Pavlásková, Eliška

Techniky posuzování rizik a jejich využití v institucionálních repozitářích – užití v Digitálním repozitáři Univerzity Karlovy v Praze

ProInflow. 2014, vol. 6, iss. 1, pp. 26-37

ISSN 1804-2406

Stable URL (handle): https://hdl.handle.net/11222.digilib/133803
Access Date: 28. 11. 2024
Version: 20220831

Techniky posuzování rizik a jejich využití v institucionálních repozitářích – užití v Digitálním repozitáři Univerzity Karlovy v Praze

Risk Assessment Techniques and Their Application in Institutional Repositories – Use in the Digital Repository of Charles University in Prague

Eliška Pavlásková

Digitální univerzitní repozitář, Univerzita Karlova v Praze
Ústav informačních studií a knihovnictví, Filozofická fakulta, Univerzita Karlova v Praze

Recenzenti:
PhDr. Ladislav Cubr
Mgr. Beáta Bellérová, Phd.

Abstrakt:
Institucionální repozitář tvoří komplexní systém skládající se z hardwaru, softwaru, lidského faktoru a vztahů jak vůči instituci samotné, tak obecně k okolí systému. Pokud chce být repozitář považován za důvěryhodný, je třeba, aby si byl vědom rizik hrozících digitálním objektům v něm uloženým. Proces posouzení rizik je určen k tomu, aby administrátorům pomohl odhalit, popsat a zhodnotit rizikové oblasti a konkrétní rizika ohrožující dlouhodobé uložení digitálních objektů.
Obecná metodika posuzování rizik je popsána v rodině norem ISO 31000. Přímo pro využití v institucionálních repozitář bylo vyvinuto několik nástrojů – například SPOT nebo DRAMBORA. Článek kromě teoretického shrnutí problematiky uvádí i praktický příklad použití těchto nástrojů v Digitálním univerzitním repozitáři Univerzity Karlovy v Praze.

Klíčová slova: *digitální repozitáře, institucionální repozitáře, řízení rizik, dlouhodobá ochrana digitálních objektů*

Abstract:
An institutional repository is a complex system of hardware and software technologies, human input and interaction with institutional as well as general system environment. If the repository is to be considered trustworthy risks of the preservation of stored digital objects should be taken into consideration. The digital preservation risk assessment process helps repository administrators to identify, describe and evaluate risk domains and specific risks. The generic guideline for the risk management implementation is codified in the standard ISO 31000. There are several

tools designated for the self-assessment of the institutional repository – for example SPOT or DRAMBORA. The article consist of theoretical summary of the issues and provides a practical example of the use of these tools in the Digital University Repository of Charles University in Prague.

Keywords: *digital repositories, institucional repositories, risk management, long term digital preservation*

Úvod

Ochrana digitálního kulturního dědictví (ať už v digitální podobě vznikajícího nebo digitalizovaného) je úzce svázána s bezproblémovým provozem informačních systémů, které toto dědictví ukládají, spravují a dále šíří. Bohužel tento požadavek je v praxi téměř nesplnitelný. Jakýkoli systém je ohrožován celou řadou rizik od těch ryze technických, mezi které patří například selhání zálohovacího zařízení, přes možnost lidské chyby až po zásahy „vyšší moci" (například ve formě povodní) nebo dokonce cílenou sabotáž. Některým z těchto ohrožení lze předcházet a jiné je možno zmírnit, předpokladem však je prevence a pečlivá příprava na rizikovou situaci.
Metodika zaměřená na prevenci potenciálních rizikových situací a na přípravu jejich řešení je obvykle prezentována pod souhrnným názvem řízení (management) rizik a zasahuje do celé řady oblastí lidské činnosti. Pro oblast dlouhodobé ochrany digitálních objektů je klíčový zejména management rizik zaměřený na informační technologie a dále samozřejmě i skupina metodik vyvinutých přímo pro tuto oblast a v rámci institucí, které mají rozsáhlé zkušenosti se správou digitálních objektů.
Jakýkoli systém určený pro dlouhodobou archivaci digitálních objektů (tedy i institucionální repozitář) by měl z hlediska dlouhodobé ochrany digitálních objektů dle Barateira[1] splňovat čtyři základní požadavky:

- Spolehlivost – systém by měl být schopen archivovat digitální objekty po celou dobu své existence.
- Zachování autenticity – musí být možné zjistit, že uchovávaný objekt je skutečně autentický. Měla by být dostupná informace o jeho provenienci a zároveň i zajištěna jeho integrita.
- Ochrana proti zastarávání – informace musí být možno zobrazit či využít i v novém technologickém kontextu.
- Škálovatelnost – systém se musí být schopen vyrovnat s nárůstem uchovávaných dat a se změnou technologických nástrojů využívaných při archivaci.

Metodika řízení a analýzy rizik by měla směřovat k maximálnímu možnému zajištění plnění těchto požadavků.
Cílem této práce je poskytnout teoretický úvod do problematiky řízení rizik v rámci institucionálního repozitáře a zhodnotit zkušenosti z praktické aplikace těchto poznatků v rámci Digitálního univerzitního repozitáře Univerzity Karlovy v Praze.

Metodika řízení rizik

Relevantní normy

Obecně je metodika pro implementaci řízení rizik podchycena ve skupině norem ISO 31000. Jedná se o rodinu norem, která sestává z následujících dokumentů:

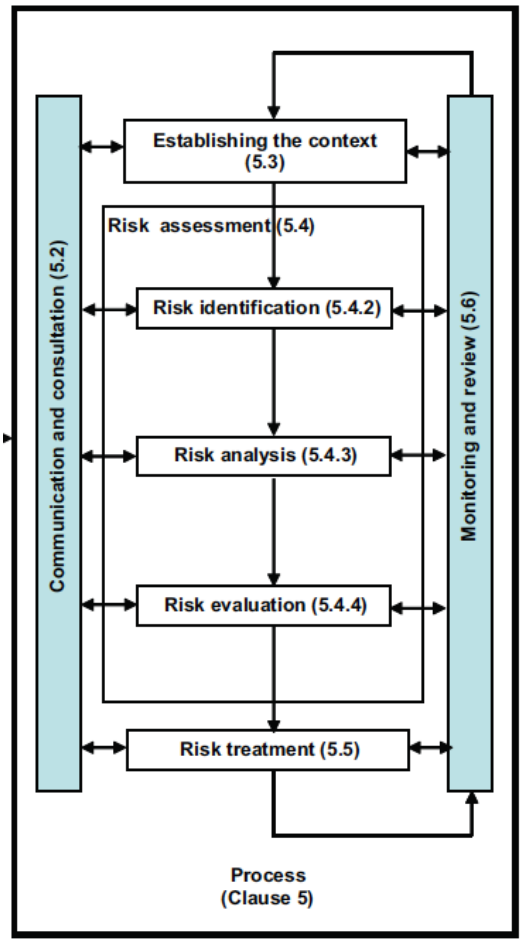
- ISO 31000:2009 – Principles and Guidelines on Implementation
- ISO/IEC 31010:2009 – Risk Management – Risk Assessment Techniques
- ISO Guide 73:2009 – Risk Management – Vocabulary

[1] BARATEIRO, José, Gonçalo ANTUNES, Filipe FREITAS a José BORBINHA. Designing Digital Preservation Solutions: A Risk Management-Based Approach. *International Journal of Digital Curation* [online]. 2010-07-21, vol. 5, issue 1, s. 4-17 [cit. 2014-05-02]. DOI: 10.2218/ijdc.v5i1.140. Dostupné z: http://ijdc.net/index.php/ijdc/article/view/143

Standard je určen k tomu, aby harmonizoval normy používané v jednotlivých specifických oblastech. Jeho cílem ovšem není nahradit existující standardy. Shrnuje hlavní požadavky na organizaci implementující politiku řízení rizik, kodifikuje terminologii a stanoví základní body procesu posouzení rizik.
Mezi pojmy, které definuje norma ISO 31000:2009,[2] patří zejména:
Riziko (Risk) – dopad nejistoty na cíle organizace.
Řízení rizik (Risk management) – koordinované aktivity řídící a kontrolující organizaci s ohledem na riziko.
Posouzení rizik (Risk assessment) – celkový proces identifikace rizik, analýzy rizik a hodnocení rizik.
Identifikace rizik (Risk identification) – proces nalezení, rozpoznání a popsání rizika.
Analýza rizik (Risk analysis) – proces zaměřený na porozumění riziku a určení úrovně rizika.
Hodnocení rizika (Risk evaluation) – proces porovnání výsledků analýzy rizik s kritérii rizika. Cílem je zjistit, zda je riziko a/nebo jeho závažnost akceptovatelné nebo tolerovatelné.
Zvládnutí rizik (Risk treatement) – proces modifikace rizika.

Proces řízení rizik

Jak již bylo výše zmíněno, proces posouzení rizik se skládá z několika fází, které jsou doplněny průběžným monitoringem a revizemi rizik společně s komunikací a konzultacemi. Tento proces popisuje obrázek č. 1.



Obr. 1 Risk management[3]

[2] ISO 31000:2009. *Risk management: Principles and guidelines*. 2009.
[3] ISO 31000:2009. *Risk management: Principles and guidelines*. 2009.

Fází první je zmapování kontextu repozitáře. Po něm následuje samotné posouzení rizik, které reprezentují tři fáze – identifikace, analýza a hodnocení. V závěru nastupuje fáze zvládání rizik.
V průběhu posuzování rizik by měl auditor úzce spolupracovat s danou institucí. V případě repozitářů se jedná zejména o časté konzultace s týmem spravující repozitáře, a s osobami odpovědnými za provoz a zabezpečení hardwarového vybavení.
Monitoring řízení rizik by měl být plánovanou a periodickou činností. Mělo by být jasné, kdo je za monitoring a revize strategie zvládání rizik odpovědný a kontrolní proces by měl být založen na měřitelných údajích.

Popis kontextu repozitáře

Stanovení kontextu organizace (v tomto případě institucionálního repozitáře) je důležitým krokem předcházejícím samotnému posouzení rizik. Je třeba zhodnotit jak interní tak externí kontext repozitáře. Za externí kontext se považuje zejména právní rámec organizace, kulturní kontext repozitáře, obecné trendy mající dopad na repozitář a vztah repozitáře k dalším institucím.
Interní kontext zahrnuje (dle ISO 31000):

- Správu samotné organizace, její interní strukturu a role zaměstnanců.
- Organizační politiku, cíle a již stanovené strategie – pro institucionální repozitář je zde klíčová zejména znalost existujících politik dlouhodobé ochrany, a to jak formálních, tak neformálních.
- Finanční, lidské, časové a technologické zdroje, a to včetně shromážděných znalostí.
- Existující informační systémy, informační toky a rozhodovací procesy (formální i neformální).
- Postoj zainteresovaných osob (stakeholders) vůči repozitáři – jejich hodnoty a chápání významu repozitáře. Z hlediska institucionálního repozitáře je zde významná i míra informovanosti managementu o povaze a významu repozitáře a o problematice dlouhodobé ochrany.
- Kulturu organizace.
- Standardy, doporučení a modely uznávané organizací – specifický pro oblast digitálních repozitářů je například referenční model OAIS[4] nebo zásady Data Seal of Approval[5].
- Smluvní závazky.

V této fázi je auditorům (jak interním tak externím) doporučováno, aby shromáždili maximální dostupné množství dokumentace. Jedná se jak o psanou dokumentaci, tak o intenzivní komunikaci se zaměstnanci repozitáře. Vhodné je shromáždit dokumenty popisující legislativní rámec provozu repozitáře. Nedostupnost klíčových informací může být identifikována jako riziko a zpracována v dalších fázích procesu.

Identifikace rizik

Tato fáze je první z trojice tvořící jádro celého procesu posouzení rizik. Cílem identifikace rizik je zejména vytvoření seznamu událostí, které mohou nějakým způsobem ohrozit dosažení cílů organizace. V případě digitálního institucionálního repozitáře se tedy jedná

[4] Consultative Committee for Space Data Systems. *Reference Model for an Open Archival Information System (OAIS)* [online]. Washington (D.C.) : CCSDS, January 2002 [cit. 2009-09-24]. [1, xiii, 139 s.]. Recommendation for Space Data System Standards, CCSDS 650.0-B-1. Blue Book, Issue 1. Dostupný z WWW: <http://public.ccsds.org/publications/archive/650x0b1.pdf>
[5] DATA SEAL OF APPROVAL BOARD. *Data Seal of Approval: Guidelines version 2*. [online]. 2013 [cit. 2014-05-05]. Dostupné z: http://www.datasealofapproval.org/media/filer_public/2013/09/27/guidelines_2014-2015.pdf

zejména o rizika, která nějakým způsobem znesnadňují možnost využití digitálních objektů nebo přímo ohrožují jejich existenci. Tento seznam je základem pro hlubší analýzu a je tedy nezbytně nutné, aby obsahoval pokud možno všechna rizika, a to včetně těch, jejichž zdroj není zřejmý nebo není pod kontrolou organizace.
V rámci nástrojů pro řízení rizik v oblasti dlouhodobé ochrany digitálních objektů jsou často dostupné i seznamy rizik nebo rizikových oblastí, na které by se auditor při identifikaci měl zaměřit. Jakkoli se nedoporučuje soustředit se při analýze pouze na tato předdefinovaná rizika, jedná se o cennou možnost, jak využít zkušeností dalších institucí a zároveň se i vyvarovat přehlédnutí možné zásadní skupiny rizik.

Analýza rizik

Auditor vychází ze seznamu identifikovaných rizik a podrobuje je detailní analýze. Je třeba prozkoumat zdroj nebo případné příčiny rizika, porozumět jeho vlastnostem a nastínit i možnosti jeho řešení. Jsou stanovena kritéria, která jsou podkladem pro zhodnocení. Stanovena je i úroveň závažnosti rizika, jeho dopadů na organizaci a pravděpodobnost, že se objeví. Neméně důležité je i pochopit možný vztah k ostatním rizikům. V některých případech je možné, že jedno riziko se stává příčinou dalšího nebo zvyšuje závažnost jeho dopadu. Dochází však i k tomu, že se dvě rizika vzájemně vylučují.

Hodnocení rizik

Produktem fáze hodnocení rizik by měl být samotný podklad pro rozhodování o strategii zvládání rizik. Zde by měla být zhodnocena úroveň závažnosti rizika vzhledem ke kontextu. Může být například rozhodnuto, že objekt v nestandardním formátu sice představuje z hlediska dlouhodobé dostupnosti velké riziko, ale jeho význam převažuje toto riziko, a proto bude i nadále uchováván.

Zvládnutí rizik

Proces zvládání rizik spočívá v přijetí opatření, která riziko nebo jeho dopad zmírňují. V některých případech může být přistoupeno i k opatřením, která zajistí, že se organizace danému riziku zcela vyhne. Mělo by se jednat o cyklický proces založený na průběžném hodnocení úspěšnosti přijatých opatření. Je důležité brát v potaz i to, že některé ze způsobů zvládání rizik mohou produkovat další rizika. Samotný výběr opatření by měl být založen na více faktorech, a to včetně finanční i obecné náročnosti vzhledem k přínosům daného opatření.
Cílem tohoto procesu je vytvořit plán (strategii) zvládání rizik, který by měl obsahovat zejména tyto informace:

- Způsob výběru vhodných opatření – včetně očekávaných přínosů
- Osoby zodpovědné za schválení a provedení plánu
- Navrhovaná opatření
- Požadované prostředky
- Ukazatele úspěšnosti
- Požadavky na monitoring
- Časový harmonogram

Dostupné nástroje

V rámci komunity zabývající se dlouhodobou ochranou digitálních objektů bylo vyvinuto několik nástrojů či metodik, které usnadňují proces řízení rizik a poskytují správcům

institucionálních repozitářů (i dalších typů digitálních archivů) vedení v procesu posuzování rizik. Jednotlivé nástroje se liší jak co do míry náročnosti hodnotícího procesu, tak z hlediska účelu.
Pro oblast institucionálních repozitářů jsou klíčové zejména nástroje SPOT[6] a DRAMBORA[7], které jsou dále detailněji popisovány.

SPOT

Pravděpodobně nejjednodušším nástrojem pro mapování rizik v oblasti dlouhodobé ochrany digitálních objektů je model SPOT (Simple Property-Oriented Threat). Tento model vymezuje šest základních oblastí, na které je třeba se při práci s digitálními objekty soustředit. V každé z těchto oblastí jsou obecně vymezeny hlavní hrozby, které objekt ohrožují. Tento rámec umožňuje repozitáři poměrně rychle a bez větších personálních a finančních nároků identifikovat rizika.
Základní oblasti definované modelem SPOT jsou:

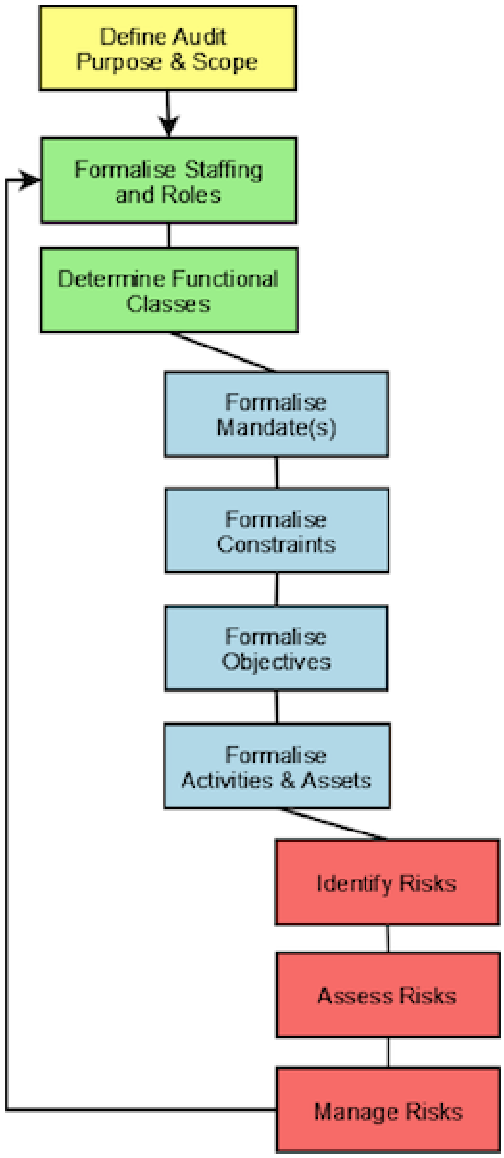
- *Dostupnost (Availability)* – ve významu dostupnosti digitálního objektu po dlouhou dobu. Hlavní hrozby v této oblasti se soustředí na péči o objekt před jeho zařazením do repozitáře, na politiku výběru objektů a na oblast autorských práv k objektu.
- *Identita (Identity)* – objekt je možné identifikovat a odlišit od ostatních, jeho obsah je optimálním způsobem popsán. Hlavní hrozby v této oblasti se soustředí opět na zpracování objektu před jeho vložením do repozitáře a na práci s popisnými a strukturálními metadaty.
- *Trvalost (Persistence)* – bitové sekvence tvořící digitální objekt by měly být uchovávány v použitelné a zpracovatelné podobě. V této oblasti se hlavní hrozby zaměřují na oblast správy fyzických médií, politiky migrace hardwaru a politiky ochrany uložených dat.
- *Reprodukovatelnost (Renderability)* – je zachována možnost interpretace (za použití vhodného hardwarového a softwarového vybavení) bit-streamu způsobem srozumitelným jak pro člověka, tak pro stroje. Objekt by si měl uchovat své signifikantní vlastnosti – tedy ty vlastnosti, které byly určeny jako zásadní pro uživatele. Hrozby se v této oblasti soustředí na správu formátů, strategie dlouhodobé ochrany a obecně na pochopení potřeb cílové komunity.
- *Srozumitelnost (Understandability)* – repozitář by měl uchovávat optimální množství informací potřebné k tomu, aby uživatelé byli schopni pochopit digitální objekt. Klíčová je v tomto ohledu zejména tvorba a uchování dostatečného množství vhodně zvolených metadat. Hlavní hrozby se soustředí na znalost cílové komunity a na stanovení vhodné politiky práce s metadaty.
- *Autenticita (Authenticity)* – jedná se o schopnost prokázat, že digitální objekt je skutečně tím, čím tvrdí, že je. Objekt by měl být důvěryhodnou replikou objektu původního a veškeré na něm provedené změny by měly být zaznamenány v příslušných metadatech. I v této oblasti se hlavní hrozby dotýkají zejména metadat, jejich správy, bezpečnostních procedur a dokumentace pracovních postupů.

DRAMBORA

Nástroj DRAMBORA (Digital Repository Audit Method Based on Risk Assessment) poskytuje auditorům webové prostředí, které je provede všemi kroky analýzy rizik. Jedná se o druhou

[6] VERMAATEN, Sally, Brian LAVOIE a Priscilla CAPLAN. Identifying Threats to Successful Digital Preservation: the SPOT Model for Risk Assessment. *D-Lib Magazine* [online]. 2012, vol. 18, 9/10, s. - [cit. 2014-05-02]. DOI: 10.1045/september2012-vermaaten. Dostupné z: http://www.dlib.org/dlib/september12/vermaaten/09vermaaten.html
[7] DIGITAL CURATION CENTRE AND DIGITALPRESERVATIONEUROPE. *DRAMBORA Interactive* [online]. (c) 2008 [cit. 2014-05-02]. Dostupné z: http://www.repositoryaudit.eu/

verzi nástroje – verze první byla dostupná pouze v papírové (přesněji řečeno PDF) podobě. Jedná se o poměrně propracované prostředí, které je ale zároveň jednoduše ovladatelné. V rámci nástroje mohou uživatelé pracovat i s detailním katalogem rizik. DRAMBORA je primárně koncipována jako nástroj k provádění interního auditu. Je však možno ji využít i pro potřeby externího auditu nebo ve smyslu přípravné fáze na oficiální certifikaci repozitáře.
Nevýhodou tohoto nástroje je zejména skutečnost, že jeho vývoj byl již ukončen. Vzhledem k tomu, že se jedná o online aplikaci, není jasné, jak dlouho a za jakých podmínek bude nástroj dostupný. Alternativou je využití DRAMBORA verze 1 – tedy papírové verze.
Práce s DRAMBORA je rozdělena do několika fází zobrazených na obrázku č. 2. První tři se zabývají mapováním personálních zodpovědností a identifikací repozitáře. Další čtyři jsou určeny k popisu kontextu repozitáře. Posouzení rizik je náplní posledních tří fází.



Obrázek č. 2 - Fáze auditu DRAMBORA[8]

[8] DIGITAL CURATION CENTRE AND DIGITALPRESERVATIONEUROPE. *DRAMBORA Interactive* [online]. (c) 2008 [cit. 2014-05-02]. Dostupné z: http://www.repositoryaudit.eu/

Své cíle, aktivity, omezení, přínosy a rizika repozitář definuje na základě deseti funkčních tříd. Třídy byly definovány ve spolupráci s pracovními skupinami zodpovědnými za vývoj kritérií pro repozitáře TRAC a Nestor. Uživatelům se důrazně nedoporučuje je měnit.
Funkční třídy zahrnují:
Procesní okruhy:

- akvizice a ingest
- ochrana integrity digitálních objektů, autenticita a využitelnost
- management metadat a zachycení aktivit systému
- šíření a využívání dokumentů
- plánování ochrany a spojených aktivit

Podpůrné okruhy:

- mandát a zavázání se k ochraně digitálních objektů
- organizační způsobilost (stav organizace)
- právní a jiná regulační legitimita
- účinné a efektivní koncepce
- odpovídající technická infrastruktura

Další dostupné nástroje

Z dalších nástrojů je třeba zmínit zejména TRAC (Trusted Repository Audit Checklist)[9]. Tento nástroj poskytuje kritéria pro audit a certifikaci repozitáře. Kritéria jsou rozdělena do tří hlavních oblastí – organizační infrastruktura, správa digitálních objektů a technologie, technologická infrastruktura a bezpečnost – tyto se dále větví do detailnějších kategorií. TRAC je podkladem pro poměrně náročnou externí certifikaci repozitáře. Může však být využit i jako referenční nástroj při identifikaci rizik.
Je třeba také poznamenat, že na základě TRAC vznikla norma ISO 16363:2012 – Systémy pro přenos dat a informací z kosmického prostoru – Audit a certifikace důvěryhodných digitálních úložišť.
Dalším zajímavým nástrojem je Plato preservation planning tool[10], který je možné využít při plánování strategie dlouhodobé ochrany. Jedná se stejně jako v případě DRAMBORA o webovou aplikaci. Tato je však dále rozvíjena a průběžně doplňována o užitečné nástroje sloužící zejména k analýze obsahu repozitáře.

Využití v institucionálním repozitáři Univerzity Karlovy v Praze

Digitální univerzitní repozitář Univerzity Karlovy v Praze funguje jako institucionální repozitář již od roku 2006. Jeho primárním obsahem byly vysokoškolské kvalifikační práce. Postupem času však začal být plněn i dalšími druhy digitálního obsahu – dnes jsou zde archivovány například i digitalizované mapy nebo elektronické verze výstav Knihovny geografie Přírodovědecké fakulty. Aktuálně tvoří Mapová sbírka jádro repozitáře – obsahuje originální scany map ve formátu tiff doplněné uživatelskými verzemi ve formátu jp2000. Obdobně repozitář pracuje i s dalšími digitalizovanými dokumenty. Druhý výrazný typ dokumentu tvoří diplomové práce (aktuálně jsou v DUR uloženy pouze starší digitalizované práce), které jsou ve formátu PDF. Vzhledem ke složení a významu sbírek je jejich dlouhodobé uchování pro repozitář klíčové.

[9] CENTER FOR RESEARCH LIBRARIES. *Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC)*. [online]. 2007 [cit. 2014-05-02]. Dostupné z: http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf
[10] *Plato* [online]. (c) 2006-2014 [cit. 2014-05-02]. Dostupné z: http://www.ifs.tuwien.ac.at/dp/plato/intro/

Rizika hrozící Digitálnímu univerzitnímu repozitáři byla posuzována dvakrát. V roce 2008 byla použita online verze nástroje DRAMBORA[11] a v roce 2014 pracovali administrátoři repozitáře s nástrojem SPOT. Důvodem využití dvou různých nástrojů byly zejména obavy z možné ztráty dat uložených v systému DRAMBORA, jehož budoucnost je v současné době nejistá. Nástroj SPOT se navíc zdál být vhodný i díky své jednoduchosti a flexibilitě. Tento předpoklad se potvrdil. Model SPOT je otevřený a zejména v prvních fázích auditu se jeho struktura ukázala být neocenitelným pomocníkem při identifikaci jednotlivých rizik. Na druhou stranu online verze nástroje DRAMBORA byla uživatelsky příjemnější a výrazně usnadňovala vyhodnocení auditu.
Postup obou auditů byl obdobný. Nejdříve byly shromážděny informace o repozitáři. Vzhledem k tomu, že se jednalo o interní audit prováděný přímo pracovníky repozitáře, šlo spíše o utřídění dosavadních znalostí a o inventuru dostupné dokumentace. V dalším kroku byla provedena identifikace jednotlivých rizik. Jejich analýza a hodnocení probíhaly prakticky současně formou diskuse v rámci administrátorského týmu. Zvládání zjištěných rizik se ukázalo být dlouhodobou a prakticky nikdy nekončící činností, kterou ovšem provedený audit značně usnadnil.
Posouzení rizik v obou případech označilo problematické oblasti, jejichž existence si byl repozitář vědom již dříve. Audit však jednotlivým rizikům (přesněji řečeno krokům vedoucím k jejich zvládání) přiřadil prioritu a upozornil na vazby mezi nimi. Stal se také užitečným podkladem pro plánování dalšího rozvoje repozitáře.
V rámci posuzování v roce 2014 byla rizika identifikována na základě skupin nástroje SPOT a následně byla určena jejich závažnost a pravděpodobnost na škále 1-5. Nejzávažnější a nejpravděpodobnější rizika v jednotlivých oblastech jsou následující:

- Dostupnost
  - Objekt byl digitalizován a jeho digitální podoba není vhodná pro zobrazení – týká se zejména starších digitalizací, jejichž výsledky jsou často uloženy mimo repozitář a mnohdy ani nejsou podchyceny v žádném z informačních systémů univerzity.
- Identita
  - Vyhledávání nepřináší relevantní výsledky – nastavení vyhledávání v systému DigiTool nepřináší vždy relevantní výsledky.
- Trvalost
  - Objekt byl fyzicky poškozen (bit-rot) – mapová sbírka – v době posuzování rizik byly odhaleny nedostatky v systému kontroly integrity objektů. Riziko mělo poměrně nízkou závažnost, vzhledem k tomu, že objekty jsou pravidelně zálohovány. V současné chvíli již ale došlo ke změně systému kontrol.
- Reprodukovatelnost
  - Nedostatek licencí – objekt není možné archivovat – používaný software je sice z hlediska reprodukovatelnosti vhodný, nicméně repozitář často bojuje s licenčním omezením počtu archivovaných objektů.
- Srozumitelnost
  - Objekty nevyhovují požadavkům znevýhodněných uživatelů – oblast uživatelského rozhraní se ukázala být nejrizikovější. Vysoké závažnosti i pravděpodobnosti dosahovala nejen rizika zaměřená na znevýhodněné uživatele, ale i rizika týkající se běžných uživatelů.
- Autenticita
  - Objekt byl změněn a byl mu přidělen nový identifikátor – repozitář sice pracuje s trvalým identifikátory, ale v některých případech je změna objektů prováděna jejich smazáním a opětovným ingestem. V tomto případě se ovšem identifikátor změní.

[11] HUTAŘ, Jan, Andrea FOJTŮ a Eliška PAVLÁSKOVÁ. DRAMBORA: Nástroj na interní audit digitálních úložišť v nové online verzi a postřehy z provedených auditů. In: *INFORUM 2008: 14. ročník konference o profesionálních informačních zdrojích* [online]. 2008 [cit. 2014-09-22]. ISSN 1801-2213. Dostupné z: http://www.inforum.cz/pdf/2008/hutar-jan-cze.pdf

Obsahově se závěry obou auditů poměrně výrazně lišily – důvodem bylo jednak použití různých metodik a dále i skutečnost, že rizika posouzená v rámci prvního auditu byla v následujících letech zmírněna nebo byla snížena pravděpodobnost jejich výskytu. Změnil se i obsah repozitáře. Výsledky auditu z roku 2014 jsou konkrétnější a snáze prakticky uchopitelné. Audit samotný vedl k úpravě některých procesů (např. kontrola integrity) a k návrhu projektů zpracovávajících problematickou oblast uživatelského rozhraní.

Závěr

Techniky posuzování rizik jsou pro institucionální repozitáře neocenitelným nástrojem. Ačkoli by se mohlo zdát, že jen systematizují závěry a postupy, které napovídá obyčejný zdravý rozum, je právě tato systematizace mnohdy tím, co odděluje pouhé vědomí toho, že „toto bychom asi měli dělat“ od konkrétního plánu a jeho převedení do praxe.
Specifické nástroje určené přímo institucionálním repozitářům navíc i poskytují záchytné body a vymezují základní oblasti zájmu. Umožňují tak auditorům rozčlenění poměrně široké a komplexní problematiky do menších a snáze uchopitelných celků.
Ze zkušeností také vyplývá, že samotné použití konkrétního nástroje se paradoxně může stát rizikem. Vzhledem k tomu, že v případě řízení rizik se rozhodně nejedná o jednorázový proces, by měl institucionální repozitář při výběru vhodného nástroje a následném zpracování výstupů z procesu posuzování rizik počítat i s nutností dlouhodobě a důvěryhodně uchovat tyto výstupy.

Použitá literatura

BARATEIRO, José, Gonçalo ANTUNES, Filipe FREITAS a José BORBINHA. Designing Digital Preservation Solutions: A Risk Management-Based Approach. *International Journal of Digital Curation* [online]. 2010-07-21, vol. 5, issue 1, s. 4-17 [cit. 2014-05-02]. DOI: 10.2218/ijdc.v5i1.140. Dostupné z: http://ijdc.net/index.php/ijdc/article/view/143

Consultative Committee for Space Data Systems. *Reference Model for an Open Archival Information System (OAIS)* [online]. Washington (D.C.) : CCSDS, January 2002 [cit. 2009-09-24]. [1, xiii, 139 s.]. Recommendation for Space Data System Standards, CCSDS 650.0-B-1. Blue Book, Issue 1. Dostupný z WWW: <http://public.ccsds.org/publications/archive/650x0b1.pdf>

CENTER FOR RESEARCH LIBRARIES. *Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC)*. [online]. 2007 [cit. 2014-05-02]. Dostupné z: http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

DATA SEAL OF APPROVAL BOARD. *Data Seal of Approval: Guidelines version 2*. [online]. 2013 [cit. 2014-05-05]. Dostupné z: http://www.datasealofapproval.org/media/filer_public/2013/09/27/guidelines_2014-2015.pdf

DIGITAL CURATION CENTRE AND DIGITALPRESERVATIONEUROPE. *DRAMBORA Interactive* [online]. (c) 2008 [cit. 2014-05-02]. Dostupné z: http://www.repositoryaudit.eu/

HUTAŘ, Jan, Andrea FOJTŮ a Eliška PAVLÁSKOVÁ. DRAMBORA: Nástroj na interní audit digitálních úložišť v nové online verzi a postřehy z provedených auditů. In: *INFORUM 2008: 14. ročník konference o profesionálních informačních zdrojích* [online]. 2008 [cit. 2014-09-22]. ISSN 1801-2213. Dostupné z: http://www.inforum.cz/pdf/2008/hutar-jan-cze.pdf

ISO 31000:2009. *Risk management: Principles and guidelines*. 2009.

Kubálková, Petra, Loská, Šárka. Risk management. Ikaros [online]. 2006, roč. 10, č. 12 [cit. 02.05.2014]. Dostupný z WWW: http://www.ikaros.cz/node/3728. urn:nbn:cz:ik-003728. ISSN 1212-5075.

NATIONAL ARCHIVES. *Risk Assessment Handbook* [online]. (c) 2011 [cit. 2014-05-02]. Dostupné z: http://www.nationalarchives.gov.uk/documents/information-management/risk-assessment-handbook.pdf

Plato [online]. (c) 2006-2014 [cit. 2014-05-02]. Dostupné z: http://www.ifs.tuwien.ac.at/dp/plato/intro/

VERMAATEN, Sally, Brian LAVOIE a Priscilla CAPLAN. Identifying Threats to Successful Digital Preservation: the SPOT Model for Risk Assessment. *D-Lib Magazine* [online]. 2012, vol. 18, 9/10, s. - [cit. 2014-05-02]. DOI: 10.1045/september2012-vermaaten. Dostupné z: http://www.dlib.org/dlib/september12/vermaaten/09vermaaten.html