Univerzita Karlova

Filozofická fakulta

Katedra pomocných věd historických a archivního studia

Bakalářská práce

Daniel Šurda

Audit a certifikace digitálních úložišť v rámci archivnictví

Audit and Certification of digital repositories within archival science

2022

Vedoucí práce: PhDr. Ing. Milan Vojáček, Ph.D.

Poděkování

Chtěl bych tímto poděkovat PhDr. Ing. Milanu Vojáčkovi, Ph.D., vedoucímu této bakalářské práce, za pomoc, připomínky, rady, trpělivost a vstřícnost, které mi během její tvorby poskytl.

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, že jsem řádně citoval všechny použité prameny a literaturu a že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze dne ....

Daniel Šurda

Abstrakt

Cílem bakalářské práce je především popsání auditních a certifikačních nástrojů pro dlouhodobá úložiště digitálních dat, které se dají použít v oblasti archivnictví. V první části práce je popsán Evropský rámec pro audit a certifikaci digitálních repozitářů, tedy certifikace dle Core Trust Seal, německé Pečeti nestoru a dle normy ISO 16363. Druhá část se zabývá akreditací digitálního archivu, která je zakotvena v české legislativě. Ve třetí kapitole autor pojmenovává některá specifika archivnictví v oblasti auditních a certifikačních nástrojů dlouhodobé ochrany digitálních dat a řeší otázku vhodnosti takových nástrojů.

Klíčová slova

audit, certifikace, archivnictví, digitální archivace, digitální úložiště, standardy k digitální archivaci

Abstract

The aim of this bachelor thesis is primarly to describe audit and certification tools for long-term digital data repositories which can be used in archiving. The first part describes European Framework for Audit and Certification of Digital Repositories (certification based on Core Trust Seal, German nestor Seal and ISO 16363). The second part deals with accreditation of digital archives which is embedded in Czech legislation. In the third part, the author names some specifics of archiving in the field of audit and certification tools for long-term digital data preservation and he deals with appropriatness of such tools.

Key words

audit, certification, archival science, digital preservation, digital repository, standards for digital preservation

Obsah

Seznam zkratek

AIP	Archival Information Package
AZ	Zákon č. 499/2004 Sb., o archivnictví a spisové službě
CCSDS	Consultative Committee for Space Data Systems
ČNB	Česká národní banka
ČSN	Česká státní norma
DIN[1]	Deutsche Industrie-Norm
DIN[2]	Deutsches Institut für Normung
DIP	Dissemination Information Package
EPS	Elektrická požární signalizace
NSESSS	Národní standard pro elektronické systémy spisové služby
IAF	International Accreditation Forum
INR	Indian rupee
ISO	International Organization for Standardization
LTP	Long Time Preservation
NABCB	National Accreditation Board for Certification Bodies
OAIS	Open Archival Information System
PTAB	Primary Trustworthy Digital Repository Authorisation Body Ltd
SAARC	South Asian Association for Regional Cooperation
SIP	Submission Information Package
VHA	Vojenský historický archiv

Úvod

Předkládaná práce se zabývá otázkou auditních a certifikačních nástrojů úložišť pro dlouhodobou ochranu digitálních dokumentů v rámci archivnictví. Auditní a certifikační nástroje slouží především k budování, případně posilování, důvěry v instituce, které se zaměřují na dlouhodobé ukládání digitálních dokumentů. Zpravidla přicházejí s katalogem požadavků, které taková instituce musí splnit. Pokud instituce požadavkům dostojí, dokazuje, že je schopna plnit své poslání, tedy zajistit nejen přístupnost dat v ní uložených, ale i jejich čitelnost pro budoucí příjemce. Taková instituce se pak svému okolí bude jevit jako důvěryhodná.

Auditní a certifikační nástroje své využití nacházejí i jinde než jen v archivářské oblasti. Setkáme se s nimi pochopitelně všude, kde je téma dlouhodobé ochrany dat v digitální podobě aktuální. Jedná se o různé typy organizací od ostatních paměťových institucí (zejména knihoven) přes vědecká pracoviště, jež potřebují ukládat výsledky svého výzkumu, až po soukromou sféru.

Vlastní text je rozdělen do tří kapitol. První se věnuje možnostem auditu a certifikace, zejména Evropskému rámci pro audit a certifikaci digitálních repozitářů. Jeho struktura je třístupňová. První stupeň představuje nejjednodušší možnost v podobě Core Trust Seal, následuje původem německá Pečeť nestoru a posledním ze stupňů je certifikace dle normy ISO 16363. Věnován je prostor ještě procesu akreditace certifikační autority dle normy ISO 16919. V závěru dochází k celkovému shrnutí, jež se snaží určit, která z možností je pro archivnictví nejvhodnější.

Druhá kapitola rozebírá detailně akreditaci digitálního archivu podle českého archivního zákona. Sleduje vlastní průběh procesu akreditace, při němž musí žadatel předložit řadu dokumentů a získat potřebné souhlasy. Dále se zabývá strukturou a obsahem vlastní dokumentace, která je z velké části postavena na Pečeti nestoru, a tématem zkušebního přenosu archiválií do Národního digitálního archivu, jehož úspěšné provedení je nezbytnou podmínkou. Prostor je dále věnován otázkám stavebně-technických a bezpečnostních podmínek. Nakonec je krátce zmíněno, kdy a jakým zákonem se možnost akreditace digitálního archivu objevila v českém archivnictví.

Třetí a poslední kapitola se věnuje otázce specifik archivnictví vůči jiným organizacím, které podobná úložiště provozují, a otázce vhodnosti auditních a certifikačních nástrojů pro archivy. Jedná se především o autorův příspěvek na toto téma, který vychází z prostudované literatury.

Použitá literatura

Dobrý úvod do problematiky auditních a certifikačních nástrojů představuje článek Andrei Mirandy *Důvěryhodná digitální úložiště, jejich audit a certifikace*, publikovaný roku 2015 v časopise Národní knihovny Knihovna: Knihovnická revue, a článek archivářů Národního archivu Jiřího Bernase, Zbyška Stodůlky a Milana Vojáčka *Certifikace NESTOR* vyšlý roku 2019 ve sborníku z konference o dlouhodobé archivaci. Jako obecné uvedení do oblasti dlouhodobé archivace posloužila skripta *Digitální archivnictví* vytvořená pro výuku na Masarykově univerzitě, *Příručka nestoru: Malá encyklopedie dlouhodobé digitální archivace* od nestoru a řada závěrečných prací pocházejících především z Ústavy informačních studií a knihovnictví na FF UK.

První i druhá kapitola vychází přímo z katalogů požadavků jednotlivých auditních a certifikačních nástrojů, jež jsou dnes většinou dostupné online ze stránek příslušných

organizací, kde se nacházejí i další informace (např. seznam certifikovaných repozitářů a základní poznatky o nich nebo ceníky služeb). Odkazy na adresy webových stránek, katalogy požadavků a další se nacházejí ve vlastním textu v poznámkách pod čarou u příslušných nástrojů. Norma ISO 16363 byla zpracována i na základě ČSN ISO 16363, kterou vydal Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Z oblasti legislativy byl použit zákon č. 499/2004 Sb., o archivnictví a spisové službě, a na něj navazující vyhlášky č. 645/2004 Sb., kterou se provádí zákon o archivnictví a spisové službě, a č. 259/2012 Sb., o podrobnostech výkonu spisové služby, vše v aktuálním znění. Dále musí být zmíněn zákon č. 500/2004 Sb., správní řád, a zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Zákon č. 167/2014 Sb., kterým se mění zákon o archivnictví a spisové službě, zákon o elektronickém popisu a další související zákony, posloužil k poznání, jak se objevila možnost akreditace digitálního archivu v českém archivnictví.

1. Možnosti auditu a certifikace

Kdo by se v dnešní době rozhodl dlouhodobě uchovávat digitální data, má dnes k dispozici řadu možností, jak prověřit a ohodnotit svůj digitální repozitář, Tyto prostředky mohou představovat jednoduchou sebeevaluaci, ale i finančně náročný proces zakončený certifikátem ISO. V případě, že by se někdo chtěl posunout ještě o úroveň výš a sám digitální repozitáře a jejich provozovatele hodnotit, má možnost projít akreditačním procesem a stát se certifikační autoritou. Akreditační proces je do této kapitoly zahrnut rovněž, neboť může být zajímavý, když si uvědomíme, že Národní archiv a Odbor archivní správy a spisové služby Ministerstva vnitra v některých případech vystupují v takovéto úloze.

1.1. Evropský rámec pro audit a certifikaci digitálních repozitářů (European Framework for Audit and Certification of Digital Repositories)

V roce 2010 vznikl *Evropský rámec pro audit a certifikaci digitálních repozitářů* na základě spolupráce tří subjektů: nizozemské *Data Seal of Approval*, *Poradního výboru pro kosmické datové systémy* (CCSDS), *pracovní skupiny pro Certifikaci důvěryhodných archivů Německého ústavu pro průmyslovou normalizaci* (DIN).[1] Z jejich spojení vzešla organizace *Trusted digital repositories*, jež zajišťuje rámec pro audit a certifikaci digitálních repozitářů.[2]

Jsou stanoveny tři stupně certifikace. Pro získání základního stupně stačí splnit podmínky Core Trust Seal (původně Data Seal of Approval). Rozšířená certifikace vyžaduje splněný základní stupeň, následně provedený interní audit (sebeevaluaci) dle normy ISO 16363 či rovnocenné německé normy DIN 31644[3] a veřejné vyhlášení výsledků. K formální certifikaci je nutné rovněž mít základní stupeň a posléze udělat externí audit dle týchž norem jako u rozšířené certifikace.[4] Formální certifikace by se ovšem prováděla složitě, poněvadž pro normu ISO existovala k roku 2019 pouze jedna certifikační autorita. V praxi se tudíž zpravidla používá pokročilé sebehodnocení na základě Pečeti nestoru, jež vychází z normy DIN.[5]

1.2. Core Trust Seal[6]

Požadavky Core Trust Seal (původně Data Seal of Approval) představují sadu pouze 16 zásad (Requirements, zkratka R) ve třech kategoriích. Všechny požadavky jsou povinné a mají se hodnotit samostatně. Stupňů, jak moc je zásada plněná, (Compliance level) je definováno pět:

0 – zásada je neaplikovatelná,

---

[1] Miranda Andrea: *Důvěryhodná digitální úložiště, jejich audit a certifikace*, Knihovna: Knihovnická revue, 2015, 26 (2).

[2] Tamtéž.

[3] Norma ISO je mnohem podrobnější, obsahuje 109 kritérií, zatímco DIN pouze 34. Viz níže.

[4] Tamtéž.

[5] Bernas Jiří, Stodůlka Zbyšek, Vojáček Milan: *Certifikace NESTOR* in: LTP 2019: Nové trendy a východiska pri budování LTP archívov: zborník príspevkov zo 4. medzinárodnej konferencie o dlhodobej archivácii, Bratislava 2019.

[6] *CoreTrustSeal Trustworthy Data Repositories Requirements: Extended Guidance 2020–2022*, Core Trust Seal, online. https://www.coretrustseal.org/why-certification/requirements/ [Core Trust Seal, 17. ledna 2022] (dále jako Požadavky CoreTrustSeal)

1 – o zásadě se ještě neuvažovalo,
2 – pro zásadu existuje teoretický koncept,
3 – zásada se nachází ve fázi zavádění a
4 – zásada je plně implementovaná. [7]

V případě, že repozitář usoudí, že zásadu nelze zavést, musí mít pro takový závěr dostatečné důvody popsané do detailu. Pokud jsou, byť jen některé, požadavky plněny na úrovni 1 nebo 2, nelze certifikaci udělit. Stupeň 3 u menšího počtu zásad nevadí.

Prohlášení, jímž se plní zásady, by mělo být dostupné co nejlehčeji, ideálně online, a mělo by obsahovat odkazy na podpůrnou dokumentaci. Nejlépe by mělo být prohlášení včetně celé dokumentace sepsáno v angličtině. Nicméně autoři jsou si vědomi, že ne vždy lze tuto podmínku dodržet, proto je možné je napsat i v jiném jazyce a připojit k nim anglický souhrn.

Core Trust Seal platí tři roky od data, kdy bylo uděleno. Počítá se s tím, že pokud repozitář funguje a plní své cíle, jak má, nebude pro něj problém certifikaci znovu získat. Dojde-li však buď k příliš velkým změnám repozitáře, jeho dat nebo cílové skupiny, či podstatné změně samotných požadavků Core Trust Seal, je třeba certifikaci obnovit dřív.

„Nultá“ kategorie kontext (Context) obsahuje pouze jednu zásadu (R0), v níž se popisuje kontext repozitáře, tj. typ repozitáře (např. archiv, muzeum, repozitář výzkumného projektu), stručný popis repozitáře a cílové skupiny, úroveň správy dat[8] a komentář k partnerům, případně přehled významných změn od minulého auditu a ostatní důležité informace.

Do první kategorie nazvané organizační infrastruktura (Organizational Infrastructure) spadají zásady R1 až R6. Repozitář musí dokázat, že:

R1 – má jasně zadaný cíl, pro nějž shromažďuje a spravuje data,
R2 – vlastní licence, souhlasy a další potřebné ke správě dat a kontroluje je,
R3 – má zpracovaný plán, jak zajistit dlouhodobé uchování a přístup k datům,
R4 – práce s daty funguje za dodržování etických a disciplinárních norem,
R5 – je přiměřeně financován a má potřebný a dostatečně proškolený personál a jasný systém řízení a
R6 – zvládl si zajistit odborné poradenství a zpětnou vazbu.[9]

Druhá kategorie obsahuje 7 požadavků (R7 až R14), které se váží ke správě digitálních objektů (Digital Object Management). Repozitář zde dokládá, že:

R7 – ručí za integritu a autenticitu uložených dat,
R8 – přijímá data i metadata na základě určitých kritérií, aby zajistil jejich relevantnost a možnost porozumění pro uživatele,
R9 – veškeré změny a procesy jsou dokumentovány,
R10 – má plán pro dlouhodobé uchovávání,
R11 – zajišťuje kvalitu a úroveň technických dat a metadat vzhledem k uživatelům,
R12 – ukládání se odehrává na základě daných pravidel,
R13 – umožňuje uživateli v datech hledat a odkazovat na ně a

[7] Požadavky CoreTrustSeal, s. 3

[8] Rozlišují čtyři typy: A. obsah je pouze ukládán; B. základní péče – stručná kontrola, doplněna základní metadata či dokumentace; C. lepší péče – konverze do nových formátů, lepší dokumentace; D. péče na úrovni dat – jako C, navíc ještě měněna data kvůli správnosti. Typů lze plnit víc současně.

[9] Požadavky CoreTrustSeal, s. 10–15.

R14 – poskytuje možnost data znovu použít a že jsou k nim dostupná metadata, která zajistí jejich čitelnost a pochopení.[10]

Poslední kategorii, Technologie (Technology), představují dva požadavky (R15 a R16). Repozitář jednak prokazuje, že funguje na dobře podporovaném softwaru a zároveň používá software i hardware vhodný pro služby, které nabízí cílové skupině (R15), a že technická infrastruktura se stará o ochranu (Security) zařízení, dat, produktů, služeb a uživatelů.[11]

V současné době byla provedena certifikace Core Trust Seal u 118 repozitářů (včetně již expirovaných),[12] z nichž pouze dva jsou české a oba se nacházejí v Praze. Získal ji Ústav formální a aplikované lingvistiky MFF UK roku 2019 pro úložiště LINDAT/CLARIN.[13] Český sociálněvědní datový archiv (ČSDA), součást Sociologického ústavu AV ČR, sice v roce 2018 certifikaci obdržel, ale už ji neobnovil.[14] Jen pro zajímavost, na Slovensku žádný repozitář certifikaci dle Core Trust Seal nemá. V Rakousku lze nalézt čtyři certifikované repozitáře, např. Österreichisches wissenschaftliches Datenarchiv.

1.3. Pečeť nestoru

Certifikace na základě Pečeti nestoru je postavena na německé normě DIN 31644. V rámci plnění požadavků archivního zákona[15] na oblast digitálního archivnictví a akreditaci digitálních archivů vznikl v rámci Národního archivu český akreditovaný překlad Pečetě nestoru jako třetí příloha metodického návody k akreditaci digitálních archivů.[16]

Digitální archiv je v normě definován jako *organizace sestávající se z osob a technických systémů, která převzala odpovědnost za dlouhodobé uchovávání a dlouhodobou dostupnost informací v digitální formě, jako i za jejich poskytnutí určité cílové skupině*. Nelze tedy certifikovat pouze softwarové a hardwarové řešení, ani jen určitý úsek digitálního archivu.[17] Pracuje se pouze s nynějším stavem, minulé stavy ani budoucí plány se neberou v potaz.

Chce-li instituce získat Pečeť nestoru, nejprve se nahlásí nestoru, který určí osoby zodpovědné za provedení evaluace. Instituce následně provádí sebeevaluaci dle odkazů a pokynů nestoru. Když má hotovo, předá podklady, napsané v angličtině či němčině, určeným osobám, jež je prověří a vypracují posudek. V případě, že se zjistí rozpory, žádá se instituce o vyjádření. Podklady putují k dalšímu posuzujícímu, který rozhodne s konečnou platností, zda instituce Pečeť nestoru získá. Pokud se tak stane, je instituci vystavena Pečeť a je zanesena do registru držitelů Pečeti nestoru. V opačném případě má instituce právo se odvolat. Pečeť nestoru platí neomezeně, není totiž předepsáno, že se má certifikace opakovat. Nicméně, po jisté době ztrácí svou výpovědní hodnotu.[18] Je vyžadován poplatek 500 € (12 170,- Kč).[19]

---

[10] Tamtéž, s. 16–23.

[11] Tamtéž, s. 24 a 25.

[12] Core Certified Repositories, Core Trust Seal, online: https://www.coretrustseal.org/why-certification/certified-repositories/ [Core Trust Seal, 20. ledna 2022]

[13] Odkaz na certifikaci: https://www.coretrustseal.org/wp-content/uploads/2019/08/LINDAT-CLARIN.pdf [Core Trust Seal, 20. ledna 2022]. Jednalo se o prodloužení, certifikaci měli už předtím.

[14] Certifikace zde: https://www.coretrustseal.org/wp-content/uploads/2018/01/Czech-Social-Science-Data-Archive.pdf [Core Trust Seal, 20. ledna 2022]. Dosud mají na webových stránkách logo Core Trust Seal.

[15] Zákon č. 499/2004 Sb., o archivnictví a spisové službě

[16] Metodický návod č. 2/2022 odboru archivní správy a spisové služby Ministerstva vnitra pro akreditaci digitálního archivu, příloha č. 3, MV ČR 2022.

[17] Metodický návod č. 2/2022, příloha č. 3, str. 2.

[18] Tamtéž, str. 2–4.

[19] Kurz 1 € = 23,40,- Kč dle ČNB k 18. únoru 2022.

Kritérií (označovány K), z nichž Pečeť nestoru vychází, je celkem 34. Stav plnění a implementace kritérií se hodnotí bodově dle následujícího klíče:

0 bodů – ještě otevřené – pro dané kritérium neexistují žádné koncepty,

3 body – plánované – existuje písemný koncept vztahující se k situaci daného archivu,

6 bodů – naplánované do detailu – koncept je detailní a jeho implementace již začala a

10 bodů – implementováno – kritérium je zcela plněno, jedná se o standardní postup.[20]

V případě, že je kritérium ohodnoceno 6 či 10 body, počítá se s existencí dokumentace, která je, pokud tomu nebrání obchodní tajemství, autorská práva, a d., zveřejněná. Kritéria K1 až K12 jsou brána jako klíčová, musí proto všechna získat 10 bodů. Ostatní kritéria musí získat v průměru nejméně 7 bodů. Kromě klíčových kritérií lze některá kritéria vyloučit, pokud to instituce může dostatečně zdůvodnit.[21]

V prvních dvanácti kritériích instituce dokazuje, že:

K1 – má jasná kritéria pro výběr dat, ví, pro jaký typ informací je její archiv příslušný (tzv. mandát nebo role archivu),

K2 – přebírá dlouhodobou odpovědnost za uchovávání dat,

K3 – definovala své cílové skupiny a přizpůsobuje se jejich změnám,

K4 – zajišťuje přiměřený přístup cílových skupin k uloženým datům, umožňuje v nich vyhledávat,

K5 – zajišťuje dlouhodobou čitelnost dat (jak obsahu, tak metadat), bere při tom ohled na cílové skupiny a pravidelně čitelnost kontroluje,

K6 – má vztahy s producenty dat postaveny na smluvních základech, jsou jasně domluveny přejímky dat, způsob jejich uchování a využití,

K7 – se při své činnosti řídí zákony a uzavřenými smlouvami,

K8 – má dlouhodobý koncept financování digitálního archivu,

K9 – digitální archiv má přiměřený počet pracovníků, existuje popis pracovních pozic a koncepce rozvoje zaměstnanců,

K10 – organizační struktura, procesy a odpovědnost jsou uzpůsobené cílům a jasně dané,

K11 – se zabývá i činnostmi souvisejícími s uchováním dat v širším měřítku, tudíž sleduje změny, plánuje apod. a

K12 – existuje krizový plán a plán, jak zajistit data i po zániku digitálního archivu.[22]

Ve zbylých dvaadvaceti kritériích instituce dokládá, že:

K13 – digitální archiv pracuje s vlastnostmi dat a rozhoduje o významných vlastnostech (vlastnostech významných pro uchování informace),

K14 – digitální archiv má rozhraní pro příjem, které je s to přijímat vstupní datové balíčky (SIP), předělávat je do archivních datových balíčků (AIP) a zachovávat integritu a autenticitu dat,

K15 – digitální archiv zahrnuje i archivní úložiště, které zachovává integritu a autenticitu dat, umožňuje dlouhodobé uchování balíčků AIP, jejich zapisování na média a změny,

K16 – digitální archiv disponuje uživatelským rozhraním, které převádí balíčky AIP do výstupních datových balíčků (DIP) a umožňuje snadnou práci s balíčky jak administrátorům, tak uživatelům,

[20] Tamtéž, s. 3.
[21] Tamtéž.
[22] Tamtéž, s. 5–16.

K17 – digitální archiv postupuje tak, aby posoudil autenticitu přijímaných dat,
K18 – digitální archiv pracuje tak, aby zajistil autenticitu uchovaných dat,
K19 – digitální archiv dovoluje kontrolovat autenticitu uložených dat, do čehož je zahrnuto i přetváření balíčků AIP na balíčky DIP,
K20 – digitální archiv má dostatečné technické oprávnění, aby mohl pracovat s daty,
K21 – digitální archiv definoval své balíčky SIP a dohodl se na nich s producenty dat,
K22 – digitální archiv převádí balíčky SIP na balíčky AIP,
K23 – digitální archiv má specifikaci svých balíčků AIP a řídí se dle ní,
K24 – digitální archiv pracuje tak, aby zachoval čitelnost balíčků AIP,
K25 – digitální archiv převádí balíčky AIP na balíčky DIP,
K26 – digitální archiv definoval své balíčky DIP, bera při tom ohled na cílové skupiny,
K27 – digitální archiv jednoznačně identifikuje data a propojuje je tak s metadaty, identifikátory jsou standardizované a kromě propojení umožňují jistý přístup,
K28 – jsou stanovena popisná metadata s ohledem na cíle digitálního archivu, cílových skupin a typu dat,
K29 – je dostatečně popsána struktura dat (strukturální metadata),
K30 – jsou jasně dána technická metadata tak, aby zajistila čitelnost, autenticitu a integritu,
K31 – digitální archiv vede záznam činností, které souvisí s uchováváním a změnami dat,
K32 – jsou definována administrativní metadata,
K33 – IT infrastruktura při zacházení s daty bere ohled na technické a bezpečnostní požadavky a
K34 – je zajišťována bezpečnost digitálního archivu a uchovávaných dat.[23]

Pečeť nestoru pochází z německého prostředí, proto asi nepřekvapí, že tři ze čtyř institucí, které ji získali, se nacházejí v Německu.[24] Jedná se o Německou národní knihovnu,[25] Lipské informační centrum pro ekonomiku[26] a Lipské informační centrum pro vědu a technologii univerzitní knihovna.[27]

1.4. Norma ČSN ISO 16363[28]

Certifikace dle této normy,[29] jejímž autorem je původně *Poradní výbor pro systémy pro data z kosmického prostoru*, představuje certifikaci formální, která na rozdíl od předchozích dvou, jež si vystačí se sebeevaluací, požaduje externí audit. Pro ten se musí

[23] Tamtéž, s. 17–38.
[24] Nestor Seal for Trustworthy Digital Archives, nestor, online: https://www.langzeitarchivierung.de/Webs/nestor/EN/Services/nestor_Siegel/nestor_siegel_node.html;jsessionid=29517BBEF055CCD9DF92495F458BEE03.intranet372 [nestor, 27. ledna 2022]
[25] Získala ji v roce 2016, materiály k certifikaci dostupné online: https://www.dnb.de/DE/Professionell/Erhalten/Zertifizierung/zertifizierung_node.html [Německá národní knihovna, 21. ledna 2022]
[26] Získalo ji roku 2017, materiály jsou též dostupné online: https://www.zbw.eu/en/about-us/key-activities/digital-preservation/ [Lipské informační centrum pro ekonomiku, 21. ledna 2022]
[27] Podklady pro certifikaci z roku 2017 také dostupné online: https://www.tib.eu/en/publishing-archiving/digital-preservation/ [Lipské informační centrum pro vědu a technologii univerzitní knihovna, 21. ledna 2022]
[28] *Systémy pro přenos dat a informací z kosmického prostoru – Audit a certifikace důvěryhodných digitálních úložišť. ČSN ISO 16363*, Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, Praha 2014.
[29] Kromě ISO 16363 lze použít i rovnocennou německou normu DIN 31644.

najít vhodná autorita, která však v roce 2019 existovala jen jedna.[30] S touto normou souvisí i další normy, za zmínku jistě stojí referenční model pro otevřený archivační systém.[31]

Proces certifikace dle ISO 16363 není jednoduchou záležitostí. Organizace *Primary Trustworthy Digital Repository Authorisation Body Ltd* (dále jen PTAB) je příslušnou certifikační autoritou[32] (certification body), která sama musela být akreditována dle ISO 17021 a ISO 16919.[33] Na svých webových stránkách[34] má podrobně popsaný proces certifikace. PTAB jako certifikační autorita rozhoduje o vydání, zrušení atd. certifikace, má tak činit na základě reality, nesmí pro to používat dodavatele či přenášet práci na někoho jiného. Měla by aktivně komunikovat s klientem, podporovat ho a vycházet mu cenami, časovými plány, … vstříc tak, aby nedocházelo ke zbytečným propadům certifikace.[35] V rámci této činnosti si musí zachovat nestrannost.[36]

Na začátku se organizace musí rozhodnout, že chce své úložiště certifikovat, kontaktuje tedy PTAB, vyplní a pošle dotazník se základními údaji. PTAB se případně doptá na některé záležitosti a následně na základě dotazníku vyhodnotí, zda je vůbec certifikace možná. V případě, že je, připraví cenový odhad a plán certifikace. Souhlasí-li s nimi organizace, dojde k sepsání smlouvy, zaplacení prvních plateb a může začít fáze 1 (Stage 1). Ve fázi 1 je určen auditní tým a organizace si vypracuje sebeohodnocení dle ISO 16363 a zašle ho společně s dalšími potřebnými a podpůrnými dokumenty PTAB. Auditní tým vše projde a snaží se odhalit možné problémy (areas of concern), které by mohly vyústit v nesoulad se standardem. Organizace pak má čas, aby provedla možné změny a vyřešila problémy. Pokud by změny byly až příliš velké, musí se fáze 1 zopakovat. Když je organizace hotová a připravená, může začít fáze 2. V ní se koná audit přímo na místě, do organizace jsou posláni auditoři (typicky dva na dva dny). Ti odhalují nesoulady se standardem (nonconformances), u nichž organizace musí odhalit příčiny, vymyslet způsob řešení a vyřešit je. Pokud to organizaci bude trvat déle než 6 měsíců, musí se s fází 2 začít od začátku. Po konci fáze 2 PTAB rozhoduje, zda certifikaci udělí.[37] Pokud organizace certifikaci získá a chce si ji udržet, musí každý rok provést kontrolní audit (surveillance audit) a jednou za tři roky recertifikaci, tedy absolvovat celý certifikační proces znovu.[38]

Náklady, které celý proces certifikace stojí, záleží na velikosti a složitosti úložiště. PTAB uvádí orientační ceny, z nichž se dá odvodit, že se jedná o drahou záležitost.[39] Poplatek za začátek certifikace a fázi 1 u první certifikace nebo recertifikace, resp. u kontrolního auditu, činí 216 000,- Kč (£7.500), resp. 115 200,- Kč (£4.000),[40] poplatek za fázi 2 představuje

[30] Bernas, Stodůlka, Vojáček: *Certifikace NESTOR* in: LTP 2019.

[31] Norma ISO 14721.

[32] Certifikační autorita musí nejprve získat akreditaci, která představuje oprávnění provádět certifikační procesy. Udělují ji akreditační autority (accreditation body), které z většiny sdružuje Mezinárodní akreditační fórum (International Accreditation Forum, IAF). U nás její pozici zastává Český institut pro akreditaci, o.p.s.

[33] Noma ISO 17021 definuje podmínky pro certifikační autority (Requierements for Certification Body) a norma ISO 16919 pro certifikační autority provádějící audit a certifikaci důvěryhodných digitálních repozitářů (Requierements for bodies providing audit and certification of candidate trustworthy digital repositories).

[34] http://www.iso16363.org/ [PTAB, 4. února 2022]

[35] Audit and certification process, PTAB, online: http://www.iso16363.org/iso-certification/certification-processes/ [PTAB, 4.února 2022]

[36] Impartiality Policy, PTAB, online: http://www.iso16363.org/iso-certification/impartiality-policy/ [PTAB, 4. února 2022]

[37] O tom rozhodují vždy jiní lidé než ti, kteří prováděli přímou kontrolu v organizaci.

[38] Overview, PTAB, online: http://www.iso16363.org/iso-certification/overview/ [PTAB, 4. února 2022]

[39] Audit Costs, PTAB, online: http://www.iso16363.org/iso-certification/audit-costs/ [PTAB, 4. února 2022]

[40] Kurz £1 = 28,8,- Kč dle ČNB ke 4. únoru 2022.

86 400,- Kč (£3.000), resp. 57 600 (£2.000). Ve fázi 2 se ještě platí každý den, který jeden auditor stráví na místě, ve výši 34 560,- Kč (£1.200) na den.[41] Samotný poplatek za certifikaci je oceněn na 86 400,- Kč (£3.000), resp. 43 200,- Kč (£1.500). Kromě těchto poplatků se ještě proplácí cestovné a základní výživné, u nichž se konkrétní sumy neuvádějí a jež jsou v čase pandemie nulové, neboť se používá vzdálený přístup. Sečteme-li všechny poplatky (včetně čtyřdenního pobytu) dostaneme, že za úspěšnou certifikaci organizace zaplatí zhruba 527 040,- Kč (£18.300), resp. 354 240,- Kč. (£12.300) u kontrolního auditu. Jako doplňkovou službu nabízí PTAB za 144 000,- Kč (£5.000) ještě „předhodnocení“, které má organizaci pomoct zaměřit se na to, co potřebuje, aby auditem úspěšně prošla.

Na rozdíl od předchozích pomůcek pro audit obsahuje norma ISO 16363 mnohem více kritérií, celkem 109, které jsou rozděleny do tří základních kategorií, jež se dále člení do více podskupin. Kvůli velkému počtu požadavků zde nebudou popsána jednotlivá kritéria samostatně jako u přechozích nástrojů pro audit a certifikaci.

První základní kategorie *Organizační struktura*[42] o 25 požadavcích se člení do pěti podskupin:

Podskupina *Vedení a životaschopnost organizace* (5 kritérií) stanovuje, že úložiště má mít cíl související s uchováním, určeno, jakými typy dokumentů se bude zabývat, vypracovaný dlouhodobý plán (v němž řeší i případné otázky nástupnictví) a sledovat okolí kvůli změnám.

Podskupina *Organizační struktura a personální zajištění* (4 kritéria) říká, že úložiště má dány úkoly, pro něž má k dispozici dostatek kvalifikovaných pracovníků včetně plánu jejich rozvoje.

Podskupina *Procesní zodpovědnost a rámec pravidel pro uchovávání* (7 kritérií) úložišti ukládá stanovit veřejně cílovou skupinu, zavést pravidla pro uchovávání a pravidelně je aktualizovat, být transparentní, provádět pravidelně sebeevaluaci a dokumentovat změny.

Podle podskupiny *Ekonomická udržitelnost* (3 kritéria) musí úložiště hospodařit udržitelně a transparentně, plánovat krátkodobě i dlouhodobě a všímat si rizik.

Podskupina *Smlouvy, licence a právní odpovědnost* (6 kritérií) praví, že úložiště pracuje s daty na smluvním základě, dodržuje platnou legislativu a má zavedena pravidla, z nichž vyplývá, kdo je za co zodpovědný.

Druhá kategorie *Správa digitálních objektů*[43] obsahuje více než polovinu všech kritérií (60) a skládá se z 6 podskupin:

Podskupina *Příjem: získávání obsahu* (10 kritérií) se zabývá příjmem a vstupními daty, úložiště tedy definuje informační obsah a vlastnosti informací, zpracovává balíčky SIP, včetně kontroly jich samotných a jejich původu, propojuje informace s vkládanými daty, komunikuje s tvůrcem, příp. vkladatelem, a to vše dokumentuje.

Na základě podskupiny *Příjem: vytváření balíčků AIP* (30 kritérií) úložiště vhodně vymezuje a používá typy balíčků AIP, přetváří balíčky SIP na AIP, přiřazuje balíčkům AIP správně nastavené a zaznamenané jedinečné identifikátory a zajišťuje, že data mají správné vysvětlující informace. Dále úložiště dokumentuje a propojuje informace o uchovávání, hlídá autenticitu a integritu balíčků AIP a jejich srozumitelnost pro cílovou skupinu.

[41] Výše je stejná jak pro prvotní certifikaci, recertifikaci, tak i kontrolní audit. Vzhledem k tomu, že do organizace jsou vysíláni dva lidé na dva dny, bude se jednat celkem o čtyři dny. Konečná suma tedy bude čtyřikrát vyšší, tj. 138 240,- Kč (£4.800).

[42] ČSN ISO 16363, kapitola 3, s. 18–27.

[43] Tamtéž, kapitola 4, s. 27–42.

Podskupina *Plánování uchovávání* (6 kritérií) udává, že úložiště má plán uchovávací strategie, sleduje jak vnější, tak vnitřní změny, je na ně připraveno (má tedy připravené příslušné plány) a dokládá vhodnost jeho činnosti.

Podskupina *Uchovávání balíčku AIP* (6 kritérií) úložišti ukládá, aby stanovilo způsob uložení balíčků AIP až na úroveň jednotlivých bitů, sleduje integritu, vede záznamy o nakládání s balíčky a ideálně má popsané způsoby práce s balíčky, dle nichž se řídí.

V podskupině *Správa informací* (4 kritéria) úložiště musí doložit, že vzájemně propojuje balíčky AIP se základními popisnými informacemi, které stanovilo s ohledem na cílovou skupinu.

Poslední podskupina *Řízení přístupu* (4 kritéria) nařizuje, že úložiště se řídí pravidly pro zpřístupňování, zaznamenává chyby, reaguje na ně a poskytuje data hodnověrně a tak, aby šlo dohledat původní dokumenty.

Poslední kategorii *Infrastruktura a řízení bezpečnostních rizik*[44] tvoří dvě podskupiny celkem o 24 kritériích:

Podskupina *Řízení rizik technické infrastruktury* (20 kritérií) praví, že úložiště sleduje rizika a reaguje na ně, používá monitor technologických změn a novinek, kontroluje hardwarové i softwarové technologie a v případě potřeby je mění, má odpovídající technologie pro cílovou skupinu a zálohování, dokumentuje ztráty dat, má stanovené klíčové procesy, dle nichž pracuje, a vhodně spravuje vícenásobné synchronizované kopie.

Dle podskupiny *Řízení bezpečnostních rizik* (4 kritéria) úložiště analyzuje všechna možná rizika související s daty, systémem, zaměstnanci a fyzickými zařízeními a je na ně připraveno, má vymezené role zaměstnanců a plány pro případ živelné pohromy a následné obnovy a alespoň jedny takové plány spolu s kopií dat jsou uloženy mimo pracoviště.

V příloze A,[45] jež má pouze informativní, nikoli závazný charakter, se ještě rozvádějí bezpečnostní otázky vztahující se k samotnému procesu auditu a certifikace. Konstatuje se zde, že se nabízejí dvě možná rizika: že audit bude provádět nepovolaná osoba se zlými úmysly, a proto bude úložiště podvedeno, nebo že při auditu dojde, ať už omylem či schválně, ke zveřejnění citlivých dokumentů, čímž může být poškozena bezpečnost či pověst úložiště, a tím i jeho důvěra. Nicméně norma je pouze označuje jako znepokojivé, ale konkrétní řešení nenabízí, neboť to není jejím předmětem.

V současné době získaly certifikaci dle ISO 16363 pouze dvě instituce. V listopadu 2017 ji získala Indira Gandhi National Centre for the Arts pro Národní kulturní audiovizuální archiv[46]. Certifikace ovšem propadla v červnu 2020 a už nebyla obnovena.[47] Druhou instituci představuje United States Government Publishing Office, jenž byl certifikován v prosinci 2018, v prosinci 2021 tedy doběhl tříletý cyklus a mělo by proběhnout obnovení.[48]

1.5. Akreditace certifikační autority dle NABCB

Jak bylo již zmíněno, certifikační autorita potřebuje nejprve získat akreditaci, aby mohla udílet certifikáty. Příkladem akreditační autority, která je oprávněná vydávat akreditace

[44] Tamtéž, kapitola 5, str. 43–51.

[45] Tamtéž, str. 52.

[46] Certified Clients, Primary Trustworthy Digital Repository Authorisation Body Ltd, online: http://www.iso16363.org/iso-certification/certified-clients/ [PTAB, 3. února 2022]

[47] Stále mají na webových stránkách prohlášení, že jsou certifikovaným úložištěm dle ISO 16363:2012. Viz: https://ncaa.gov.in/repository/ [Indira Gandhi National Centre for the Arts, 3. února 2022]

[48] Certified Clients, Primary Trustworthy Digital Repository Authorisation Body Ltd, online: http://www.iso16363.org/iso-certification/certified-clients/ [PTAB, 3. února 2022]

v oblasti digitálních úložišť, je indický Národní akreditační výbor pro certifikační autority (National Accreditation Board for Certification Bodies, NABCB),[49] který byl zřízen indickou vládou pro vlastní potřeby, který však funguje i pro zahraniční klienty a který akreditoval organizaci PTAB. Byl proto vzat jako příklad.

Akreditační proces je složitější než certifikační. Je postaven na obecné normě ISO 17021 a dalších, které se váží již ke konkrétnímu oboru (v našem případě se jedná ISO 16919). Žádat o ni mohou jen organizace, které jsou schopny žalovat a které je možno žalovat, které již nějakou dobu existují a provedly předtím interní audit.[50] Taková organizace nejprve podá žádost, u níž jsou jasně stanoveny požadavky na formu a na zahrnuté dokumenty, na sekretariát NABCB, jenž zjistí další potřebné informace a rozhodne se, zda se vůbec začne s vlastním procesem. V případě, že se rozhodne pokračovat, připraví plán akreditace a předběžný odhad nákladů, určí počet svědků a sestaví hodnotící komisi (Assessment Team). Vlastní hodnotící proces se skládá ze tří fází: hodnocení dokumentů, hodnocení na místě a hodnocení pomocí svědků.[51]

Při hodnocení dokumentů se procházejí doručené dokumenty a komise si může vyžádat další potřebné nebo chybějící. Pokud touto fází projde organizace v pořádku, dochází k auditu na místě. Při něm se zjišťuje faktický stav a stupeň souladu. Navštěvuje se jak sídlo a centrum organizace, tak i všechny pobočky. Komisaři mají právo nahlížet do dokumentů, pořizovat záznamy apod. Dopadne-li i tato fáze uspokojivě, následuje hodnocení pomocí svědků, při němž jsou vyzpovídáni klienti dané organizace. Na konci každé fáze je vypracována závěrečná zpráva, kterou musí schválit i žádající organizace. Na úplném konci vznikne ještě souhrnná závěrečná zpráva. Celý proces by neměl trvat déle než rok.[52]

O udělení akreditace rozhoduje akreditační komise. Při rozhodování se opírá o materiály od organizace, dokumenty od hodnotící komise i vlastní zdroje (může třeba využít služeb externího odborníka). Schválit či odmítnout akreditaci musí jednohlasně. V případě, že ji udělí, dostane organizace dokumentaci k akreditaci včetně grafiky, pro jejíž použití platí zvláštní pravidla (např. musí být uveden kód akreditace).[53]

Prvotní akreditace platí na tři roky, opakované akreditace na čtyři.[54] Zároveň je třeba každý rok provést kontrolní hodnocení (surveillance assessment), které nejde úplně do hloubky (neprochází se všechny pobočky atd.), menší nesoulady pomíjí, ale u těch větších zahajuje řízení, aby došlo k jejich nápravě. Opakovaná akreditace (Reaccreditation) funguje stejně jako prvotní akreditace s tím rozdílem, že je možné už na něco navázat.[55]

Nesoulady (Noncorformities) jsou rozděleny do tří kategorií. Kritické nesoulady (critical noncorformities) by vážně ohrožovaly proces certifikace, poškozují důvěryhodnost organizace nebo jsou proti zákonu a na jejich opravu má organizace 30 dní. Vážné nesoulady (major noncorformities) by ohrožovaly proces certifikace (ale ne tolik jako kritické), nemají základ v systémové chybě (na rozdíl od kritických) a opraveny mají být do 60 dnů. Poslední vedlejší nesoulady (minor noncorformities) by měly jen zanedbatelný dopad na proces certifikace a vyřešit se mají v co nejkratší době (nejdéle však do 90 dnů). U všech typů jsou nejvýše dva

[49] Její webové stránky: http://nabcb.qci.org.in/ [NABCB, 19. února 2022]

[50] Accreditation Procedure for Management Systems Certification Bodies, NABCB 2021, s. 4 a 5, online: http://nabcb.qci.org.in/documents/BCB%20201%20(MS)%20-%20Accreditation%20Procedure%20for%20MS_Mar%202021.pdf [NABCB, 16. února 2022]

[51] Tamtéž, s. 6–9 a 12.

[52] Tamtéž, s. 12–19.

[53] Tamtéž, s. 19 a 20.

[54] Tamtéž, s. 9.

[55] Tamtéž, 21 a 22.

pokusy na opravu. Vedle nesouladů jsou ještě zmíněny obavy (concerns), jež sice nejsou přímo nesouladem, nýbrž se jím mohou snadno stát, případně se jím určitě stanou, pokud o ně nebude postaráno.[56]

Poplatky za akreditaci[57] počítají přirozeně především s Indií, v případě tamních organizací stanovují cenu podle jejich ročního obratu. U zahraničních zemí rozlišují organizace ze zemí SAARC[58] a mimo ně. Zde zmíněné hodnoty jsou platné pro země mimo SAARC. Za žádost se u prvotní, resp. další, akreditace platí 71 900,- Kč (250 000 INR), resp. 35 950,- Kč (125 000 INR).[59] Náklady na jednoho člověka na den představují 19 552,- Kč ($800).[60] Roční poplatek za akreditaci je ve výši 43 140,- Kč (150 000 INR) u prvotní či u následujících 35 950,- Kč (125 000 INR). Organizace platí za každý vystavený certifikát od 14 380,- Kč (500 INR) do 28 760,- Kč (1 000 INR).[61] V případě, že organizace získá akreditaci pro další oblast, neplatí plnou sazbu, nýbrž pouze poplatek za rozšíření ve výši 143 800,- Kč (5 000 INR). Nakonec se platí i cestovné, jehož výše závisí na aktuální situaci. Zajímavostí může být, že při cestě delší než šest hodin jednak cestují komisaři business třídou, jednak se hradí i čas strávený na cestách třiceti procenty cestovného.[62] Pokusíme-li se sečíst ceny, dostaneme, že poplatky za prvotní akreditaci začínají minimálně na 310 000,- Kč, je do nich zahrnuta cena za žádost a roční poplatek a dále 11 pracovních dní.[63] Pracovních dní bude nejspíš víc a náklady velmi vzrostou proplácením cest, proto konečná suma bude určitě mnohem vyšší.

1.6. Závěr

V nastíněných možnostech certifikace jsou patrné značné rozdíly, ať už v počtu podmínek, možných úrovních plnění jednotlivých kritériích nebo požadavcích na předkládané dokumenty. Core Trust Seal představuje nejjednodušší možnost certifikace pouze o 16 podmínkách. Z podmínky R0 vyplývá, že je určen různým druhům institucí, nejen archivům, a podíváme-li se na instituce, které certifikaci získaly, zjistíme, že jsou mezi nimi skutečně zastoupeny digitální knihovny, datová centra výzkumných institucí a mnohé další typy. Certifikace Core Trust Seal je časově omezená a pro její udělení stačí vnitřní hodnocení.

Pečeť nestoru s 34 podmínkami je již složitější, o čemž svědčí i fakt, že ji získaly pouze čtyři instituce, buď knihovny, nebo informační centra.[64] Na rozdíl od Core Trust Seal u Pečeti nestoru dochází k přísnějšímu hodnocení a platí po neomezenou dobu. Nejkomplexnější možnost certifikace představuje certifikace dle normy ISO 16363, jež přichází se 109 požadavky. Vyžaduje složitý průběh hodnocení, který zahrnuje jak interní, tak externí audit. Ten se navíc musí průběžně opakovat, aby certifikace nepropadla. Složitost certifikace dokládá i to, že certifikovány byly pouze dvě instituce. Velký rozdíl oproti předchozím

[56] Tamtéž, oddíl 9. Assessment findings (Noncorformities/Concerns) and Corrective Actions, s. 26–28.

[57] Fee Structure for Management Systém Accreditation (QMS, EMS, FSMS, OHSAS, ISMS, ITSMS, EnMS, RTSMS, TDRMS, BCMS & ABMS), NABCB 2018, online: http://nabcb.qci.org.in/pop/BCB%20F002%20-%20Fee%20Structure%20-%20MS.pdf [NABCB, 16. února 2022]

[58] Jihoasijská asociace pro regionální spolupráci (South Asian Association for Regional Cooperation, SAARC.) Jedná se o spolek devíti jihoasijských států, např. Afganistán, Indii nebo Maledivy.

[59] Kurz 100 Rs (indických rupií, INR) = 28,76,- Kč dle ČNB k 19. únoru 2022.

[60] Kurz $1 = 21,44,- Kč dle ČNB k 19. únoru 2022.

[61] Výše se určuje podle počtu vydaných certifikátů.

[62] Tamtéž, s. 1.

[63] Počet pracovních dní je přibližně určen v Accreditation Procedure…, Annex 2, s. 33, NABCB 2021.

[64] Je nutné zmínit, že nižší počet certifikovaných institucí je také způsoben tím, že Pečeť nestoru je omezena především na německé jazykové prostředí.

možnostem tvoří skutečnost, že pro získání certifikace dle normy ISO je nutno zaplatit výrazný poplatek.[65]

Core Trust Seal se pro potřeby archivnictví jeví jako až moc obecné, o čemž svědčí velká různost certifikovaných institucí a nízký počet podmínek. Jako nevýhodu lze vnímat i to, že je certifikát vydán na základě vnitřního hodnocení, takže jeho výpovědní hodnota není tak vysoká jako u zbylých dvou možností. Norma ISO naopak představuje nástroj, jehož splnění by sice bylo ideálem, neboť vše popisuje detailně a dopodrobna, proces certifikace je prováděn důkladně, přičemž zahrnuje sebeevaluaci i externí audit. Je ovšem otázka, zda není pro archivy tato varianta až příliš složitá a snaha o její splnění i udržení (faktické i finanční) by nespotřebovala zdroje a síly, které by bylo radno investovat jinam.

Nejlepší východisko tak představuje Pečeť nestoru, jež přichází s rozumným počtem požadavků. Bylo by ale dobré, aby si k ní archivy přidaly závazek, že ji po jisté době[66] získají znovu, neboť sama o sobě časově omezená není.

[65] Poplatek za prvotní audit začíná na půl milionu. Za pečeť nestoru se platí 12 170,- Kč.

[66] Takovou dobu není v prostředí neustále se měnících technologií možné pevně určit. Domníváme se však, že by nikdy neměla přesáhnout deset let. Ideálně by měl audit proběhnout při výrazné změně v technologiích či zavedených postupech.

2. Akreditace digitálního archivu dle archivního zákona

V českém archivnictví existuje na základě §60a archivního zákona (dále také jako AZ) možnost akreditace digitálního archivu, která v tomto případě představuje oprávnění k ukládání archiválií v digitální podobě. V jejím rámci dochází podobně jako u výše popsaných certifikačních nástrojů k hodnocení vybraných kritérií, a navíc ještě ke zkušebnímu přenosu dat do Národního archivu. To vše proto, aby byla zajištěna skutečně dlouhodobá ochrana a čitelnost dat, a to i v případě zániku digitálního archivu. Hlavními východisky je v tomto případě archivní zákon (§ 18b, § 18c, § 60a, § 60b, § 60c a § 61 odst. 2 a 4) a již zmíněný metodický návod č. 2/2022 odboru archivní správy a spisové služby Ministerstva vnitra pro akreditaci digitálního archivu.

2.1. Proces akreditace

Požádat o udělení akreditace může ten, kdo již má akreditovaný archiv,[67] nebo lze žádost o akreditaci digitálního archivu spojit s žádostí o akreditaci archivu.[68] Digitální archiv tedy nesmí existovat bez akreditovaného archivu.

Osoba, která chce zřídit akreditovaný digitální archiv, podává Ministerstvu vnitra[69] žádost o udělení oprávnění k ukládání archiválií v digitální podobě. Ta musí splňovat jednak obecné náležitosti podle správního řádu, jednak musí obsahovat konkrétní informace vztahující se k akreditaci. Mezi obecné náležitosti podle správního řádu patří jasné uvedení, kdo žádost podává, včetně jeho identifikace,[70] čeho se žádost týká, označení Ministerstva vnitra (jakožto orgánu, kterému je žádost určena) a podpis.[71] Konkrétní požadavky vztahující se k akreditaci představují název a adresa sídla archivu a úložišť, podklady pro zhodnocení stavebně-technických a bezpečnostních podmínek, popis způsobu uložení digitálních archiválií, koncepci dlouhodobého uložení a ochrany, identifikaci digitálních archiválií, seznam metadat používaných k popisu a evidenci, návrh provozního řádu digitálního archivu a potvrzení Národního archivu o úspěšné zkoušce přesunu digitálních archiválií.[72]

Ministerstvo vnitra samostatně rozhoduje jen v otázkách názvu a adresy sídla archivu a úložišť a podkladů pro zhodnocení stavebně-technických podmínek. U zbylých požadavků je vyžadován závazný souhlas Národního archivu, jehož stanovisko musí být pro všechny z nich kladné.[73] Na vydání rozhodnutí má Ministerstvo vnitra jeden rok.

O akreditaci může digitální archiv přijít, pokud o to jeho zřizovatel požádá, nebo o tom rozhodne Ministerstvo vnitra. V případě, že digitální archiv neplní stanovené podmínky, Ministerstvo vnitra mu určí lhůtu pro napravení situace. Když ani po dané době nedojde k nápravě, Ministerstvo vnitra akreditaci odebere. Zřizovatel bývalého digitálního archivu se má domluvit, kam digitální archiválie přemístí. Nedohodne-li se s žádným digitálním archivem, převezme digitální archiválie Národní archiv.[74] V případě, že by stávající zřizovatel digitálního archivu zanikl, nepřechází akreditace na jeho případného právního nástupce.[75]

[67] Akreditace archivů je upravena § 58 AZ.

[68] § 60a odst. 1 AZ.

[69] V rámci Ministerstva vnitra je pro otázky archivnictví a spisové služby, tedy i pro akreditaci (digitálních) archivů příslušný Odbor archivní správy a spisové služby.

[70] U fyzické osoby např. příjmení, adresa. U právnické osoby název, IČO, adresa sídla apod.

[71] § 37 odst. 2 zákona č. 500/2004 Sb., správního řádu.

[72] § 60a odst. 2 AZ.

[73] § 60a odst. 3 AZ.

[74] § 60b AZ.

[75] § 60c odst. 2 AZ.

2.2. Struktura a obsah dokumentace

V metodickém návodu pro akreditaci digitálního archivu je nastíněna doporučená struktura a obsah žádosti.[76] Jako východisko je přitom použita Pečeť nestoru. Rozlišují se tři skupiny požadavků.

První skupinu představuje koncepce dlouhodobého uchovávání a ochrany dokumentů, které se mají dostat do archivu. Z kritérií nestoru sem spadají kritéria K1 až K13 a K34. Všechna jsou označena jako zcela zásadní a je vyžadováno jejich úplné zpracování a začlenění do běžného provozu.[77]

Do druhé skupiny se řadí popis způsobu uložení digitálních archiválií. Odpovídají jí kritéria K14 až K20 a K33. K33 musí být plně zavedeno. Ostatní rovněž, případně se mohou nalézat ve stadiu konkrétního konceptu a zavádění do provozu.[78]

Poslední třetí skupinu tvoří seznam metadat k popisu archiválií a evidenci archivních souborů a popisů původců. V Pečeti nestoru se jedná o kritéria K21 až K32. Kritéria musí být buď plně zavedena, nebo již začleňována do běžné praxe.[79]

Porovnáme-li požadavky Pečeti nestoru a české akreditace digitálního archivu, zjistíme rozdíly. Pečeť nestoru rozlišuje čtyři úrovně plnění požadavků a umožňuje v některých případech (mimo klíčové podmínky) jejich prominutí. Česká akreditace dovoluje pouze dvě úrovně plnění požadavků, tj. detailní koncept, který je zaváděn do procesu, nebo plnou implementaci. Tyto úrovně odpovídají stupňům plnění za 6 a 10 bodů u Pečeti nestoru. Pečeť nestoru za klíčové označuje kritéria K1 až K12, přičemž u každé z nich vyžaduje splnění na 10 bodů. Česká akreditace k takovým kritériím přidává ještě K33 a K34 (IT infrastrukturu a bezpečnost). Požadavky české akreditace jsou tedy přísnější než Pečeť nestoru.

K doložení, že archiv podmínky splňuje, musí prokázat celou řadu skutečností. U první skupiny se jedná o mandát archivu, popsání cílových skupin, odpovědnost za uchovávání, plán financování, vhodný počet a typ zaměstnanců, vhodnou organizační strukturu, připravené krizové řízení, zpracovanou bezpečnost, zajištění přístupu a čitelnosti k uchovávaným datům a plánování uchovávání.[80]

U druhé skupiny je potřeba popsat fungování jednotlivých součástí digitálního úložiště a IT infrastrukturu ve všech úrovních (od rozvodů po software) a prokázat, že archiv má všechna potřebná technická oprávnění k práci s archiváliemi.[81]

Splnění třetí skupiny se dokládá dostatečnou specifikací metadat, popsáním balíčků SIP, AIP a DIP a převodů mezi nimi. Dále se musí zajistit čitelnost jednotlivých balíčků a mají být zaznamenány všechny postupy, jež souvisí s uchováváním.[82]

Kromě těchto tří skupin vycházejících z Pečeti nestoru je zmiňována ještě skupina vycházející z požadavků archivního zákona na portál digitálního archivu a správu metadat. Digitální archiv má mít zřízený portál pro zpřístupnění archiválií, jehož prostřednictvím je umožněn dálkový přístup jak pro výběr a příjem digitálních archiválií včetně metadat, tak pro přístup k nim, případně k digitalizátům analogových archiválií.[83] Digitální archiv ještě

[76] Metodický návod č. 2/2022 odboru archivní správy a spisové služby Ministerstva vnitra pro akreditaci digitálního archivu, str. 4–7.

[77] Tamtéž, str. 4 a 5.

[78] Tamtéž, str. 5.

[79] Tamtéž, str. 5.

[80] Tamtéž, str. 6.

[81] Tamtéž, str. 6 a 7.

[82] Tamtéž, str. 7.

[83] § 18b odst. 2 a 5 AZ.

shromažďuje, vytváří a spravuje metadata sloužící k identifikaci a popisu archiválií a evidenci přístupových práv k nim, ve spolupráci s Národním archivem má na starosti evidenci Národního archivního dědictví, popis a evidenci původců a archivu a případných kulturně vědeckých institucí a ukládá spisové a skartační plány. Všechny tyto informace a metadata zpřístupňuje skrz portál s funkčním vyhledávacím systémem a správně nastavenými přístupovými právy. V případě, že by digitální archiv uchovával archiválie jiného archivu, musí mu dálkově zpřístupnit údaje o změnách nebo poškozeních archiválie.[84] K doložení, že zákonné požadavky splnil, potřebuje digitální archiv jednak dokumentaci použitých řešení, jednak musí jejich použití ukázat v praxi.[85]

2.3. Zkušební přenos digitálních archiválií

V rámci procesu akreditace musí digitální archiv provést zkušební přenos digitálních archiválií do Národní archivu. Tato podmínka je vyžadována kvůli tomu, aby byla zajištěna čitelnost dat Národním archivem, jenž v případě, že digitální archiv zanikne, data převezme.

Přenos konkrétně popisuje příloha č. 2 metodického návodu pro akreditaci digitálního archivu. Jejím základem je stanovit datovou strukturu takovou, aby byla snadno zpracovatelná, přenositelná a nezávislá na hardwaru i softwaru. Jako nejvhodnější jsou označeny dvě specifikace vyšlé z projektu E-ARK (European Archival Records and Knowledge Preservation). Specifikace CSIP (Common Specification for Information Packages) upřesňuje společné vlastnosti balíčků SIP, AIP i DIP. Specifikace AIP (Archival Information Package) rozšiřuje CSIP pro použití u balíčků AIP.[86]

Základní podoba balíčku je stanovena tak, že se jedná o soubor ve formátu ZIP, který obsahuje kořenovou složku. Jak složka, tak balíček jsou pojmenovány pomocí UUID (Universally Unique Identifier), které je odlišné pro každý balíček. V kořenové složce se nachází tři podsložky a soubor *mets.xml*, který popisuje strukturální metadata celého balíčku. V podsložce *metadata* se nalézají popisná[87] a uchovávací metadata. Složka *representations* obsahuje vlastní reprezentace dat. Složka *submission* kopíruje strukturu balíčku a jsou v ní obsažena použitá schémata.[88]

Je vidět, že téma zkušebního přenosu není zcela popsané a zmapované a že je stanoven pouze jeho obecný rámec. Jedním z důvodů může být fakt, že požadavek zkušebního přenosu je poměrně nový a nebyl tedy ještě pořádně vyzkoušen v praxi. Další důvod by mohla představovat samotná data, jež budou zkušebně přenášena. Ta totiž mohou nabývat různých podob, velikostí, struktury nebo počtu. Různý přístup by vyžadoval např. spis, rozsáhlá databáze nebo fotodokumentace různých akcí. Dá se předpokládat, že ke každému typu uchovávaných dat je potřeba přistupovat individuálně a že k případnému zobecnění ještě nejsou potřebné zkušenosti.

[84] § 18c odst. 2, 3, 4, 5 a 6 AZ.

[85] Metodický návod č. 2/2022 odboru archivní správy a spisové služby Ministerstva vnitra pro akreditaci digitálního archivu, str. 7.

[86] Příloha č. 2 metodického návodu č. 2/2022 odboru archivní správy a spisové služby Ministerstva vnitra pro akreditaci digitálního archivu, str. 1.

[87] Popisná metadata musí zohlednit vyhlášku č. 645/2004 Sb., kterou se provádí zákon o archivnictví a spisové službě, a musí být v souladu s formátem EAD3. Jejich přehled se nachází na str. 2 a 3 přílohy č. 2 metodického pokynu pro akreditaci digitálního archivu.

[88] Tamtéž, str. 1 a 2.

2.4. Stavebně-technické podmínky

Bližší určení stavebně-technických a bezpečnostních podmínek se nachází v § 61 odst. 2 a 4 AZ. Ještě konkrétněji jsou rozvedeny v příloze č. 1 metodického návodu č. 2/2022 pro akreditaci digitálních archivů, v níž jsou ještě uvedeny způsoby, jimiž se jejich splnění dokládá.

Do stavebně-technických podmínek spadají požadavky jak na samotnou budovu, tak i na její umístění. Budova má být umístěna mimo záplavová území, ochranná pásma letišť a oblasti s plynným a prachovým znečištěním. Prostory, v nichž jsou uloženy archiválie, musí být chráněny tak, aby vlivy způsobené přírodou či člověkem (např. působení fyzikálních jevů nebo průnik vody), nezpůsobily zničení archiválií. Dále se musí nalézat nad hladinou spodní vody, mít zajištěné větrání k udržení vhodné teploty a relativní vlhkosti vzduchu a přístroje k jejich měření. Úložiště, kde jsou umístěny archiválie s magnetickým záznamem, musí být chráněna před účinky elektromagnetického pole. Zároveň má mít digitální archiv minimálně dvě plnohodnotná úložiště, jež se od sebe nachází vzdušnou čarou minimálně 50 km a jež jsou zároveň umístěna na takových místech, která vylučují možnost, aby se týž umělý či přírodní jev, který by případně ohrozil archiválie nebo znemožňoval záchranné práce, projevil současně nebo následně na obou z nich.[89]

Aby byly splněny tyto požadavky, je nutné doložit, že pozemek byl posouzen z hlediska radonového rizika. V případě, že leží blízko vodního toku, je ještě potřeba vyjádření příslušného orgánu a v případě, že se nachází v ochranném pásmu letišť, je nutný souhlas Úřadu pro civilní letectví. Fakt, že v datových sálech riziková potrubí chybí nebo jsou zabezpečena proti průnikům, se dokazuje stavební dokumentací[90] a záznamem pověřeného pracovníka ministerstva. Stavební dokumentace se také používá pro dokázání, že jsou podzemní podlaží umístěna nad hladinou spodní vody, že jsou místa s digitálními archiváliemi vybavena přepěťovou ochranou, že jsou chráněna před statickým nábojem a negativním působením elektromagnetického pole a že je v nich instalován zdroj a rozvod chladu. Dále je nutný snímek části územního plánu obce se záznamem pracovníka ministerstva, aby se prokázalo, že se blízko úložiště nenachází chemické či biologické provozy. K doložení, jakým způsobem je úložiště větráno a že je vybaveno přístroji k měření teploty a relativní vlhkosti vzduchu, slouží záznam pracovníka ministerstva, certifikát ventilačního nebo klimatizačního systému a záznamy o naměřených hodnotách. Dále je potřeba doložení stavebního řešení a zpráva o revizi hromosvodu a uzemnění kvůli ochraně před účinky blesku. Nakonec je ještě nutný výpis ze stavební dokumentace užitného zatížení a výpis z mapy o umístění dalšího plnohodnotného úložiště.[91]

2.5. Bezpečnostní podmínky

Mezi bezpečnostní podmínky patří požadavek na zpracování bezpečnostní dokumentace, v níž se řeší jak ochrana před vnikem nepovolaných osob, krádežemi a teroristickými útoky, tak i požární dokumentace. V archivu musí být elektronická požární signalizace a ruční hasicí přístroje.[92] V přízemí, prvním a druhém podlaží a místech, kde by bylo možné se do budovy

[89] § 61 odst. 2 AZ.

[90] Stavební dokumentace současně dokládá i základní části archivního pracoviště, jako je místnost operátorů, diskovna, umístění záložního agregátu a d.

[91] Příloha č. 1 metodického návodu č. 2/2022 odboru archivní správy a spisové služby Ministerstva vnitra pro akreditaci digitálního archivu, str. 1–2.

[92] V místech, kde jsou uloženy archiválie, smějí být pouze práškové hasicí přístroje.

dostat zvenku či kde je rozhraní mezi veřejně přístupnou a nepřístupnou částí, se mají nasadit mechanická a elektronická zabezpečovací zařízení. U klíčů od vstupů do budovy je záhodno, aby se o jejich výdej a vracení staral pověřený zaměstnanec. V případě, že je vstup do archivu realizován elektronickým systémem, musí být vhodně nastavena přístupová práva zaměstnanců.[93]

K doložení, že jsou tyto podmínky splněny, je potřeba zpracovat bezpečnostní dokumentaci, která bude potvrzena pracovníkem ministerstva. Výpisem ze stavební dokumentace, příslušnými certifikáty a ověřením ze strany ministerstva se dokládá stabilní i záložní elektrické napájení[94] a mechanická a elektronická zabezpečovací zařízení,[95] do nichž spadá i detekce neoprávněných přístupů na střechu, do serverovny atd. K prokázání, že je zajištěno stabilní internetové připojení, stačí kopie smlouvy s poskytovatelem internetového připojení. Do protipožární ochrany spadá zpracovaná požární dokumentace, použití elektrické požární signalizace (EPS), hasicí přístroje a samočinné hasicí zařízení. Jejich existence a používání se dokládá kopií kolaudačního protokolu, kopií požárně bezpečnostního řešení stavby, kopií revizních zpráv o kontrole hasicích přístrojů a systémů EPS a samočinného hasicího zařízení (spolu s certifikátem obou systémů) a záznamem o provedení preventivní požární prohlídky. Zda jsou přístupová práva pro vstup do archivu nastavena vhodně, se prokazuje buď kopií příslušné směrnice archivu, nebo záznamem pracovníka ministerstva.[96]

Pokud by uvedené podmínky nebylo možné splnit, existuje ještě možnost provést analýzu rizik. V případě, že by míru rizika šlo akceptovat, je možné takové místo pro archiv použít.[97]

Do bezpečnostních podmínek ještě spadá oblast kybernetické bezpečnosti, jejímž hlavním východiskem je zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Zřizovatel archivu se musí zařadit do správné skupiny podle § 3 téhož zákona a splnit požadavky, které vyplývají z jeho zařazení. Aby tyto skutečnosti doložil, stačí, aby vydal čestné prohlášení.

2.6. Závěr

Dosud k akreditaci digitálního archivu podle archivního zákona nedošlo. Do roku 2019 se o akreditaci digitálního archivu pokusil jeden specializovaný archiv, ale neuspěl.[98] V roce 2021 byla zamítnuta žádost VHA o akreditaci Digitálního archivu Ministerstva obrany (DAMO). Další archivy o akreditaci digitálního archivu uvažují. Akreditovat digitální archiv nemusí bezpečnostní archivy a Národní archiv, poněvadž bezpečností archivy ji získávají ze zákona[99] a Národní archiv je ze zákona příslušný pro uložení digitálních archiválií.[100]

Možnost akreditace digitálního archivu se objevila v roce 2012, kdy byl novelizován archivní zákon zákonem č. 167/2012 Sb., jenž spolu s ním změnil zákon o elektronickém podpisu a celou řadu dalších souvisejících zákonů. V archivním zákonu se tak objevila nebo byla upravena řada ustanovení, na které zde bylo odkazováno. Nově přibyly odst. 3 v § 15, § 18b, § 18c a § 60a až § 60c. Změněny byly podmínky upravené v § 61 odst. 2 a 4.

---

[93] § 61 odst. 4 AZ.

[94] Jejich základem je dostatečná přípojka, kvalitní a vhodné rozvody a ochranné prvky (jističe a další) a nepřerušitelný zdroj napájení.

[95] Prakticky se jedná např. o kamerové systémy nebo poplašná zařízení.

[96] Příloha č. 1 metodického návodu č. 2/2022 odboru archivní správy a spisové služby Ministerstva vnitra pro akreditaci digitálního archivu, str. 3.

[97] Tamtéž, str. 4.

[98] Bernas, Stodůlka, Vojáček: *Certifikace NESTOR* in: LTP 2019.

[99] § 60a odst. 5 AZ.

[100] § 15 odst. 3 AZ.

Metodický návod Ministerstva vnitra pro akreditaci digitálního archivu byl vydán až roku 2019, aby posloužil jako návod pro případné zájemce o akreditaci.[101] V únoru 2022 byla uveřejněna jeho druhá verze.

[101] Bernas, Stodůlka, Vojáček: *Certifikace NESTOR* in: LTP 2019.

3. Specifika archivnictví a vhodnost certifikačních nástrojů

Výše popsané možnosti auditu a certifikace lze použít i v jiných oblastech než jen v archivnictví. Úložiště pro dlouhodobou ochranu digitálních dokumentů nalézají své uplatnění u vědeckých pracovišť, v komerční sféře i u dalších paměťových institucí, mezi nimiž mají knihovny v této oblasti nejvýznamnější postavení.[102]

Tato kapitola se pokouší pojmenovat a více rozvinout některá specifika, která jsou vlastní jen archivnictví a oddělují jej tak od jiných, zejména paměťových, institucí. V poslední části se věnuje otázce vhodnosti auditních a certifikačních nástrojů pro archivářskou oblast. Rozhodně se nejedná o vyčerpávající přehled a pojednání, nýbrž spíše o nástin a rozvedení některých skutečností.

3.1. Velká šíře dat

Základní rozdíl mezi archivy a dalšími institucemi tvoří rozdíl v šíři ukládaných dat. Ta se projeví při všech fázích archivace, tedy již na vstupu do instituce. Např. u knihoven lze předpokládat, že do ní budou ukládány publikace, které vznikly digitalizací či rovnou bez analogové předlohy a které tak budou mít formu kombinovanou textovou a obrazovou. Jejich další zpracování tak půjde předem snadno odhadnout a snadno realizovat. Rovněž u vědeckých pracovišť se dá očekávat, že budou pracovat s předem stanovenými daty, aplikacemi a formáty. I v tomto případě půjde uložení snadno naplánovat. Do archivů však proudí data velké řady původců, kteří nepředstavují ucelenou skupinu. Může jít o jednotlivce, již si do archivů ukládají své osobní fondy, pracují na různých platformách, v odlišných aplikacích atd. Zpracování jejich pozůstalostí tak bude vyžadovat osobní přístup. Největšími producenty jsou pak státní úřady, které mají za úkol rozličné agendy, jejichž výstupy by měly skončit v archivech. Jenže vedle agend, které si vystačí s „klasickými papírovými“ dokumenty v digitální podobě,[103] existuje celá řada takových, jež produkují specifická a velmi specializovaná data (např. stavební úřady). Takové úřady a agendy potřebují také zvláštní prostředky (programové vybavení či formáty). Takové vstupy budou rovněž často vyžadovat individuální přístup. Objevit se může dokument ve formátu PDF/A, rozsáhlá databáze s údaji, jimž porozumí jen odborník v daném oboru, či soubor s 3D modelem nějakého objektu, soubor v proprietárním formátu, neboť se jedná o tak zvláštní záležitost, že jiný formát v podstatě neexistuje, či třeba zdrojový kód nějaké aplikace.[104]

Se značnou šíří ukládaných dat se archivy budou potýkat i ve fázi vlastního uložení a dlouhodobého uchovávání. Jedním ze způsobů, jak archivy své poslání splní, bude jistě i

[102] Důkazem může být i fakt, že většina závěrečných prací na FF UK, které se dané či podobné problematice (např. digitalizaci) věnují, pochází z Ústavu informačních studií a knihovnictví.

[103] Jimi se myslí soubory statické textové či kombinované textové a obrazové, použije-li se terminologie vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby.

[104] Nemyslí se tím, že archiv je jediné místo, kam se takové soubory dostanou, ale že archiv musí řešit všechny možnosti naráz. Např. muzeum bude pracovat s 3D modely, ale zdrojový kód ho už zajímat nebude. Protože nemá, jak by se do muzea dostal.

formátová standardizace dat.[105] Je však otázka, zda bude možná u všech souborů.[106] Spolu se standardizací vždy hrozí možnost ztráty dat,[107] která se může zvyšovat spolu s tím, že se archivy budou snažit zachovat čitelnost všech dat. Vzhledem k tomu, že kvůli velké různosti dat nebude v moci archivů, aby ke každému druhu přistupovaly individuálně, budou migrovat „specifická" data do formátů, které pro ně nebudou tak vhodné. Informace v nich obsažené tak zůstanou čitelné, ale za cenu možné ztráty některých dat. Dá se očekávat, že jiné instituce se do takové situace nedostanou, protože nebudou mít tak široké rozpětí vkládaných informací.

Kromě migrace a s ní spojené formátové standardizace budou muset archivy řešit i otázky spojené s emulací, neboť se v úložištích jistě vyskytnou i data, která migrovat nepůjde. Oba způsoby uchovávání povedou archiv k tomu, aby sám v daných oblastech prováděl výzkum. O svěřená data, ale i o jejich čitelnost si totiž nemůže dovolit přijít, na rozdíl třeba od komerční sféry. Navíc se u všech druhů dat nelze spoléhat, že za nějakou delší dobu budou ještě existovat a že v té době tak budou dostupné nástroje pro práci s nimi, či alespoň takové, které je umožní přečíst.

Na straně výstupu se velká šíře nakonec projeví taktéž. Vzhledem k tomu, že do archivu vkládají svá data různí původci, jsou data uložena v různých režimech. Archiválie, jež se do archivů dostaly od státních úřadů cestou skartačního, příp. mimoskartačního, řízení, jsou k nahlížení dostupné většinou 30 let od jejich vzniku.[108] Jiné archiválie ovšem mohou být přístupné rovnou. Existují totiž výjimky, které hranici prohlížení posouvají či ji případně úplně ruší. Např. archiválie, které byly již před vložením do archivu veřejně přístupné, jsou dostupné volně.[109] Do archivu mohou uložit dokumenty i neveřejné instituce jako depositum, přičemž si režim zpřístupnění nastaví, jak samy budou chtít.[110] Dá se očekávat, že zvlášť v případě soukromé či vědecké sféry nebude různost režimů zpřístupnění tak velká.

Dalším rozdílem oproti jiným druhům institucí jsou případní zájemci o uložená data. Vzhledem k širokému rozpětí dat, která jsou v archivech uložena, lze předpokládat mnoho cílových skupin. Ty se budou zaměřovat jak na různá data, tak i na různé vlastnosti stejných dat.[111] Z toho důvodu bude nutné promýšlet, jak připravit přístup k archiváliím tak, aby dokázal postihnout skutečně všechny vlastnosti. Nebude tedy možné spolehnout se pouze na jeden způsob zpřístupnění, jelikož např. prostředí pro uveřejnění zdigitalizované knihy nebude vhodné pro zkoumání databáze. Do archivů navíc nepřistupují pouze osoby (ať už fyzické či právnické), příp. vědecké či kulturní organizace, sledující vlastní zájem (jako je tomu v případě knihoven či muzeí), nýbrž se na archivy obrací třeba i orgány činné v trestním řízení v rámci plnění svých povinností. Pro ně platí zase jiná pravidla přístupu.

---

[105] Formátová standardizace zhruba znamená, že se data stejné formy převedou do jednoho univerzálního formátu. Např. všechny zvukové soubory se přemigrují do formátu MP3. Nelze ji použít u všech typů dat, např. zdrojový kód takto převést nelze (ovšem soubor, jenž ho obsahuje, ano).

[106] Tím se nemyslí soubory, u kterých nelze obecně měnit formát (viz poznámka výš), ale soubory s daty, které jsou tak specifické, že vhodnější či nástupnický formát pro ně existovat nebude.

[107] Různé formáty zachycují různé vlastnosti, ačkoli jsou určeny pro stejný typ dat. Např. obrazový formát GIF nezná alfa kanál, neumí tedy různé stupně průhlednosti. Zatímco formát PNG, který je také obrazový, jej zná.

[108] Viz § 37 odst. 1 archivního zákona.

[109] § 37 odst. 1–7 archivního zákona.

[110] Podmínky, jejichž splněním se k takovým archiváliím lze dostat, nabývají různých podob, od pouhého písemného souhlasu až po povinnost pozvat původce na oběd. Může se ale také stát, že přístup k nim umožněn vůbec nebude.

[111] Zatímco jeden badatel bude řešit obsah webových stránek, druhý se zaměří na technologie, kterými byly vytvořeny.

3.2. Možnost ovlivnění vstupních dat

Archivy mají nějaké možnosti a nástroje, kterými mohou podobu vstupních dat ovlivnit či ji přímo ovlivňují. Základem pro ně je skutečnost, že archivy jsou součástí veřejné správy, do níž by se z její činnosti měly ukládat dokumenty s trvalou hodnotou.[112] V tomto systému by tak archivnímu uložení měla předcházet spisová služba, jejíž správné a kvalitní vedení by mělo trvalé uchování značně zjednodušit. Zásadní jsou v této oblasti dvě právní normy. Jedná se o vyhlášku č. 259/2012 Sb., o podrobnostech výkonu spisové služby, a tzv. národní standard.[113] Ve vyhlášce je pro archivnictví důležitý § 23, který definuje výstupní datové formáty pro některé druhy dokumentů.[114] Národní standard, kromě vlastní obsáhlé definice požadavků na elektronické systémy spisové služby, obsahuje přílohy, podle nichž se vytváří a vyměňují balíčky SIP. Ovlivnit spisovou službu archivy mohou ještě skrze předarchivní péči a s ní spojené konzultace, rady a kontroly. Ty však závisí na tom, jak aktivní archiv v této oblasti bude a jak moc bude původce přístupný změnám. Třeba knihovny ale takovou možnost, dokonce legislativně zakotvenou, nemají.

3.3. Spojení vědeckých, kulturních a úředních funkcí

Od ostatních obdobných institucí se archivy i archiváři odlišují také tím, že jejich práce v sobě zahrnuje činnosti jak vědecké, kulturní, tak úřední. V oblasti vědy provádějí výzkum na poli samotného archivnictví, pomocných věd historických, spisové služby a dalších věd, které s jejich působením souvisejí, věnují se otázkám restaurování a konzervování apod. Zároveň se věnují kultuře tím, že pořádají výstavy, přednášky, pečují o (národní) kulturní památky a spolupracují s dalšími organizacemi s podobným zaměřením. Nakonec jsou ale i úřadem, jenž vykonává spisovou službu, provádí výběr archiválií ve skartačním či mimoskartačním řízení, vydává rozhodnutí podle správního řádu a jehož archiváři jsou ve služebním poměru.[115] Toto pro ostatní obdobné instituce neplatí.

3.4. Změna osoby archiváře

Dalším specifikem archivnictví může být i samotná proměna osoby archiváře. Před archivy, tudíž i před archiváře klade digitální doba nové nároky. Archivář na jedné straně stále musí zůstat klasickým archivářem, který ovládá němčinu s latinou, čte novogotické písmo a vyzná se v dějinách jednotlivých institucí. Na druhou stranu se musí vyznat v otázkách spisové služby a právních předpisů, ať už jsou spojeny s otázkami ochrany osobních údajů, nebo se spisovou službou a dalšími záležitostmi třeba souvisejícími s tzv. eGovernmentem. Dále by se hodilo, aby se stal odborníkem na informační technologie, neboť jen formátů je celá řada, ale pro dlouhodobé ukládání jsou vhodné jen některé. Bez příslušných znalostí však neurčí, které to jsou. Vyznat by se měl ovšem i v oboru, od nějž informace do archivu přicházejí,

[112] Fakt, že jsou úložištěm dat s trvalou hodnotou, je samozřejmě společný všem paměťovým institucím.

[113] Plným názvem Národní standard pro elektronické systémy spisové služby (NSESSS). Jeho nynější verze byla zveřejněna ve Věstníku Ministerstva vnitra čá. 57/2017.

[114] Definují se formáty pro soubory statické textové, kombinované textové a obrazové (oboje PDF/A), statické obrazové (PNG, TIFF, JPEG), dynamické obrazové (GIF, MPEG 1, 2 nebo 4), zvukové (MP2, MP3 a WAV), pro databáze a datové věty (XML), pro účetní záznamy v elektronické podobě (ISDOC) a pro metadata souborů z elektronických systémů spisové služby (XML).

[115] Srov. § 46 nebo § 49 archivního zákona.

jinak nebude s to určit vlastnosti, které jsou pro určitý druh dat významné.[116] Aby data zobrazil, může potřebovat speciální programové vybavení, které bude vyžadovat, aby s ním uměl zacházet.[117] Jiné druhy úložišť tak velké nároky nebudou mít, protože jsou více specializované nebo vlastní pracovníci se v daném oboru beze zbytku vyznají (např. u úložišť vědeckých pracovišť).

3.5. Jedinečnost archiválií, autenticita a integrita

Na rozdíl od knihoven vlastní archivy zpravidla limitovaný počet stejných variant jedné fyzické archiválie. Často je daná archiválie jedinečná (např. osobní deník či úřední kniha) a v případě zničení se už nedá nahradit. Knihy vycházejí ve větších nákladech, proto ztráta, příp. zničení, jednoho exempláře nepředstavuje takový problém. Větší počet téhož uchovávaného předmětu výrazně usnadňuje digitalizaci. Knihovna, vlastní-li více výtisků téže knihy, si může dovolit knihu rozešít a skenovat volné listy, což je mnohem rychlejší a efektivnější.

V případě digitálních archiválií nepředstavuje jejich počet výraznější omezení, protože u nich není problém vytvářet identické kopie. Na otázky autenticity a integrity je tak u digitálních archiválií kladen větší důraz, neboť musejí především prokázat, že jsou skutečně tím, za co se vydávají, a že nedošlo k jejich změně. Vzhledem k tomu, že v archivech jsou ukládány dokumenty úřední povahy, které mohou mít velkou právní váhu, budou na archivy kladeny značné nároky i v této oblasti.

3.6. Vhodnost auditních a certifikačních nástrojů

Při řešení vhodnosti auditních a certifikačních nástrojů v rámci archivnictví je dobré začít poznatkem, že archiv skutečně představuje, příp. by měl představovat, úložiště, které je složeno z lidí a ze systémů a jehož cílem je dlouhodobá ochrana a uchovávání digitálních dokumentů. Tudíž splňuje definice kladené auditními či certifikačními nástroji, proto je lze na archivy uplatnit. Archiv je ovšem zároveň něčím víc než jen dlouhodobým úložištěm digitálních dokumentů. Jedná o složitější instituci, jež má za úkol i výzkum, kulturní působení a péči o analogové archiválie. Pro ni takové nástroje už dělané nejsou.

Další otázku představuje sám důvod, proč se audity a certifikace dělají, tj. důvěra. Na jedné straně se jí archivy tradičně těší. Asi málokoho by napadlo, že dokumenty v nich uložené jsou neautentické podvrhy. I v digitální oblasti se zdá, že je důvěra zachována, jelikož data jsou po celou dobu chráněna v rámci spisové služby, z níž plynule přechází do digitálního úložiště. Na druhou stranu by byla velká chyba aplikovat na digitální svět měřítka, která známe z analogového světa. V digitálním světě je pozice autenticity i integrity mnohem vratší. Provést změnu dat tak, aby nebyla poznatelná, je velmi snadné.[118] Proto potřebujeme nástroje, kterými důvěru posílíme.

---

[116] Takové vlastnosti jsou jedním z kritérií pro výběr formátu pro dlouhodobé uložení. Mezi další kritéria patří např. robustnost nebo otevřenost formátu.

[117] Je zřejmé, že archiváři nemůžou všechny role obsáhnout sami. Objevuje se tak nutnost mezioborové spolupráce.

[118] Když budeme chtít na papírový dokument psaný rukou něco připsat tak, aby nové nešlo odlišit od starého, budeme muset použít co nejpodobnější pero a naučit se rukopis autora. Když budeme chtít na tomtéž něco přepsat tak, aby nebylo vůbec poznat, že dokument byl změněn, v domácích podmínkách se to nejspíš nepovede. U digitálního souboru vytvořeném v MS Word, si stačí obstarat aplikaci, která dokáže se stejným typem souboru pracovat, nastavit správně písmo, text vymazat, napsat nový a uložit. Nikdo nepozná rozdíl.

Při používání auditních a certifikačních nástrojů se musí dát pozor, aby se nestaly samoúčelné. Snaha získat certifikát může způsobit, že se archiv zaměří pouze na jednu oblast své činnosti a ostatní vytěsní. Obdržený certifikát potom může vést k „usnutí na vavřínech". To je, zvlášť v digitálním světě, mylný názor. Zároveň ale procesy spojené s auditem a certifikací pomáhají odlišit důležité záležitosti od nepodstatných, uvědomit si vlastní poslání, pojmenovat rizika, a tak posouvají archiv o kousek dál.

Vlastní realizace auditu či certifikace jistě spolyká nějaké prostředky, kterých archivy zase tolik nemají. Nabízí se zde otázka, zda není možné investovat peníze, čas, vědomosti, …, jinak? Lépe? Zda nebude lepší věnovat přes půl milionu Kč, který by jinak šel na certifikaci podle ISO 16363, na vývoj emulátoru, který jednou umožní přečtení dat z nějaké specifické agendy?

Z výše uvedeného vyplývá, že nástroje pro audit a certifikaci jsou vhodné pro to, aby je archivy používaly. Jak už bylo napsáno v závěru první kapitoly, za nejvhodnější se dá považovat Pečeť nestoru, protože Core Trust Seal je až příliš obecná a certifikace podle normy ISO 16363 zase moc nákladná. V českém prostředí lze za nejlepší označit akreditaci digitálního archivu dle §60a archivního zákona. Ta používá Pečeť nestoru a obohacuje ji o další praktické prvky (např. stavebně-technické podmínky). Archivy by se ale v oblasti dlouhodobého uchovávání digitálních dokumentů neměly spokojit pouze s těmito nástroji. Bylo by dobré, aby se aktivně podílely na výzkumu a vývoji v této oblasti, protože se dá očekávat, že u některých typů dat to za ně nikdo neudělá. Podobné audity by se neměly stát jedinými, které archivy absolvují. K dispozici existuje celá řada nástrojů pro další oblasti, např. DRAMBORA pro bezpečnost či model Life pro ekonomické záležitosti.[119] Mimo tyto oblasti by se archivy dle našeho názoru měly zaměřit i na nové oblasti, kde vznikají data, která nikdo nesbírá. Jimi se myslí např. prostředí sociálních sítí a nových médií. Ty získaly v moderním světě nezastupitelné místo a vyskytují se na nich informace, které si dlouhodobé uchovávání jistě zaslouží. Vždyť celá řada institucí má dnes profily na Facebooku či Twitteru, jež jsou spravovány s větší péči než jejich webové stránky či fyzické nástěnky a na nichž se objevují podstatné příspěvky. Zvlášť jednotlivci, kteří mají celospolečenský vliv, se v tomto prostředí pohybují a zanechávají zde materiály, které si zaslouží, aby je budoucí generace zkoumaly.

[119] O nich více ve Fojtů Andrea: *Strategie, návrh, řízení a administrace rozsáhlých digitálních knihoven a archivů*. Praha, 2014. Dizertační práce. Univerzita Karlova, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí práce Papík, Richard, str. 123–135.

Závěr

První kapitola rozebrala podrobně jednotlivé auditní a certifikační nástroje. Core Trust Seal představuje nejjednodušší možnost a zároveň první stupeň certifikace dle Evropského rámce pro audit a certifikaci digitálních repozitářů. Obsahuje pouze 16 zásad rozdělených do tří kategorií a vystačí si s výstupem vnitřního auditu, který následně posuzuje rada. Vzhledem k nenáročnosti je nejvíce rozšířeným typem certifikace. Pečeť nestoru, druhý stupeň certifikace, přichází s 34 požadavky rozdělenými na klíčová kritéria, jež musí být beze zbytku splněna, a ostatní, jejichž plnění není vyžadováno tak striktně. Vychází z německého prostředí, proto nepřekvapí, že všechny čtyři instituce, které ji obdržely, se nacházejí v Německu či Rakousku. I ona nepožaduje externí audit. Třetí stupeň certifikace, certifikace dle normy ISO 16363, je postavena na složitém certifikačním procesu, který zahrnuje jak interní, tak externí audit. K jeho provedení je potřeba najít příslušnou certifikační autoritu. Na rozdíl od ostatních dvou se za ni platí vysoká částka v řádech stotisíců korun. Musí se prokázat plnění celkem 109 kritérií, které jsou rozděleny do tří základních kategorií (Organizační struktura, Správa digitálních objektů a Infrastruktura a řízení bezpečnostních rizik). Zmíněn, spíš pro zajímavost, byl ještě proces akreditace certifikační autority na základně ISO 16919, který opravňuje k provádění certifikace podle ISO 16363. Na závěr bylo řečeno, že jako nejlepší nástroj pro archivnictví se jeví Pečeť nestoru, jež představuje zlatý střed mezi jednoduchou certifikací dle Core Trust Seal a až příliš komplexní certifikací podle ISO 16363.

Tématem akreditace digitálního archivu podle § 60a archivního zákona se zabývá druhá kapitola. Nastíněn byl vlastní proces, který v sobě zahrnuje prokázání, že archiv plní formální podmínky (např. je již akreditovaný podle § 58 nebo se uchází o obě akreditace naráz), vyhovuje stavebním, technickým i bezpečnostním podmínkám, a provedení zkušebního přenosu archiválií do Národního digitálního archivu. I akreditace podle § 60a má vlastní katalog požadavků, který vychází především z kritérií Pečeti nestoru, k nimž jsou přidány podmínky vyplývající z legislativy.

V poslední kapitole, jejímž úkolem bylo pokusit se postihnout specifika archivnictví vůči jiným institucím a vhodnost auditních a certifikačních nástrojů, byla jako hlavní odlišnost označena velká šíře původců dat (od jedinců přes soukromé organizace až po specializované státní úřady), která způsobuje velkou různost dat, které se do archivu nakonec dostanou. Z toho důvodu bude těžké se všemi pracovat tak, aby u nich nedošlo ke ztrátě některých informací či vlastností. Vzhledem k rozmanitosti lze totiž očekávat, že bude docházet ke zjednodušování a zobecňování. Z různosti původců pramení i rozdílné režimy přístupu. Jako další odlišnost byl zmíněn fakt, že archivnictví má možnost, dokonce legislativně zakotvenou, ovlivnit data, která proudí do archivů, a že archivy jako jediné v sobě spojují úkoly vědecké, kulturní i úřední. V otázce vhodnosti se dochází k závěru, že auditní a certifikační nástroje vhodné jsou, ale neměly by se stát alfou a omegou dlouhodobé archivace digitálních dat. Neměly by být opomenuty nástroje pro audit dalších oblastí (např. ekonomické) a je potřeba se zaměřit na digitální oblasti, které zůstávají stranou zájmu, ačkoli na nich vznikají data s trvalou hodnotou, které pomalu vytlačují a nahrazují ta klasická.

Literatura a zdroje

[1] *Accreditation Procedure for Management Systems Certification Bodies,* NABCB, online 2021. Dostupné z: http://nabcb.qci.org.in/documents/BCB%20201%20(MS)%20-%20Accreditation%20Procedure%20for%20MS_Mar%202021.pdf [16. února 2022]

[2] *Accreditation Criteria For Trustworthy Digital Repository Certification Bodies*, NABCB, online 2019. Dostupné z: http://nabcb.qci.org.in/documents/BCB%20160%20(TDRMS)-Accreditation%20Criteria.pdf [16. února 2022]

[3] Bárta Stanislav, Brzobohatá Hana, Červená Radana, Jelínek Jiří, Stodůlka Zbyšek, Zemánková Michaela: *Digitální archivnictví*, Masarykova univerzita, Brno 2019.

[4] Bartošek Miroslav: *Archivematica - open source systém pro digitální archivaci*. Knihovna: Knihovnická revue, 2015, 26 (2), s. 25–38.

[5] Bernas Jiří, Stodůlka Zbyšek, Vojáček Milan: *Certifikace NESTOR* in: LTP 2019: Nové trendy a východiska pri budování LTP archívov: zborník príspevkov zo 4. medzinárodnej konferencie o dlhodobej archivácii, Bratislava 2019.

[6] *CoreTrustSeal Trustworthy Data Repositories Requirements: Extended Guidance 2020–2022*, Core Trust Seal, online 2022. Dostupné z: https://www.coretrustseal.org/why-certification/requirements/ [30. ledna 2022]

[7] Cubr Ladislav: *Autenticita a digitální informace*. Praha, 2017. Dizertační práce. Univerzita Karlova, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí práce Ivánek, Jiří.

[8] Cubr Ladislav: *Strategie ochrany digitálních dokumentů*. Praha, 2009. Diplomová práce. Univerzita Karlova, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí práce Hutař, Jan.

[9] Cubr Ladislav: *Trvalá udržitelnost digitálního dědictví*. Praha, 2010. Rigorózní práce. Univerzita Karlova, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí práce Bratková, Eva.

[10] Dobiášovský Jan: *Správa digitální knihovny Národní technické knihovny a dlouhodobá ochrana digitálních dokumentů: případová studie*. Praha, 2017. Bakalářská práce. Univerzita Karlova, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí práce Římanová, Radka.

[11] Fojtů Andrea: *Strategie, návrh, řízení a administrace rozsáhlých digitálních knihoven a archivů*. Praha, 2014. Dizertační práce. Univerzita Karlova, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí práce Papík, Richard.

[12] Holá Martina: *Problematika vývoje Národního digitálního archivu*. 2017. Bakalářská práce. Univerzita Karlova, Filozofická fakulta, Katedra PVH a archivního studia. Vedoucí práce Dvořák, Tomáš.

[13] Hutař Jan: *Digitalizace, popis pomocí metadat a jejich formáty*. Praha, 2012. Dizertační práce. Univerzita Karlova, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí práce Kalkus, Stanislav.

[14] Lambertová Jana: *Analýza funkčního modelu Otevřeného archivního informačního systému (OAIS)*. 2018. Bakalářská práce. Univerzita Karlova, Filozofická fakulta, Katedra PVH a archivního studia. Vedoucí práce Dvořák, Tomáš.

[15] Metodický návod č. 2/2022 odboru archivní správy a spisové služby Ministerstva vnitra pro akreditaci digitálního archivu, MV ČR 2022.

[16] Miranda Andrea: *Důvěryhodná digitální úložiště, jejich audit a certifikace*, Knihovna: Knihovnická revue, 2015, 26 (2), s.49–57. Dostupné z: https://knihovnarevue.nkp.cz/archiv/2015-2/knihovny-a-informace/duveryhodna-digitalni-uloziste-jejich-audit-a-certifikace [17. ledna 2022]

[17] Neuroth H., Oßwald A., Scheffel R., Strathmann S., Huth K. (eds.): *nestor Handbuch: Eine kleine Enzyklopädie der digitalen Langzeitarchivierung*, online 2010. Dostupné z: https://www.langzeitarchivierung.de/Webs/nestor/EN/Publikationen/nestor_Handbuecher/nestor_handbuecher_node.html [17. ledna 2022]

[18] *Systémy pro přenos dat a informací z kosmického prostoru – Audit a certifikace důvěryhodných digitálních úložišť. ČSN ISO 16363*, Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, Praha 2014.

[19] Vyhláška č. 645/2004 Sb., kterou se provádí zákon o archivnictví a spisové službě.

[20] Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby.

[21] Zákon č. 499/2004 Sb., o archivnictví a spisové službě.

[22] Zákon č. 500/2004 Sb., správní řád.

[23] Zákon č. 167/2014 Sb., kterým se mění zákon o archivnictví a spisové službě, zákon o elektronickém podpisu a další související zákony.

[24] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.