwalnych w sytuacjach kryzysowych. Archiwa cyfrowe, w szczególności długoterminowe, opracowują strategię postępowania i zapewnienia ciągłości ochrony zasobów w sytuacjach kry-

zysowych. Przy założeniu ewentualnej potrzeby przekazania zasobów archiwalnych do instytucji partnerskiej bądź następczej, archiwum cyfrowe stosownie wcześniej planuje proces przekazania swoich obowiązków, definiuje jego warunki i przygotowuje potrzebną infrastrukturę. Przede wszystkim konieczny jest staranny dobór instytucji partnerskiej oraz zawiązanie umowy o partnerstwie, na mocy której w razie konieczności instytucja ta obejmie zagrożone zasoby stosową ochroną. W takich sytuacjach szczególne znaczenie ma staranna dokumentacja dotycząca wszystkich zasobów kolekcji wraz z metadanymi. Dokumentacja stanowi dla archiwum przejmującego obowiązki ochrony podstawowe źródło wiedzy o ilościowym i jakościowym stanie zasobów, jak i przyjętej strategii ich archiwizacji.

5. Zarządzanie jakością w archiwum cyfrowym. Oddział zarządzania jakością kontroluje realizację wszystkich procesów i zadań składających się na osiągnięcie celów archiwum cyfrowego. Oddział obejmuje kontrolą procesy zachodzące we wszystkich obszarach działalności archiwum.

5.1. Podział zadań i obowiązków w ramach realizowanych procesów. Oddział zarządzania jakością dba o przyporządkowanie wszystkim procesom i zadaniom realizowanym w archiwum cyfrowym odpowiednich zasobów kadrowych i materialnych. Szczególnie starannie definiuje odpowiedzialność za realizację procesów i zadań współzależnych (przy wzajemnym oddziaływaniu wielu osób, bądź zespołów na efekt końcowy). Równie istotna jest odpowiedzialność za procesy zewnętrzne, realizowane poza archiwum, jednak wpływające na przebieg procesów wewnętrznych (np. tworzenie i dostarczanie obiektów cyfrowych do archiwum).

5.2. Zarządzanie dokumentacją archiwum cyfrowego. Oddział zarządzania jakością dba o sprawne działanie systemu zarządzania dokumentacją dotyczącą wszystkich elementów składowych archiwum. Sprawuje kontrolę nad przestrzeganiem reguł dotyczących kompletności, poprawności, aktualności, zrozumiałości oraz dostępności dokumentacji. Dokumentacja archiwum powstaje wg precyzyjnych wytycznych.

5.3. Reagowanie archiwum cyfrowego na zmiany. Oddział zarządzania jakością nadzoruje procesy monitoringu zmian głównie natury technicznej (np. standardy formatów zapisu i nośników danych cyfrowych), ale również organizacyjnej (np. sposób finansowania działań archiwum, przekazanie odpowiedzialności instytucji partnerskiej lub następczej), a także natury społecznej (np. postaw i oczekiwań użytkowników archiwum). Opóźniona reakcja na zmiany może wywołać poważne utrudnienia w realizacji celów archiwum, dlatego system zarządzania jakością dba, aby zmiany możliwie wcześnie rozpoznać, przewidzieć ich wpływ na realizację zadań archiwum, następnie zaplanować, wprowadzić i skontrolować właściwe działania aktualizacyjne.

B. SCHEMAT POSTĘPOWANIA Z OBIEKTAMI CYFROWYMI

Wszelkie zabiegi na obiektach cyfrowych – głównie natury technicznej – odnoszą się do zachowania autentyczności, integralności, wiarygodności oraz dostępności zarówno obiektów, jak i ich metadanych.

6. Zabezpieczenie integralności obiektów cyfrowych. W celu zapewnienia integralności obiektów cyfrowych, rozumianej głównie jako kompletność obiektu cyfrowego, oraz wykluczenie wszelkich niezamierzonych modyfikacji na nim, archiwum podejmuje stosowne działania natury organizacyjnej oraz

technicznej. Odpowiednio wczesna reakcja na przewidywalne zmiany umożliwia rozpoznanie oraz korektę nieprawidłowości.

6.1. Zabezpieczenie integralności obiektów cyfrowych „na wejściu" do archiwum cyfrowego (za OAIS: *Ingest*). Archiwum cyfrowe ustala z twórcami, głównie wydawcami oraz dostawcami, jakimi cechami muszą charakteryzować się obiekty cyfrowe, aby archiwum przejęło odpowiedzialność za dalszą ochronę ich integralności. Archiwum określa również techniczne wymagania dostarczenia publikacji. „Na wejściu" do archiwum obiekt cyfrowy poddawany jest przede wszystkim kontroli na integralność; sprawdzane są także inne parametry jakościowe.

6.2. Zabezpieczenie integralności obiektów cyfrowych w procesie archiwizacji (za OAIS: *Archival Storage*). Archiwum cyfrowe chroni integralność obiektów cyfrowych poprzez rozmaite zabiegi. Przede wszystkim ustala jakość mediów stosowanych do zapisu danych cyfrowych (wybiera nośniki certyfikowane i spełniające określone normy jakościowe).

Archiwum ustala możliwie jednoznaczną politykę dostępu do obiektów cyfrowych przez pracowników archiwum, np. administratora systemu, w celu przeprowadzania prac konserwatorskich.

Archiwum kieruje się zrozumiałymi zasadami określania stopnia fizycznej redundancji. Precyzyjnie określa właściwą lokację archiwizowanych obiektów cyfrowych oraz przynależnych podsystemów.

6.3. Zabezpieczenie integralności obiektów cyfrowych w procesie użytkowania (za OAIS: Access). Archiwum cyfrowe definiuje jasne zasady użytkowania obiektów cyfrowych. Chroni obiekty, ich metadane, także inne elementy systemu przed jakimkolwiek działaniem nieupoważnionych użytkowników. Uprawnionym użytkownikom daje możliwość skontrolowania integralności obiektów cyfrowych.

Archiwum wyznacza granice swojej odpowiedzialności za integralność obiektów w procesie ich udostępniania użytkownikom.

7. Zabezpieczenie autentyczności obiektów cyfrowych. Archiwum cyfrowe musi ochronić autentyczność obiektu cyfrowego, pojmowaną jako możliwość potwierdzenia autorstwa oraz prawdziwości treści w nim zawartych. Obiekt cyfrowy jest autentyczny wówczas, gdy przedstawia dokładnie to, co jego autor zamierzał za jego pośrednictwem przedstawić. Archiwum cyfrowe zabezpiecza autentyczność obiektów cyfrowych na etapie przyjęcia, przechowywania oraz udostępniania. Archiwum starannie dokumentuje przypadki, w których stwierdzono wątpliwość co do autentyczności obiektu oraz takie, w których autentyczność ewidentnie nie potwierdza się.

7.1. Zabezpieczenie autentyczności obiektów cyfrowych „na wejściu" do archiwum. Archiwum elektroniczne wymaga od firm wydawniczych oraz dostawczych, z którymi współpracuje, formalnego potwierdzenia rejestracji swojej działalności (przez autoryzowaną instytucję). „Na wejściu" archiwum cyfrowe wymaga od twórców potwierdzenia autentyczności obiektu, na przykład na podstawie metadanych, dotyczących pochodzenia obiektu. Obiekty autentyczne mogą być oznaczane cyfrową sygnaturą.

7.2. Zabezpieczenie autentyczności obiektów cyfrowych w procesie archiwizacji. Archiwum cyfrowe tworzy pełny wykaz, starannie opisanych przypadków manipulacji, w których wyniku doszło do zmian tudzież usunięcia zarówno samego obiektu, jak i metadanych.

7.3. Zabezpieczenie autentyczności obiektów cyfrowych w procesie użytkowania. Archiwum cyfrowe powinno potwierdzić swoją autentyczność przed

użytkownikami; dysponować i w razie potrzeby oddawać do wglądu dokumenty, z których wynika, że archiwum prowadzi zarejestrowaną, autoryzowaną działalność. Archiwum cyfrowe w procesie udostępniania stosuje sygnatury cyfrowe. Ważne jest udokumentowanie ich pochodzenia i zasad stosowania. W celu możliwości oszacowania przez użytkowników autentyczności obiektów, archiwum udostępnia metadane, w których zawarty jest opis pochodzenia obiektu oraz dokumentacja wszelkich zmian, jakie powstały w wyniku procesu archiwizacji. Użytkownik może również zapoznać się z wykazem obiektów cyfrowych, w przypadku których archiwum ma wątpliwości, bądź nie potwierdza autentyczności.

8. Długoterminowe planowanie technicznych procesów archiwizacji. Archiwum cyfrowe opracowuje długoterminowe plany, w których zawarte są wszelkie obecne oraz przyszłe zadania i terminy ich wykonania. Szczególne znaczenie ma strategiczne planowanie długoterminowe dotyczące zadań natury technicznej (patrz pkt. 4.4), np. zmiana nośników, konwersja do aktualnych formatów, przegląd integralności, autentyczności, kontrola dostępności, odczytu i prezentacji danych. Zadania techniczne odnoszą się zarówno do obiektów cyfrowych, jak i ich metadanych.

9. Określenie procedur gromadzenia obiektów cyfrowych. Archiwum cyfrowe opracowuje procedury dotyczące gromadzenia obiektów cyfrowych. W tym celu ustala zarówno wytyczne selekcji i oceny, jak i dostarczenia obiektów do archiwum. Dopuszcza się zarówno manualny, jak i zautomatyzowany tryb dostarczenia obiektów do archiwum.

9.1. Opracowanie specyfikacji dotyczącej obiektów cyfrowych przekazywanych do archiwum (za OAIS: *Submission Information Packages*, SIPs). Archiwum cyfrowe ustala z twórcami (głównie wydawcami i dostawcami), jakie parametry są konieczne, aby obiekt cyfrowy został przekazany do archiwum. Dzięki tym ustaleniom możliwa jest automatyzacja procesu dostarczania obiektów do archiwum, jak i implementacja tzw. workflowu, sekwencji procedur przyjęcia i wdrożenia obiektu do zasobu archiwalnego. Specyfikacja jest podstawą kontroli jakości obiektów cyfrowych przekazywanych do archiwum.

9.2. Identyfikacja szczególnie znaczących i wartych zachowania cech obiektów cyfrowych. W niektórych przypadkach archiwum cyfrowe podejmuje decyzję o tym, które z cech obiektów cyfrowych zasługują na szczególną ochronę. Czyniąc to powinno się brać pod uwagę własne cele archiwum cyfrowego lub misję, którą musi pełnić, możliwości techniczne oraz ponoszone nakłady, wreszcie potrzeby użytkowników.

Niekiedy w celu zachowania możliwie wielu cech obiektów cyfrowych zachodzi konieczność ochrony jednego obiektu w kilku wariantach.

9.3. Przejęcie technicznej kontroli nad obiektami cyfrowymi. Zdarza się, że do archiwum cyfrowego trafiają obiekty wyposażone w mechanizm ograniczający ich użytkowanie (z racji obostrzeń prawnych lub komercyjnych interesów twórców). Archiwum dba jednak, aby przed włączeniem obiektów do archiwalnych zasobów usunąć wszelkie elementy ich wyposażenia, które mogłyby w jakikolwiek sposób blokować, ograniczać lub utrudniać realizację procesów ich długoterminowej ochrony.

10. Definiowanie i przestrzeganie procedur archiwizacji obiektów cyfrowych. Istota archiwów cyfrowych tkwi w realizacji procesów archiwizacyjnych. Najważniejsze z nich to zdefiniowanie obiektu archiwalnego, jego zapis oraz wykonywanie zabiegów konserwatorskich.

10.1. Definiowanie obiektów archiwalnych (za OAIS: *Archival Information Packages*, AIPs). Na obiekt archiwalny składają się dane reprezentujące zawartość (treść) dokumentu, zapisane w określonym formacie, oraz metadane istotne dla procesów długoterminowej archiwizacji tegoż dokumentu, wpisane w zdefiniowaną strukturę.

Definiowanie obiektów archiwalnych obejmuje identyfikację zastosowanych do obiektów struktur, formatów i dostępnych metadanych (patrz pkt. 12). Skuteczność procesu długoterminowej archiwizacji zależy w dużej mierze od zastosowanych formatów. Archiwa cyfrowe zalecają tzw. uniwersalne otwarte formaty (w skrócie UOF).

10.2. Transformacja gromadzonych obiektów cyfrowych do postaci obiektów archiwalnych. Archiwum cyfrowe przekształca gromadzone obiekty cyfrowe do postaci obiektów archiwalnych oraz dołącza do nich metadane, zawierające informacje istotne dla realizacji procesów długoterminowej archiwizacji tychże obiektów.

10.3. Zabezpieczenie zapisu i odczytu obiektów archiwalnych. Archiwum cyfrowe, z pomocą narzędzi, którymi dysponuje, zapewnia odczyt obiektów archiwalnych, rozumiany jako możliwość odczytu mediów cyfrowych oraz zapisanych w nich kodów zerojedynkowych.

10.4. Stosowanie strategii długoterminowej ochrony obiektów archiwalnych. Z prowadzonych przez archiwum cyfrowe planów działania (patrz pkt. 8) wynika, jakim zabiegom i w jakim czasie powinny zostać poddane obiekty archiwalne. Dla każdego obiektu archiwum wyznacza termin kontroli, w wyniku której podejmowane są decyzje o poddaniu go stosownym zabiegom konserwatorskim.

11. Ustalenie wytycznych użytkowania zasobów archiwalnych. Archiwum cyfrowe udostępnia zasoby archiwalne na podstawie zdefiniowanych zasad użytkowania. Ustalone są zasady przeszukiwania zasobów, dostępu do nich oraz zakres użytkowania.

11.1. Definiowanie obiektów użytkowych (za OAIS: *Dissemination Information Packages*, DIPs). W zależności od zgłaszanych potrzeb użytkowników oraz parametrów obiektów archiwalnych, archiwum cyfrowe definiuje obiekty użytkowe. Wyznacza otoczenie dla procesów wyszukiwania oraz użytkowania obiektów. W zależności od kontekstu użytkowania archiwum może udostępnić obiekt cyfrowy w rozmaitych postaciach użytkowych. Należy jednak mieć świadomość, że użytkowanie obiektu cyfrowego nie oznacza dostępu do chronionego obiektu archiwalnego, lecz do jego kopii lub derywatu, wraz z wszelkimi informacjami potrzebnymi w procesie użytkowania obiektu. Dopuszcza się również wymianę obiektów pomiędzy archiwami. Wówczas konieczna jest transformacja obiektu do standaryzowanego formatu eksportowego.

11.2. Transformacja obiektów archiwalnych do postaci obiektów użytkowych. Obiekty użytkowe powstają, przy zastosowaniu określonych metod, na bazie obiektów archiwalnych. Obiekty te mogą być przechowywane w archiwum i udostępniane w przypadku nowej kwerendy, z uwzględnieniem ewentualnego dostosowania obiektu do nowego kontekstu użytkowania. Mogą również mieć charakter jednorazowy, co oznacza, że za każdym razem, gdy zgłaszane jest zapotrzebowanie na obiekt użytkowy, jest on na bieżąco tworzony z obiektu archiwalnego.

12. Zarządzanie danymi. Oddział zarządzania danymi wspiera wszystkie istotne procesy zachodzące w archiwum cyfrowym, od gromadzenia i przyję-

cia obiektów, poprzez ich archiwizację, do udostępniania. Chroni także ich integralność oraz autentyczność na wszystkich etapach ich przetwarzania i funkcjonowania w archiwum. W realizacji swych zadań oddział zarządzania danymi bazuje na starannie utworzonych i zapisanych metadanych, zawierających:

– dane identyfikacyjne obiektów cyfrowych, stanowiące podstawę zarządzania nimi oraz ich relacjami[12],

– opis formy, treści i struktury obiektów, istotnych z punktu widzenia procesów ich wyszukiwania i użytkowania,

– opis techniczny obiektów, ważny dla zapewnienia możliwości odczytu, prezentacji i interpretacji obiektu, ochrony jego integralności oraz planowania i przeprowadzania zabiegów konserwatorskich,

– dokumentację wszelkich zauważonych zmian w obiektach, konieczną z punktu ochrony autentyczności obiektów,

– ewidencję wszelkich dokumentów o charakterze prawnym (ustaw, zarządzeń, umów, porozumień), których przestrzeganie jest konieczne w toku organizacji i realizacji działalności archiwum.

W zależności od konkretnych potrzeb archiwa mogą stosować rozmaite schematy metadanych. Sensowne jest jednak, z racji ewentualnej współpracy i potrzeby wymiany metadanych z instytucjami partnerskimi, zastosowanie formatu najbardziej rozpowszechnionego. Archiwum ustala reguły wypełniania pól metadanych (np. znormalizowaną terminologią). Możliwe jest również zastosowanie specjalnych narzędzi do automatycznego generowania (ekstrahowania) metadanych.

12.1. Trwałe identyfikowanie obiektów archiwalnych oraz ich relacji. Archiwum cyfrowe stosuje wewnętrzny system identyfikacyjny w celu efektywnego zarządzania obiektami archiwalnymi oraz ich relacjami, także w celu jednoznacznego przyporządkowania danych treściowych do metadanych. Zastosowanie standaryzowanych identyfikatorów trwałych (unikalnych; ang. *Persistent Identifier*) zapewnia autentyczność i niezawodność w procesach bibliograficznych poszukiwań oraz cytowania treści obiektów archiwalnych. Elektroniczne publikacje są sygnowane m.in. następującymi identyfikatorami:

– ISBN (International Standard Book Number) – międzynarodowy standard identyfikacyjny dla monografii,

– ISSN (International Standard Serial Number) – międzynarodowy standard identyfikacyjny dla periodyków,

– URN (Uniform Resource Names) – międzynarodowy internetowy standard identyfikacyjny dla obiektów sieciowych,

– HDL (Handle System) – identyfikator, przypisywany na stałe do obiektów cyfrowych niezależnie od ich fizycznego umiejscowienia i powiązany z danymi ze specjalnej bazy, na podstawie których możliwe jest uzyskanie podstawowych informacji o obiekcie[13],

[12] Pojęcie relacji obiektu archiwalnego (z niem. *Beziehung eines Archivobjekts*) autorzy publikacji opisują jako związek obiektu z innymi elementami do niego przynależnymi, np. kilka części składających się na jedną publikację elektroniczną lub kilka różnych wersji tej samej publikacji. (patrz: *Kriterienkatalog*..., 2006, s. 23).

[13] Więcej informacji na temat systemu HDL znajduje się na stronach WWW: <http://www.cnri.reston.va.us/about_cnri.html>, <http://pl.wikipedia.org/wiki/Handle_System> [dostęp: 12.09.2008].

– DOI (Digital Object Identifier) – identyfikator obiektów cyfrowych, stosowany między innymi w branży wydawniczej do oznaczania elektronicznych wersji publikacji naukowych[14]. Techniczną podstawą dla DOI jest HDL,

– SRef (Scientific Reference linking system) – baza danych przechowująca hiperłącza do publikacji wraz z unikatowymi identyfikatorami publikacji; umożliwia wydawcom stosowanie odsyłaczy, które będą poprawnie funkcjonowały pomimo zmian adresu publikacji, do której prowadzi odsyłacz[15].

12.2. Tworzenie metadanych opisujących treść i formę oraz umożliwiających identyfikację obiektów cyfrowych. Archiwum cyfrowe tworzy metadane, które stosownie do jego potrzeb, opisują treść i formę obiektu oraz umożliwiają jego identyfikację. Zakres, struktura oraz treść metadanych opisowych są zależne od celów archiwum, potrzeb użytkowników oraz od samych obiektów cyfrowych. Formalny i treściowy opis obiektów umożliwia ich wyszukiwanie. Obecnie w instytucjach bibliotecznych oraz archiwalnych stosuje się rozmaite formaty metadanych. W bibliotekach najpopularniejszy jest Dublin Core (DC)[16].

12.3. Tworzenie metadanych opisujących strukturę obiektów cyfrowych. Archiwum cyfrowe tworzy metadane strukturalne, dzięki którym możliwe jest przedstawienie kompleksowej struktury obiektu cyfrowego, a następnie jego zrekonstruowanie i użytkowanie jako całości. Np. zdygitalizowana wersja drukowanej książki składa się m.in. z dwustu pojedynczych plików graficznych; w metadanych strukturalnych zapisuje się ich odpowiednie przyporządkowanie do właściwych miejsc na stronach książki. Podobną rolę pełnią metadane strukturalne w przypadku archiwizacji stron internetowych. Strony WWW składają się zazwyczaj z większej liczby stron HTML oraz plików graficznych (np. w formacie JPEG), powiązanych ze sobą linkami. W metadanych strukturalnych znajduje się dokładny opis tychże powiązań.

12.4. Tworzenie metadanych rejestrujących zmiany w obiektach cyfrowych. Archiwum cyfrowe dokumentuje w metadanych wszelkie zmiany, jakie zachodzą w obiektach cyfrowych, zarówno w wyniku zamierzonych, jak i niepożądanych działań. Dokumentowanie zmian jest zabiegiem koniecznym, raz – dla udowodnienia autentyczności obiektu archiwalnego, dwa – dla realizacji technicznych prac na obiektach. Metadane dokumentujące zmiany pełnią szczególnie istotną rolę w tych archiwach, które zdecydowały się na migrację jako strategię długoterminowej archiwizacji. Migracja wiąże się z regularnymi zmianami obiektów cyfrowych. W tego typu metadanych rejestruje się też zmiany wynikające z procesów transformacji obiektów cyfrowych do postaci obiektów przekazywanych do archiwum, postaci obiektów archiwalnych oraz postaci obiektów użytkowych.

12.5. Tworzenie metadanych opisujących techniczne parametry obiektów cyfrowych. Archiwa cyfrowe sporządzają tzw. metadane techniczne dla obiektów cyfrowych, w których szczegółowo opisują techniczne parametry samych obiektów, jak i wszystkich plików przynależących do poszczególnych obiektów kompleksowych. Dzięki tym metadanym możliwe jest zabezpiecze-

[14] Temat identyfikatorów obiektów cyfrowych jest szerzej omawiany w WWW pod adresem: <http://www.doi.org/index.html> [dostęp: 12.09.2008].

[15] Opis systemu SRef znajduje się w WWW pod adresem: <http://www.sref.org/site/index.php> [dostęp: 12.09.2008].

[16] Temat formatów metadanych, w szczególności DC: (Dublin Core Metadata Element Set, ISO 15836) jest szerzej omówiony w WWW pod adresem: <http://dublincore.org> [dostęp: 12.09.2008].

nie integralności obiektów oraz zarządzanie pracami konserwatorskimi na obiektach.

12.6. Tworzenie metadanych opisujących zasady użytkowania obiektów cyfrowych. Archiwum cyfrowe tworzy metadane obiektów cyfrowych, w których starannie opisuje zasady użytkowania obiektów archiwalnych. Szczególnie pieczołowicie tworzy się takie metadane dla obiektów, których użytkowanie jest z jakichś powodów ograniczone, np. z racji praw autorskich. Metadane „użytkowe" służą zatem powiadomieniu użytkowników o prawach i warunkach użytkowania obiektów cyfrowych, zarządzaniu procesem użytkowania (np. kontrola dostępu do obiektu) oraz zarządzaniu prawami autorskimi do obiektów.

12.7. Przyporządkowanie metadanych do obiektów cyfrowych. Archiwum cyfrowe powinno opracować system jednoznacznego oraz stabilnego wiązania metadanych zarówno z obiektami cyfrowymi w całości, jak i z poszczególnymi częściami, składającymi się na ten obiekt. Archiwa mogą to osiągnąć np. poprzez zastosowanie trwałych identyfikatorów do obiektów cyfrowych oraz ich poszczególnych części, albo poprzez przechowywanie obiektu cyfrowego wraz z przynależącymi do niego częściami i metadanymi w jednej dokładnie zdefiniowanej strukturze (za OAIS: SIP, AIP, DIP) oraz tym samym miejscu (tzw. hermetyzowanie, kapsułowanie).

C. INFRASTRUKTURA I BEZPIECZEŃSTWO

W archiwum cyfrowym istotne znaczenie ma techniczna sprawność oraz bezpieczeństwo systemu. W tym celu archiwum wdraża odpowiednią infrastrukturę z zakresu technologii informacyjnych (IT).

13. Zapewnienie stosownej infrastruktury z zakresu IT. Infrastruktura IT jest konieczna do realizacji zadań związanych z zapewnieniem wszystkim obiektom archiwalnym bezpieczeństwa i stabilności w technicznym znaczeniu. Archiwum implementuje infrastrukturę, dostosowaną do indywidualnych, często bardzo specyficznych, potrzeb.

13.1. Zastosowanie infrastruktury IT w pracach na obiektach cyfrowych. Archiwum cyfrowe implementuje infrastrukturę, umożliwiającą realizację technicznych zadań związanych z ochroną obiektów cyfrowych na wszystkich etapach ich funkcjonowania w archiwum (w procesach przyjęcia, wdrożenia do kolekcji archiwalnej i użytkowania) oraz wspierającą procesy zarządzania danymi.

13.2. Zastosowanie infrastruktury IT w realizacji założeń bezpieczeństwa systemu. Archiwum cyfrowe przy wyborze i implementacji infrastruktury IT uwzględnia wymagania dotyczące bezpieczeństwa całości systemu. Możliwe są np. techniczne zabezpieczenia w postaci haseł albo biometrycznych barier dostępu.

14. Zastosowanie infrastruktury w celu ochrony archiwum cyfrowego i jego kolekcji. W archiwum cyfrowym potrzebna jest infrastruktura chroniąca obiekty archiwalne przed zagrożeniami wewnętrznymi oraz zewnętrznymi. Zagrożenia wewnętrzne, najczęściej wynikają z błędów systemowych i są to na przykład niedomagania sprzętu albo uszkodzenia nośników danych cyfrowych. Natomiast zagrożenia zewnętrzne są utożsamiane przede wszystkim z naturalnymi zagrożeniami, głównie pożarem, powodzią, trzęsieniem ziemi, etc., ale także z niepożądaną działalnością człowieka. Archiwum cyfrowe powinno radzić sobie z odpieraniem zagrożeń obiektów archiwalnych przede

wszystkim, ale chronić także wszelkie zasoby materialne i ludzkie, współtworzące system. Ponadto archiwum cyfrowe preferuje przetrzymywanie kopii bezpieczeństwa kolekcji archiwalnej w miejscu fizycznie oddalonym od głównej siedziby archiwum.

AUDYT WIARYGODNYCH ARCHIWÓW ELEKTRONICZNYCH

Grupa RLG-NARA zaznacza, że samo wyszczególnienie kryteriów audytu i certyfikacji wiarygodnych archiwów cyfrowych to za mało. Pełna użyteczność tych procesów zależeć będzie od narzędzi, które umożliwią wgląd i obiektywną, wewnętrzną oraz zewnętrzną kontrolę procesów zachodzących w archiwum. Standaryzowana, obiektywna metoda kontroli i certyfikacji wiarygodności archiwów cyfrowych jest absolutnie niezbędnym elementem długoterminowej archiwizacji zasobów cyfrowych (*An Audit Checklist...*, 2005, pp. 5-7).

Obecnie narzędziem audytu wiarygodności archiwów cyfrowych są katalogi kryteriów zaproponowane przez grupy RLG-NARA i NESTOR. Ocena wiarygodności archiwum cyfrowego dotychczas powstaje na podstawie kontroli i adnotacji faktu występowania określonego kryterium w następujących fazach: koncepcyjnej, planowania i dokumentacji, implementacji, ewaluacji. Uzupełnieniem obu katalogów kryteriów jest tabela, służąca za narzędzie adnotacji występowania poszczególnych kryteriów archiwum cyfrowego w tych czterech fazach. Dodatkowo tabela została uzupełniona o rubrykę, w której zaznacza się fakt opublikowania dokumentacji z procesu wdrożenia do archiwum określonego kryterium. Jest to zabieg, przyczyniający się do budowania pozytywnego wizerunku i wiarygodności archiwum.

Warto zaznaczyć, że w tabeli występowania kryteriów, poszczególne ich fazy zapisane są w formie czasu przeszłego dokonanego. Zatem adnotacja w tabeli świadczy o przejściu określonego kryterium przez kolejną z pięciu faz (zaprojektowano, zaplanowano i udokumentowano, zaimplementowano, oceniono oraz opublikowano).

PODSUMOWANIE

Zaproponowane katalogi, choć wciąż w wersji roboczej i dyskusyjnej, są niewątpliwie znaczącym uzupełnieniem wiedzy o organizacji i funkcjonowaniu repozytoriów cyfrowych. Dokumenty te przede wszystkim dostarczają systematyzacji dotychczasowych rozpoznań z tego zakresu oraz stanowią punkt zaczepienia dla prac nad procesami oceny i certyfikacji archiwów cyfrowych. Katalogi nie są ani kompletne, ani szczegółowe, charakteryzuje je raczej wysoki poziom abstrakcji wymienionych kryteriów, a to dlatego, że w zamiarze odnoszą się do szerokiego spektrum archiwów cyfrowych. Wykazy szczegółowe i kompletne musiałyby odnosić się do konkretnych archiwów cyfrowych.

Autorzy katalogów podkreślają, że bardzo trudna, a nawet niemożliwa jest absolutna ocena spełnienia przez archiwa cyfrowe powyższych kryteriów. Zakres wdrożenia i spełniania kryteriów jest zależny od indywidualnych założeń poszczególnych archiwów. Proces oceny wiarygodności należy przede wszystkim rozpocząć od rozpoznania celów archiwum oraz przyporządkowa-

nych im zadań i na tej podstawie szacować zasadność i zakres występowania kryteriów.

Ujęte w katalogach kryteria ewaluacji wiarygodności archiwów cyfrowych to początek drogi do międzynarodowego porozumienia w tej kwestii. Kolejny etap prac powinien polegać na ustaleniu jednego wspólnego zestawu kryteriów, w celu poddania go procesom standaryzacji przez odpowiedni komitet standaryzacyjny ISO. Pełny proces standaryzacji może potrwać nawet kilka lat, jednak jest on elementem niezbędnym do ustalenia i obowiązywania międzynarodowych, zunifikowanych procedur kontroli i certyfikacji archiwów cyfrowych.

Obecnie we wszelkich kwestiach związanych z procesami tworzenia oraz rozpoznawania wiarygodnych archiwów cyfrowych pomocne są trzy organizacje, tj.: Center for Research Library (CRL), Digital Curation Center (DCC) oraz Network of Expertise in Long-Term Storage of Digital Resources (NESTOR). Organizacje te współtworzą grupę, formę wirtualnej agencji, na rzecz rozwoju certyfikacji archiwów cyfrowych. Podstawę ich pracy stanowią dotychczasowe ustalenia oraz omówione w artykule katalogi kryteriów (*Trustworthy Repositories*..., 2007, p. 51).

BIBLIOGRAFIA

An Audit Checklist for the Certification of Trusted Digital Repositories. Draft for Public Comment (2005). RLG Mountain View, CA. [online]; [dostęp: 15.09.2008]. Dostępny w World Wide Web: <http://worldcat.org/arcviewer/1/OCC/2007/08/08/0000070511/viewer/file2416.pdf>.

Attributes of a Trusted Digital Repository. Meeting the Needs of Research Resources. An RLG-OCLC Report. Draft for Public Comment (2001). OCLC. Attributes of Trusted Digital Repositoris [online]; [dostęp: 19.08.2009]. Dostępny w World Wide Web: <http://www.worldcat.org/arcviewer/1/OCC/2007/08/08/0000070513/viewer/file2342.pdf>.

Borghoff, Uwe M. (2005). *Vergleich bestehender Archivierungssysteme* [online]. Universität der Bundeswehr München. Fakultät für Informatik. Nestor – Materialien 3 [online]; [dostęp: 21.01.2007]. Dostępny w World Wide Web: <http://www.langzeitarchivierung.de/downloads/mat/nestor_mat_03.pdf>.

Clavel-Merrin, Genevieve (2000). The Nedlib List of Terms. *Nedlib Report Series* 7. Amsterdam: Koninklijke Bibliotheek.

Consultative Committee for Space Data System (1999). *Reference Model for an Open Archival Information System (OAIS). Draft Recommendation for Space Data System Standards.* CCSDS 650.0-R-1. *Red Book.* Newport Beach, Ca. [online]; [dostęp: 20.08.2008]. Dostępny w World Wide Web: <http://ssdoo.gsfc.nasa.gov/nost/wwwclassic/documents/pdf/CCSDS-650.0-B-1.pdf>.

Dobratz, Susanne, Neuroth, Heike (2004). Nestor. Network of Expertise in Long-term Storage of Digital Resources – A Digital Preservation Initiative for Germany [online]. *D-Lib Magazine*, April 2004, vol. 10, no. 4. [dostęp: 20.09.2008]. Dostępny w World Wide Web: <http://www.dlib.org/dlib/april04/dobratz/04dobratz.html>.

Eine kleine Enzyklopädie der digitalen Langzeitarchivierung (2008). Nestor Handbuch [online]; [dostęp: 20.08.2008]. Dostępny w World Wide Web: <http://nestor.sub.uni-goettingen.de/handbuch/nestor-handbuch.pdf>.

Januszko-Szakiel, Aneta (2005). Open Archival Information System – standard w zakresie archiwizacji publikacji elektronicznych. *Przegląd Biblioteczny*, z. 3, s. 342-358.

Konstankiewicz, Marek (2005). Wykaz ważniejszych resortowych aktów prawnych regulujących zasady postępowania z dokumentacją. Uzupełnienie i kontynuacja (część XVIII). *Archiwista Polski*, nr 3 (39).

Konstankiewicz, Marek (2006). Wykaz ważniejszych aktów prawnych regulujących zasady postępowania z dokumentacją. Uzupełnienie i kontynuacja (część XVIII). *Archiwista Polski*, nr 2 (42).

Kriterienkatalog vertrauenswürdige digitale Langzeitarchive (2006). Version 1. Entwurf zur öffentlichen Kommentierung. Nestor Materialien 8. Frankfurt am Main [online]; [dostęp: 20.08.2008]. Dostępny w World Wide Web: <http://edoc.hu-berlin.de/series/nestor-materialien/2006-8/PDF/8.pdf>.

Nestor – Das deutsche Kompetenznetzwerk zur digitalen Langzeitarchivierung (2008). [online];[dostęp: 20.09.2008]. Dostępny w WWW: <http://www.langzeitarchivierung.de/>.

Pest, Czesław (2007). Zastosowanie programu TABULARIUM do kompleksowej obsługi archiwum i biblioteki. *Archiwista Polski*, nr 1(45).

Radwański, Aleksander (2005). Normalizacja informatycznych systemów archiwalnych. W: *Nowe technologie archiwizacji – digitalizacja archiwów i bibliotek. Materiały konferencyjne z VIII seminarium z zakresu składowania i archiwizacji, 19-20 maja 2005.* Wierzba: Dom Pracy Twórczej PAN. Warszawa: Centrum Promocji Informatyki.

Reitz, Joan M. (2004). *Dictionary for Library and Information Science*. Westport; London: Libraries Unlimited.

Sasin, Wiesław Z. (2004). *Przechowywanie i archiwizowanie dokumentacji przedsiębiorstwa według nowych zasad normatywnych. Poradnik dla wszystkich firm z instrukcją wzorcową. Stan prawny na dzień 1 lutego 2004 r.* Skierniewice: Wydaw. „Sigma".

Trusted Digital Repositories. Attributes and Responsibilities. An RLG-OCLC Report (2002). OCLC. Attributes of Trusted Digital Repositories [online]; [dostęp: 19.08. 2009]. Dostępny w World Wide Web: <http://www.oclc.org/programs/ourwork/past/trustedrep/repositories.pdf>.

Trustworthy Repositories Audit & Certification. Criteria and Checklist (2007). Version 1.0. [online]; [dostęp: 30.09.2008]. The Center for Research Libraries. Dostępny w World Wide Web: <http://www.crl.edu/PDF/trac.pdf>.

ANETA JANUSZKO-SZAKIEL
Andrzej Frycz Modrzewski Academy in Cracow
e-mail: ajanuszko-szakiel@afm.edu.pl

CREDIBILITY OF DIGITAL ARCHIVES

KEYWORDS: Digital archives. Digital repositories. Trustworthy digital archives. Certification of digital archives. Audit of digital archives.

ABSTRACT: The author dicusses various meanings of digital archive term and presents types of currently operating digital archives. Attention is drawn to differences between archives of memory-guarding institutions and archives of business or administration sectors, followed by a detailed analysis of digital archive credibility evaluation and a list of credibility features which identify trustworthy services. The article is intended to serve as a documentation of all valid agreements on the organization, operation, audit and certification of trustworthy digital archives. The agreements in question are a result of international cooperation of such institutions as: DCC – Digital Curation Centre, OCLC – Online Computer Library Center, RLG – Research Library Group, NARA – National Archives and Records Administration, NESTOR – Network of Expertise in Long-term Storage of Digital Resources and CRL – U. S. Center for Research Libraries. The agreements are available in English: Trustworthy Repositories Audit & Certification. Criteria and Checklist (TRAC) and German: Kriterienkatalog vertrauenswürdige digitale Langzeitarchive.

Tekst w wersji poprawionej wpłynął do redakcji 29 lipca 2009 r.