Důvěryhodná digitální úložiště, jejich audit a certifikace

Trustworthy digital repositories, their audit and certification

Mgr. Andrea Miranda, Ph.D. / Univerzita Karlova v Praze, Ústřední Knihovna (Charles University in Prague, Central Library), Ovocný trh 560/5, 116 36 Praha 1

Resumé:
Cílem příspěvku je informovat čtenáře o významu a atributech důvěryhodných úložišť a formou přehledu popsat nejznámější přístupy k auditu a certifikaci důvěryhodných digitálních úložišť. Vychází z předchozího výzkumu projektu Cesnet **Pilotní projekt pro low-barrier přístup k ochraně digitálního obsahu (LTP-pilot)** a publikační činnosti autorky, zejména z její dizertační práce Analýza, návrh, administrace a řízení rozsáhlých digitálních knihoven, obhájené v roce 2014 v Ústavu informačních studií a knihovnictví na Univerzitě Karlově v Praze.

Klíčová slova: důvěryhodné digitální úložiště, digitální knihovny, ISO 14721, Data Seal of Approval, Evropský rámec pro audit a certifikaci digitálních repozitářů, Nestor, ČSN ISO 16363, audit a certifikace digitálního repozitáře

Summary:
The aim of the submitted article consists in informing the reader about the importance and the attributes of reliable repositories and in describing, by way of an overview, the most common types of approach to the audit and certification of digital repositories meeting the requirement of trustworthiness. It is based upon the previous research within the Cesnet project, and namely Pilot Project of Low-barrier Approach to the Protection of Digital Contents (LTP-pilot) and the publication activities of the author, in particular her PhD thesis Analysis, draft, administration and control of vast digital libraries, as defended at the Institute of Information Studies and Librarianship of the Charles University in Prague in 2014.

Keywords: trustworthy repository, digital libraries, ISO 14721, Data Seal of Approval, European framework for auditing and certification of digital repositories, Nestor, ČSN ISO 16363, audit a certification of a digital repository

Tento text vznikl v rámci řešení výzkumného projektu Fondu rozvoje CESNET č. 516R1/2014 s názvem „Pilotní projekt pro low-barrier přístup k ochraně digitálního obsahu (LTP-pilot)“.

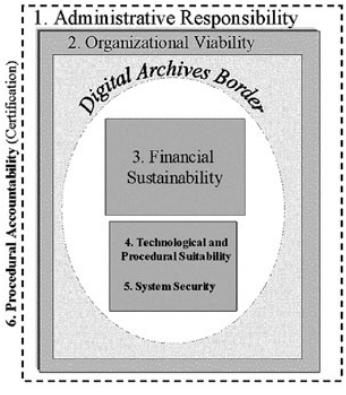
Důvěra uživatelů je jedním z klíčových aspektů úložiště jakéhokoliv typu a obsahu (repozitáře, knihovny či archivu). Nejčastěji ji definujeme jako spolehlivost, víru či předpoklad, že osoba nebo organizace bude dodržovat rámec společných hodnot a představ. Za důvěryhodné digitální úložiště možno označit úložiště, které v souladu s jejich posláním poskytují spolehlivý a dlouhodobý přístup k organizovaným digitálním zdrojům v cílové skupině – dnes i do budoucna. Taková organizace rozumí hrozbám i rizikům správy digitálních informací. Certifikát pak slouží jako „záruka“ pro dané cílové skupiny, jež s důvěrou odevzdávají či využívají data digitálních úložišť. Slouží též i jako objektivní auditní nástroj a výchozí bod pro hodnocení veškerých procesů a činností vztahujících se k digitálním objektům v digitálních knihovnách, repozitářích či archivech.

1 Atributy důvěryhodných repozitářů

Bez ohledu na typ architektury a způsob uchovávání a zpřístupňování musí důvěryhodné repozitáře především[1,2]:

1. zavázat se k trvalé správě/ochraně digitálních objektů pro definovanou komunitu/-y;
2. prokázat organizační způsobilost pro tento úkol (tj. vhodné financování, personální zajištění, vhodné procesy);
3. dostatečně demonstrovat fiskální zodpovědnost a udržitelnost;
4. dostát smluvním a právním požadavkům a splnit povinnosti v této oblasti;
5. mít vypracován účelný a účinný strategický rámec;
6. získávat a zpracovávat digitální objekty podle stanovených kritérií, která odpovídají jeho cílům a schopnostem;
7. udržovat a zajišťovat dlouhodobou integritu, autenticitu a použitelnost spravovaných digitálních objektů;
8. archivovat potřebná metadata o všech akcích, které byly s digitálními objekty v průběhu skladování provedeny; související informace o vzniku, podpoře dostupnosti a využívání objektů před jejich vstupem do repozitáře;
9. splnit potřebná kritéria pro zpřístupňování;
10. mít strategický program pro plánování ochrany;
11. mít odpovídající technickou infrastrukturu, potřebnou k trvalému udržování a zabezpečení spravovaných digitálních objektů

Tato kritéria představují klíčové charakteristiky důvěryhodnosti repozitářů, jež je možné shrnout do šesti základních atributů důvěryhodných repozitářů přehledně ilustrovaných v modelu na obrázku.



Model důvěryhodného digitálního repozitáře[3]

[1] HUTAŘ, Jan. Proč jsou české digitální repozitáře nespolehlivé? Knihovna: knihovnické revue [online]. 2008, roč. 19, č. 1, s. 39–53 [cit. 2015-09-30]. ISSN 1801-3252. Dostupné z: *http://oldknihovna.nkp.cz/knihovna82/82039.htm*.

[2] FOJTŮ, Andrea. Strategie, návrh, řízení a administrace rozsáhlých digitálních knihoven a archivů. [online]. Praha, 2014 [cit. 2015-10-02]. Dostupné z: *https://is.cuni.cz/webapps/zzp/detail/103016/*. Disertační práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví.

[3] HODGES, Patricia a Wendy Pradt LOUGEE. Digital libraries: a vision for the 21st century: a festschrift in honor of Wendy Lougee on the occasion of her departure from the University of Michigan. Ann Arbor, MI: Scholarly Pub. Office, the University of Michigan University Library, c2003, 191 p. ISBN 0-9745109-1-2.

Jakmile je dosaženo konformity úložiště s referenčním modelem OAIS (Open Archival Information System), je splněn základní předpoklad pro důvěryhodný repozitář. Celkově je tak nutné podchytit šest základních atributů důvěryhodných úložišť: administrativní odpovědnost (*Administrative Responsibility*), organizační životaschopnost (*Organizational Viability*), finanční udržitelnost (*Financial Sustainability*), technickou a procedurální vhodnost (*Technological and Procedural Suitability*), systémovou bezpečnost (*System Security*) a procedurální zodpovědnost (*Procedural Accountability Certification*).

1. *Administrativní odpovědnost* odkazuje na dodržování národních a mezinárodních standardů, dodržování rad expertů a využívání praktických zkušeností širší komunity, včetně auditu a certifikace zvolených a zavedených procesů a standardů.
2. *Organizační životaschopnost* zdůrazňuje potřebu prokázání životaschopnosti a důvěryhodnosti. Důležitý je i závazek k dlouhodobému uchovávání v prohlášeních o poslání a odpovídající právní status. Organizační zodpovědností je poskytnutí informací o možných technických problémech a manažerským úkolem je zabezpečit, aby tyto problémy byly vyřešeny dle zavedených procedur a obecně platných standardů.
3. *Finanční udržitelnost* podporuje zavedení a udržení vhodných obchodních praktik a kontrolovatelného obchodního plánu, vyvažování rizik, výhod, investic i výdajů, demonstraci finančního zdraví a trvalý finanční závazek.
4. *Technická a procedurální vhodnost* usiluje o výběr a zavedení nejvhodnější strategie pro dlouhodobou ochranu digitálních dokumentů, zajištění vhodné infrastruktury (hardware, software a zařízení) pro získávání, uchovávání a zpřístupňování.
5. *Systémová bezpečnost* odkazuje na přijaté koncepce a plány postupů v případě nenadálých pohrom nejrůznějšího typu (od finančních potíží až po přírodní katastrofy).
6. *Procedurální zodpovědnost* představuje množství vzájemně souvisejících úkolů a funkcí, přičemž postupy repozitáře jsou dokumentovány a mohou být zpřístupněny na požádání.

2 Evropský rámec pro audit a certifikaci digitálních repozitářů

Evropský rámec pro audit a certifikaci digitálních repozitářů vznikl ze spolupráce představitelů auditních a certifikačních nástrojů – nizozemské certifikační iniciativy Data Seal of Approval, pracovní skupiny Poradního výboru pro kosmické datové systémy (CCSDS – Consultative Committee for Space Data Systems) a pracovní skupiny pro Certifikaci důvěryhodných archivů v rámci Německého ústavu pro průmyslovou normalizaci (DIN - Trustworthy Archives – Certification). Počátkem července 2010 podepsaly tyto skupiny Memorandum o porozumění, čímž daly vzniknout organizaci Trusted Digital Repositories a rámci pro důvěryhodný audit a certifikaci repozitářů. Tento rámec představuje tři úrovně, podle kterých mohou repozitáře postupně zlepšovat svoje poslání, naplňovat roli správce svěřených digitálních dokumentů a zvyšovat tak důvěryhodnost u cílové komunity a producentů dat.

Jedná se o tyto stupně:

- *Základní certifikace*: udělena repozitářům, jež splní podmínky auditu skupiny Data Seal of Approval (dále DSA, *http://datasealofapproval.org/en-gb/*).
- *Rozšířená certifikace*: udělována na základě již existující certifikace DSA a následného interního auditu podle norem ISO 16363 nebo DIN 31644, přičemž o výsledcích tohoto „samo-auditu“ repozitář veřejně informuje.
- *Formální certifikace*: naplněna v případě, kdy kromě základní certifikace získá repozitář i certifikaci na základě kompletního externího auditu podle normy ISO 16363 nebo rovnocenné německé normy DIN 31644.

2.1 Pravidla Data Seal of Approval (DSA)

Pravidla DSA (2. verze, z 19. června 2013)[4], jsou prvním stupněm Evropského rámce pro audit a certifikaci úložišť a nabízí nástroj, který má především manažerům repozitářů a digitálních knihoven poskytnout vhodný výchozí bod pro dlouhodobou ochranu digitálních dokumentů. Tento nepříliš rozsáhlý dokument obsahuje celkem 16 zásad ve třech klíčových kategoriích, jež slouží k ověření kvalitativních aspektů vytváření, uchovávání a využití výzkumných dat společenských a humanitních věd v digitální podobě. Aby repozitář získal pečeť a označení *důvěryhodného repozitáře* (Trusted Digital Repository – TDR) musí vyhovět minimálně zásadám 4 až 13. Pro získání pečetě Data Seal of Approval musí repozitář navíc umožnit producentům a uživatelům dat naplnění v zásadách 1 až 3 a 14 až 16 ve třech základních kategoriích (producenti dat, datový repozitář a příjemci dat).

Kategorie producenti dat (*Data Producers*) – odpovídá za kvalitu dat, kterou přímo ovlivňuje samotná hodnota výstupů vědeckého a akademického výzkumu. Podstatný je i formát, ve kterém jsou data a související informace pro jejich archivaci prezentována. Velmi důležitá je i dokumentace v podobě metadat a dalších kontextuálních informací.

Zásady 1–3:

1. Producent dat vkládá data do digitálního repozitáře společně s informacemi, které ostatním subjektům umožňují zhodnotit kvalitu těchto dat, a také to, nakolik data odpovídají etickým a jiným normám platným pro danou disciplínu.
2. Producent dat odevzdává data ve formátech doporučovaných digitálním repozitářem.
3. Producent dat odevzdává data společně s metadaty vyžadovanými digitálním repozitářem.

Kategorie datový repozitář (*Data Repository*) – odpovídá za řádné uchování a dostupnost dat v dlouhodobém měřítku. Na kvalitu dat působí dva důležité faktory: ***procesy a kvalita prostředí organizace***, do které je repozitář zasazen, ***kvalita technické infrastruktury repozitáře***.

Zásady 4–12:

4. Digitální repozitář má jasně stanovené poslání (*mission*) v oblasti digitální archivace a uplatňuje jej.
5. Digitální repozitář věnuje dostatečnou péči dodržování právních předpisů a smluv, a to včetně těch, které se vztahují k ochraně osob.
6. Digitální repozitář aplikuje organizací schválené procesy a postupy pro správu ukládání dat.
7. Digitální repozitář má plán dlouhodobé ochrany digitálního obsahu v něm uloženého.
8. Archivace probíhá v průběhu celého životního cyklu dat a podle jasně stanovených postupů
9. Digitální repozitář přebírá od producentů dat odpovědnost za zpřístupnění digitálních objektů.
10. Digitální repozitář umožňuje uživatelům najít a použít data a trvale na ně odkazovat.
11. Digitální repozitář zajišťuje integritu digitálních objektů a metadat.
12. Digitální repozitář zajišťuje autenticitu digitálních objektů a metadat.

[4] Zásady DSA jsou dostupné v českém překladu na stránkách Univerzity Karlovy v Praze – *http://dsa.cuni.cz/*. Na jejich překladu se podílela i autorka tohoto článku.

Kategorie příjemci dat (*Data Consumers*) – tato kategorie řeší kvalitní využití dat cílovými skupinami. To ovlivňuje zejména míra, do jaké jsou výstupy z vědy a výzkumu dostupné (co nejsnáze a co nejširší cílové skupině) v rámci stanoveného národního legislativního rámce a politiky přístupů (dostupnost dat podle autorského práva).

Zásady 13–15:

13. Technická infrastruktura zřetelně podporuje úkoly a funkce popsané v mezinárodně uznávaných archivních standardech jako je např. OAIS.
14. Uživatel dat dodržuje přístupová pravidla stanovená digitálním repozitářem.
15. Uživatel souhlasí s pravidly pro sdílení a správné využívání znalostí a informací, která jsou obecně uznávána v dané oblasti, a řídí se jimi.
16. Uživatel respektuje digitálním repozitářem stanovená licenční omezení týkající se užití dat.

Základním principem Data Seal of Approval je interní, vlastní sebehodnocení. Teprve na jeho základě je tento typ interního auditu recenzován Radou Data Seal of Approval. Toto recenzní řízení může trvat až dva či tři měsíce, během kterých hodnotitelé Data Seal of Approval (interní i externí poradci a experti na problematiku dlouhodobé ochrany) sepisují posudek. Všechny Zásady by měly být podpořeny veřejně dostupným prohlášením (URL odkaz na text, nejlépe v anglickém jazyce). Pokud daný dokument není k dispozici v anglickém jazyce, musí být v tomto jazyce dostupné alespoň jeho stručné shrnutí. Je možno odkázat i na rozpracovanou dokumentaci, avšak v takovém případě je potřebné uvést i termín, ve kterém se předpokládá její dokončení.

Samotné Zásady Data Seal of Approval jsou založeny na pěti vůdčích principech:

- Data lze najít na internetu.
- Data jsou zpřístupněna v souladu s relevantní legislativou a s ohledem na ochranu osobních dat a práv duševního vlastnictví.
- Data jsou dostupná ve využitelném formátu.
- Data jsou spolehlivá.
- Na data lze odkazovat.

Hodnotí se i stupeň shody[5] dokumentace vůči stanoveným Zásadám:

- stupeň 0 – N/A: není aplikovatelné.
- stupeň 1 – Ne: ještě jsme nad tím neuvažovali.
- stupeň 2 – Teoreticky: máme teoretický návrh.
- stupeň 3 – Rozpracováno: jsme v implementační fázi.
- stupeň 4 – Implementováno: tuto zásadu jsme plně implementovali pro potřeby našeho repozitáře.

2.2 DIN 31644, Nestor

Další certifikace z Evropského rámce pro audit a certifikaci digitálních repozitářů – DIN 31644[6] – pochází z německy mluvícího prostředí; rozsahem a účelem je možné ji zařadit na vyšší stupeň než Data Seal of Approval.

[5] Jedná se vždy o stupeň 3 nebo 4. Není nutné, aby všechny zásady zajišťoval přímo daný konkrétní digitální repozitář; může je outsourcovat.

[6] DIN 31644:2012-04. *Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive* [online]. Berlin: Beuth Verlag, 2012 [cit. 2013-05-30]. Dostupné také z: *http://www.beuth.de/de/norm/din-31644/147058907*.

DIN 31644 Information und Dokumentation – Kriterien für vertrauenswürdige digitale Langzeitarchive reprezentuje standardní rámec umožňující vyhodnocování **důvěryhodnosti digitálního úložiště z organizačního** i technického hlediska. Slouží též jako návod pro návrh, plánování a implementaci digitálního repozitáře. Původní zaměření standardu na instituce typu archivů, muzeí a knihoven bylo rozšířeno na všechny organizace, jejichž cílem je uchovávání informací v digitální podobě. Hlavní část normy se skládá z 34 kritérií strukturovaných do 3 částí: 1. organizace, 2. správa duševního vlastnictví a jejich reprezentace, a dále pak 3. infrastruktura a bezpečnost.

Norma vychází z katalogu Nestor – N*etwork of Expertise in Long-Term Storage and Long-Term availability of Digital Resources in Germany,* který představuje soupis 14 kritérií s podrobným vysvětlením a konkrétními příklady. Klíčovým konceptem kritérií Nestor pro dlouhodobé uchovávání a dlouhodobé zpřístupňování je důvěryhodnost repozitáře (*Vertrauenswürdigkeit des Langzeitarchivs*).

Hodnocení repozitářů je možné rozdělit do tří hlavních okruhů[7]:

A. *organizační rámec* – digitální repozitář působí v určitém organizačním rámci, který stanovuje jeho cíle, právní podmínky, personální a finanční zabezpečení.
B. *správa objektů* – repozitář analyzuje stanovené cíle a strategie, na základě kterých specifikuje veškeré nutné požadavky a aktivity dlouhodobé archivace v rámci celého životního cyklu digitálních objektů. Tento cyklus odpovídá hlavním fázím funkčních entit Příjem, Permanentní úložiště a Přístup (referenční model OAIS). Při práci s objekty je nutné dodržet[8]:
    - integritu a autenticitu získaných informací, resp. digitálních objektů (ty totiž představují klíčový aspekt důvěryhodnosti),
    - dlouhodobé plánování technických ochranných opatření pro trvalé uchování informací, resp. digitálních objektů,
    - standardy přenosu, archivace a využívání digitálních informací, resp. objektů,
    - správu dat, pomocí které je možné dostat z digitálních objektů užitečné infor mace pro stanovenou cílovou komunitu.
C. *infrastruktura a zabezpečení* – představují souhrn technických a bezpečnostních otázek, včetně komunikačních a síťových služeb, hardware a programového vybavení (software). Chrání tak digitální objekty před systémovými a vnějšími hrozbami.

Hodnocení kritérií ve výše stanovených okruzích vychází ze čtyř základních principů:

– **Dokumentace – cí**le, koncepce a specifikace a postupy implementace digitálního repozitáře jsou řádně zdokumentovány. Na základě náležité dokumentace je možné posoudit architekturu, design, finanční zabezpečení a organizační rámec podle odpovídajících standardů kvality a bezpečnosti.

[7] NESTOR. nestor - Materialien 8: nestor-Kriterien, Kriterienkatalog vertrauenswürdige digitale Langzeitarchive, Version 2 [online]. Frankfurt am Main: nestor c/o Deutsche Nationalbibliothek, 2008 [cit. 2015-09-30]. urn:nbn:de:0008-2008021802. Dostupné z: *http://edoc.hu-berlin.de/series/nestor-materialien/8/PDF/8.pdf*.

[8] FRUCHT, B., et al. nestor Kriterien Katalog vertrauenswürdige digitale Langzeitarchive [online]. cca2009 [cit. 2013-05-30]. Dostupné z: *http://www.wirtschaftsarchive.de/arbeitskreise/fachliche-arbeitskreise/elektronische-archivierung/NestorKriterienkatalog2.pdf.*

- **Transparentnost** – dosažena zveřejňováním relevantních částí dokumentace pro koncové uživatele a další zainteresované strany. Partneři (např. producenti dat) tak mají přehled o tom, komu a za jakých podmínek poskytují svá data. Právě dodržováním pravidla transparentnosti si repozitář buduje důvěryhodnost, neboť tak umožňuje okamžité vyhodnocení kvality digitálního repozitáře **zúčastněnými stranami.**
- **Adekvátnost** – hodnocení musí proběhnout ve vhodném kontextu v souladu s cíli a posláním (mission statement) repozitáře, jelikož absolutní standard neexistuje. Veškerá kritéria je proto nutné vnímat v kontextu daného repozitáře. V závislosti na cílech a úkolech digitálního repozitáře se míra a relevance těchto kritérií může u různých repozitářů **výrazně lišit.**
- **Měřitelnost** – dlouhodobá ochrana digitálních materiálů není vždy jednoznačně měřitelnou záležitostí, přesto je možné nalézt jisté indikátory, které ukazují na stupeň důvěryhodnosti repozitáře. Díky transparentnosti dokumentace je pak naplnění těchto indikátorů, resp. kritérií, snáze vyhodnotitelné.

2.3 Standard ISO 16363

Standard **ČSN ISO 16363 (319621) Systémy pro přenos dat a informací z kosmického prostoru** – *Audit a certifikace důvěryhodných digitálních úložišť* stanovuje doporučený postup pro posuzování důvěryhodnosti digitálních úložišť. Hlavním účelem tohoto standardu je stanovit doporučený postup proces auditu (včetně interního) a certifikace sloužící k posouzení důvěryhodnosti digitálních úložišť. Důvěra je zde hodnocena z pohledu referenčního modelu OAIS[9], který tvoří výchozí podklad kritérií standardu ISO 16363. Norma naopak neslouží k definici konkrétních technologií, softwarového či hardwarového zabezpečení. Převládá mylný názor, že většina metrik v normě souvisí s technologiemi, i když například první kategorie kritérií se zabývá zejména riziky spojenými s organizací, která úložiště vlastní či spravuje.

Vzhledem ke své organizační, časové a taktéž finanční náročnosti má standard své opodstatnění zejména pro větší až velké digitální knihovny, repozitáře či archivy[10]. Jako auditní nástroj slouží pro vyhodnocení spolehlivosti, zavázanosti a připravenosti institucí převzít na sebe zodpovědnost za dlouhodobé uchovávání obsahu. Je určen pro ty, kteří pracují pro/jsou zodpovědní za digitální repozitáře, knihovny nebo archivy a hledají objektivní prostředek pro vyhodnocení důvěryhodnosti jejich úložiště. Norma obsahuje celkem 108 kritérií (normativních metrik), rozdělených do tří základních kategorií[11]:

---

9 *Systémy pro přenos dat a informací z kosmického prostoru - Otevřený archivační informační systém - Referenční model: Space data and information transfer systems - Open archival information system (OAIS) - Reference model = Systèmes de transfert des informations et données spatiales - Système ouvert d'archivage d'information (SOAI) - Modèle de référence : ČSN ISO 14721 : schváleno v* červnu *2012 ve Washingtonu, DC, USA*. 2. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014, 97 s.

10 Pojem Velké digitální knihovny významově odkazuje na anglický pojem Very Large Digital Libraries (VLDL). Do této kategorie lze zařadit krajské až národní knihovny.

11 *Systémy pro přenos dat a informací z kosmického prostoru - Audit a certifikace důvěryhodných digitálních* úložišť*: Space data and information transfer systems - Audit and certification of trustworthy digital repositories = Systèmes de transfert des informations et données spatiales - Audit et certification des référentiels numériques de confiance : ČSN ISO 16363 : schváleno v září 2011 ve Washingtonu, DC, USA*. 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014, 53 s.

A. Organizační infrastruktura (Organizational Infrastructure)
   1. Řízení a životaschopnost organizace.
   2. Organizační struktura a personální zabezpečení.
   3. Procedurální zodpovědnost a strategický rámec.
   4. Finanční udržitelnost.
   5. Smlouvy, licence a závazky.

B. Správa digitálních objektů (Digital Object Management)
   1. Ingest: akvizice obsahu.
   2. Ingest: tvorba archivních balíčků.
   3. Plánování dlouhodobé ochrany.
   4. Archivní úložiště & ochrana/správa AIP balíčků.
   5. Informační management.
   6. Správa přístupu.

C. Technologie, technická infrastruktura a bezpečnost (Technologies, Technical Infrastructure, & Security)
   1. Systémová infrastruktura.
   2. Vhodné technologie.
   3. Bezpečnost.

Je nutné si uvědomit, že úložiště jako organizační celek se dotýká pracovníků na nejrůznějších úrovních. Vedení a nižší management musí znát alespoň požadavky na důvěryhodné úložiště z části A (Organizační struktura). Systémoví administrátoři, síťoví správci a další techničtí pracovníci, kteří zodpovídají za mnohé části infrastruktury, budou pracovat s částí C (technologie, technická infrastruktura a bezpečnost). Producenti a příjemci dat naleznou relevantní informace především v dokumentaci pro část A a B.

Závěr

Důvěra digitálních úložišť není dána pouhým technologickým (softwarovým nebo hardwarovým) zabezpečením. Bezproblémové fungování digitálních úložišť totiž ovlivňuje nejen technická a procedurální vhodnost, ale i finanční udržitelnost a systémová bezpečnost. Na digitální repozitář jako organizaci působí administrativní odpovědnost, kdy se instituce zavazuje k vytvoření důvěryhodného repozitáře.

K prokázání plné kontroly nad veškerými postupy, aktivitami a procesy digitálních úložišť slouží auditní a certifikační nástroje, z nichž nejvyužívanější jsou ty, které jsou součástí Evropského rámce pro audit a certifikaci digitálních repozitářů. Pro menší úložiště je určen zejména Data Seal of Approval. Pro větší až velké digitální knihovny, repozitáře a archivy je určen audit a certifikace podle ČSN ISO 16363. DIN 31644 je vhodný především pro německou cílovou skupinu; jako další zdroj k auditu a certifikaci poslouží i pro české a slovenské digitální úložiště.

Použitá literatura:

DIN 31644:2012-04. *Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive* [online]. Berlin: Beuth Verlag, 2012 [cit. 2013-05-30].
Dostupné také z: *http://www.beuth.de/de/norm/din-31644/147058907*.

FOJTŮ, Andrea. *Strategie, návrh, řízení a administrace rozsáhlých digitálních knihoven a archivů*. [online]. Praha, 2014 [cit. 2015-10-02]. Dostupné z: *https://is.cuni.cz/webapps/zzp/detail/103016/*. Disertační práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví.

FRUCHT, B., et al. nestor Kriterien Katalog vertrauenswürdige digitale Langzeitarchive [online]. cca2009 [cit. 2013-05-30]. Dostupné z: *http://www.wirtschaftsarchive.de/arbeitskreise/fachliche-arbeitskreise/elektronische-archivierung/NestorKriterienkatalog2.pdf*.

HODGES, Patricia a Wendy Pradt LOUGEE. *Digital libraries: a vision for the 21st century: a festschrift in honor of Wendy Lougee on the occasion of her departure from the University of Michigan*. Ann Arbor, MI: Scholarly Pub. Office, the University of Michigan University Library, c2003, 191 p. ISBN 0974510912.

HUTAŘ, Jan. Proč jsou české digitální repozitáře nespolehlivé? *Knihovna*: knihovnické revue [online]. 2008, roč. 19, č. 1, s. 39–53 [cit. 2015-09-30]. ISSN 1801-3252.
Dostupné z: *http://oldknihovna.nkp.cz/knihovna82/82039.htm*.

NESTOR. nestor - Materialien 8: nestor-Kriterien, Kriterienkatalog vertrauenswürdige digitale Langzeitarchive, Version 2 [online]. Frankfurt am Main: nestor c/o Deutsche Nationalbibliothek, 2008 [cit. 2015-09-30]. urn:nbn:de:0008-2008021802.
Dostupné z: *http://edoc.hu-berlin.de/series/nestor-materialien/8/PDF/8.pdf*.

Systémy pro přenos dat a informací z kosmického prostoru - Otevřený archivační informační systém - Referenční model: Space data and information transfer systems - Open archival information system (OAIS) - Reference model = Systèmes de transfert des informations et données spatiales - Système ouvert d'archivage d'information (SOAI) - Modèle de référence : ČSN ISO 14721 : schváleno v červnu 2012 ve Washingtonu, DC, USA. 2. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014, 97 s.

Systémy pro přenos dat a informací z kosmického prostoru - Audit a certifikace důvěryhodných digitálních úložišť: Space data and information transfer systems - Audit and certification of trustworthy digital repositories = Systèmes de transfert des informations et données spatiales - Audit et certification des référentiels numériques de confiance : ČSN ISO 16363 : schváleno v září 2011 ve Washingtonu, DC, USA. 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014, 53 s.