Univerzita Hradec Králové
Filozofická fakulta

Katedra pomocných věd historických a archivnictví

ARCHIVISTIKA 4

studijní opora pro kombinovanou formu bakalářského studia

Historické vědy

Mgr. Radek Pokorný

Hradec Králové

2021

Anotace přednášky

Účelem výuky je osvojení znalostí nutných pro zvládnutí práce s výpočetní a komunikační technikou v archivech. Základem je teorie digitálního dokumentu a problematika dlouhodobého ukládání digitálních dat. Součástí je i seznámení s moderními specializovanými archivními softwary.

Základní informace o kurzu

- typ předmětu: povinný předmět
- doporučený ročník / semestr: třetí ročník /zimní semestr
- rozsah studijního předmětu: 4 přednášky + 4 semináře (celkem 8 hodin)
- počet kreditů: 2
- způsob ověření studijních výsledků: zápočet
- forma způsobu ověření studijních výsledků a další požadavky na studenta: písemný test, docházka na seminář
- garant předmětu: PhDr. Jiří Pavlík, Ph.D.
- vyučující: Mgr. Radek Pokorný

Tematický plán kurzu

1.-2. Základy práce s výpočetní technikou, hardware a software. Teorie informace a digitálního dokumentu.

3. Autenticita digitálních dokumentů.

4.-5. Vývoj a současný stav eGovernmentu, základní projekty, komparace se zahraničím, dopad na spisovou službu a archivní činnost.

6. Národní standard pro elektronické spisové služby.

7.-9. Překážky dlouhodobého ukládání digitálních dat a jejich řešení. Digitální archivy a digitální archiválie.

10.-11. Specializované archivní programy.

Základní literatura

povinná literatura:

CUBR, Ladislav. Dlouhodobá ochrana digitálních dokumentů. 1. vyd. Praha: Národní knihovna České republiky, 2010. 154 s. ISBN 978-80-7050-588-5.

Národní standard pro elektronické spisové služby. Věstník MV ČR 2017

LECHNER, Tomáš. Elektronické dokumenty v právní praxi. Praha: Leges, 2013. 255 s. Praktik. ISBN 978-80-87576-41-0.

MATES, Pavel a SMEJKAL, Vladimír. E-government v České republice: právní a technologické aspekty. 2., podstatně přeprac. a rozš. vyd., V nakl. Leges vyd. 1. Praha: Leges, 2012. 464 s. Teoretik. ISBN 978-80-87576-36-6.

Informatika / J. Glenn Brookshear ; [a přispěvatelé David T. Smith, Dennis Brylow ; překlad Jakub Goner]. -- 1. vyd.. -- Brno : Computer Press, 2013. -- 608 s.

ČSN ISO 14721 a ČSN ISO 16363.

POLČÁK, Radim a kol. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018.

BÁRTA, Stanislav (red.) – BRZOBOHATÁ, Hana – ČERVENÁ, Radana – JELÍNEK, Jiří – STODŮLKA, Zbyšek - ZEMÁNKOVÁ, Michaela. *Digitální archivnictví*. FF MU : Brno, 2018.

doporučená literatura:

PETERKA, J. Báječný svět elektronického podpisu. CZ NIC, z.s.p.o.,2017.
V elektronické starší verzi k 2011 (nezahrnuje legislativní změny po roce 2016) dostupná na adrese:
http://aleph.svkhk.cz/exlibris/aleph/u23_1/hka01/objects/view/116/NIC_Bajecny_svet_elektronickeho_podpisu_000469377.pdf)

KMENT, Vojtěch. *Elektronické právní jednání: analýza s důrazem na využití elektronického podpisu a elektronické pečeti podle práva EU*, České republiky a Německa. Praha: Wolters Kluwer, 2018.

Digital Preservation: Putting It to Work. Editors: Traczyk, T., Ogryczak, W., Pałka, P., Śliwiński, T. (Eds.), 2017. ISBN 978-3-319-51801-5

Digital Preservation Handbook, 2nd Edition, http://handbook.dpconline.org/, Digital Preservation Coalition © 2015.

Corrado, Edward M. and Heather Lea Moulaison. Digital Preservation for Libraries, Archives, and Museums. Rowman and Littlefield, 2014. ISBN: 978-0-8108-8712-1

GIARETTA, David. Advanced digital preservation [online]. Berlin: Springer, ©2011 [cit. 2014-11-17]. ISBN 978-3-642-16809-3. Dostupné z: http://www.springerlink.com/content/978-3-642-16808-6/contents.

Konferenční sborníky Co po nás zbude – CNZ, dostupné na http://www.cnz.cz/akce-cnz/konference-cnz; Archivy knihovny, muzea v digitálním světě, dostupné na http://www.skipcr.cz/akce-a-projekty/akce-skip/archivy-knihovny-muzea-v-digitalnim-svete/; Internet ve státní správě a samosprávě, příspěvky dostupné na https://www.isss.cz/archiv.asp

Digital Preservation CZ – BLOG, Blog o dlouhodobé ochraně digitálních informací, dostupné na http://digital-preservation-cz.blogspot.cz/ CoSECTOR BLOG, dostupné na https://blog.cosector.com/topic/digital-preservation; E-ARK Project (European Archival Records and Knowledge Preservation), dostupné na http://www.eark-project.com/

Jak postupovat při samostudiu

Každé téma je strukturováno na oddíl obecných cílů, povinných studijních materiálů, dílčích úkolů, základních tezí a doplňující literatury. **Obecné cíle** reflektují základ zkoušené látky v rámci závěrečného zápočtového testu. **Studijní materiály** u každého tématu obsahují odbornou literaturu či periodika, jež jsou dostupná buď v Lesákově knihovně sídlící přímo v budově Filozofické fakulty Univerzity Hradec Králové, nebo v Univerzitní knihovně UHK, či ve Studijní a vědecké knihovně v Hradci Králové, popřípadě také v Knihovně města Hradce Králové nebo veřejné knihovně Státního okresního archivu Hradec Králové. Některé studijní materiály jsou v digitální podobě nebo jsou k dispozici i v digitální podobě a jsou uvedeny odkazy na jejich dálkové zpřístupnění v síti Internet. Aby si mohli studenti prověřit získané znalosti ze studia, každé téma provází též série **dílčích úkolů** v podobě konkrétních otázek.

Tato sekce otázek vede studenty k rozvoji analytického myšlení a lepšímu porozumění danému tématu. Vybrané pojmy pak upozorňují na důležitá témata z obsahu přednášek, nenahrazují však studijní materiály. Poslední část, uzavírající strukturu didaktické pomůcky, je **seznam doplňující literatury**, která, jak už název vypovídá, doplňuje studentům jejich obzory v dané problematice a odkazuje je na tituly, kde by v intencích probrané látky mohli naleznout více podrobnějších informací.

1.-2. Základy práce s výpočetní technikou, hardware a software. Teorie informace a digitálního dokumentu.

OBECNÉ CÍLE

1. Získat znalost základních pojmů a principů z oblasti informačních a komunikačních technologií.
2. Chápat pojem dokumentu, jeho význam pro obor archivní a spisové služby.

STUDIJNÍ MATERIÁLY

BROOKSHEAR, J. G. [a přispěvatelé David T. Smith, Dennis Brylow ; překlad Jakub Goner]. – *Informatika*. 1. vyd.. -- Brno : Computer Press, 2013. -- 608 s.

CEJPEK, J. *Informace, komunikace a myšlení : úvod do informační vědy*. Praha: Karolinum, 2005.

VOJTÁŠEK, Filip: Dlouhodobá archivace digitálních dokumentů, Ikaros [online], 2000, roč. 4, č. 10 [cit. 2009-03-26], dostupný na WWW: http://www.ikaros.cz/node/675

CUBR, Ladislav. Dlouhodobá ochrana digitálních dokumentů. Praha: Národní knihovna ČR, 2010.

Multilingual Archival Terminology [online]. International Council on Archives, 2012 [cit. 2018-02-28]. Dostupné z: http://www.ciscra.org/mat/

Dictionary on Archival Terminology - DAT III: English, German, French and Russian lists [online]. Marburg: Archivschule Marburg - Hochschule für Archivwissenschaft, 2004 [cit. 2018-02-28]. Dostupné z: https://internet.archivschule.uni-marburg.de/datiii/index.html

PEARCE-MOSES, Richard. *A Glossary of Archival and Records Terminology* [online]. Chicago: The Society of American Archivists, 2005 [cit. 2018-02-28]. ISBN 1-931666-14-8. Dostupné z: https://www2.archivists.org/glossary

Terminology database. *InterPARES 2 Project: International Research on Permanent Authentic Records in Electronic Systems* [online]. Vancouver: InterPARES Trust (ITrust 2013-2018), 2018 [cit. 2018-02-28]. Dostupné z: http://www.interpares.org/ip2/ip2_terminology_db.cfm

Glossary of Recordkeeping Terms. *United Nations: Archives and Records Management Section* [online]. 2012 [cit. 2018-02-28]. Dostupné z: https://archives.un.org/content/glossary-recordkeeping-terms

Glossary of Recordkeeping Terms. *New South Wales Government - State Archives & Records* [online]. Kingswood, Australia [cit. 2018-02-28]. Dostupné z: https://www.records.nsw.gov.au/recordkeeping/resources/glossary

DURANTI, Luciana - FRANKS, Patricia C. eds. *Encyclopedia of Archival Science*. MD: Rowman & Littlefield, 2015

Legislativa a standardy:

Zákon č. 499/2004 Sb., archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů.

Národní standard pro elektronické systémy spisové služby, Věstník Ministerstva vnitra č. 57/2017.

Zdroje:

Zákony pro lidi [online]. AION CS [cit. 2018-02-28]. Dostupné z: https://www.zakonyprolidi.cz/

DÍLČÍ ÚKOLY

1. Co je to entropie informace?

2. Jaká je nejmenší jednotka informace?

3. Popište základní hardware osobního počítače.

4. Jaký je účel operačního systému a jaké operační systémy jsou v současnosti využívány?

5. Jaké jsou základní rozdíly mezi analogovým a digitálním dokumentem?

6.Jaké jsou základní typy digitálního dokumentu dle způsobu jeho vzniku?

7. Jaký je vztah pojmu písemnost – dokument?

8. Popište vzájemnou souvislost pojmů data – informace – dokument. Jaký typ informace se dle vašeho názoru stává nejčastěji zaznamenaným v dokumentech relevantních pro archivní praxi?

VYBRANÉ POJMY

DOPLŇUJÍCÍ LITERATURA

ROSICKÝ, A. *Informace a systémy : základy teorie pro úspěšnou praxi*. Praha:Oeconomica, 2009.

BUCKLAND, Michael: *What is a „digital document* [online], Document Numérique, 1998, Vol. 2, No. 2, s. 221–230 [cit. 2021-09-20], dostupný na WWW: <http://people.ischool.berkeley.edu/~buckland/digdoc.html>

PŘICHYSTAL, Jan. Úvod do teorie informace. In: Úvod do teorie informace [online]. 2007 [cit. 2021-09-20]. Dostupné z: https://akela.mendelu.cz/~jprich/predn/teoinf.pdf.

3. Autenticita digitálních dokumentů.

OBECNÉ CÍLE

1. Získat znalosti o způsobech zajišťování autenticity digitálních dokumentů.
2. Zvládat principy elektronického podpisu.

STUDIJNÍ MATERIÁLY

Webové stránky Ministerstva vnitra České republiky, Metodický návod pro ověřování platnosti uznávaných elektronických podpisů a elektronických pečetí. https://www.mvcr.cz/soubor/metodicky-navod-pro-overovani-platnosti-uznavanych-podpisu-a-peceti.aspx.

PETERKA, J. Báječný svět elektronického podpisu. CZ NIC, z.s.p.o.,2017.

V elektronické starší verzi k 2011 (nezahrnuje legislativní změny po roce 2016) dostupná na adrese:

http://aleph.svkhk.cz/exlibris/aleph/u23_1/hka01/objects/view/116/NIC_Bajecny_svet_elektronickeho_podpisu_000469377.pdf)

KMENT, Vojtěch. *Elektronické právní jednání: analýza s důrazem na využití elektronického podpisu a elektronické pečeti podle práva EU*, České republiky a Německa. Praha: Wolters Kluwer, 2018.

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

DÍLČÍ ÚKOLY

1. **Popište typologii elektronických podpisů.**
2. **Jakou roli hrají hashovací funkce při vytváření elektronického podpisu, pečeti či časového razítka?**
3. **K čemu slouží transakční protokol?**

4. **Jaké principy asymetrického šifrování používá elektronický podpis, pečeť a časové razítko?**
5. **V čem jsou odlišné principy ověřování autenticity analogových a digitálních dokumentů?**
6. **Popište proces ověřování platnosti elektronického podpisu.**
7. **Kdo jsou veřejnoprávní podepisující a jakou úroveň elektronického podpisu jsou povinni používat při podpisu dokumentu, kterým se právně jedná?**

VYBRANÉ POJMY

elektronický podpis – elektronický autentizační prvek založený na datech v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání. Nejčastěji je založen na technologii PKI (Public Key Infrastructure) využívající metod asymetrické kryptografie. Podepisující zašifruje dokument pomocí svého privátního klíče a příjemce jej pomocí svého veřejného klíče dešifruje, resp. ověřuje integritu dokumentu porovnáním jeho velikost v podobě kontrolního součtu, který je v elektronickém podpisu při jeho podepsání. K posouzení, zda byl dokument podepsán osobou, která to prohlašuje, slouží certifikát, který může být vytvořen podepisujícím nebo vydán třetí stranou (certifikační autorita).

prostý elektronický podpis, bez přívlastků – cokoliv, co má elektronickou podobu a bylo použito jako podpis, například biometrický podpis, naskenovaný obrázek ručního podpisu apod., lze využít výhradně při soukromoprávních úkonech.

zaručený elektronický podpis – podpis založený na certifikátu, na který ale nejsou kladeny žádné právní nároky a pravidla, např. testovací, firemní, spolkový, opět využitelný pouze v soukromoprávní sféře anebo v rámci dané organizace.

zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis – založený na certifikátu vydávaném uznávanou certifikační autoritou, nepoužívá však kvalifikovaný prostředek, dle § 6 zákona č. 297/2016 Sb. jím soukromoprávní osoba právně jedná vůči veřejnoprávnímu podepisujícímu nebo jiné osobě v souvislosti s výkonem jejich působnosti, nejtypičtější situace je jeho použití při digitálním jednání klienta (občana) vůči

veřejné správě, např. při podpisu e-mailu, dokumentů nezasílaných pomocí datových schránek apod.

kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném kvalifikovaným poskytovatelem služeb vytvářejících důvěru (certifikační autorita) a vytvořený pomocí kvalifikovaného prostředku pro vytváření elektronických podpisů (USB token, čipová karta). Tím jsou povinny podepisovat dle § 5 zákona č. 297/2016 Sb. vybrané orgány veřejné moci (tzv. veřejnoprávní podepisující) při právním jednání nebo jiná osoba při výkonu své působnosti, typickou situací je podpis dokumentu odesílaného úřadem klientovi datovými schránkami či jinou formou elektronické komunikace

uznávaný elektronický podpis je česká legislativní zkratka, která označuje zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis, pokud jej použije klient vůči veřejnoprávnímu podepisujícímu, a kvalifikovaný elektronický podpis

hashovací funkce – matematická funkce (resp. algoritmus), která mapuje bitové řetězce na bitové řetězce pevné délky, tzn. z libovolně velkých dat na vstupu vytvoří předem pevně stanovený blok dat na výstupu, přičemž splňuje následující dvě vlastnosti: 1. je výpočetně neproveditelné nalézt pro daný výstup vstup, který se mapuje na tento výstup a 2. je výpočetně neproveditelné nalézt pro daný vstup další vstup, který se mapuje na stejný výstup. Jakákoliv změna vstupu tedy vede k odlišnému výstupu, a to i přesto, že výstup může být mnohonásobně menší než vstup. Toho se využívá při porovnávání dat, zajištění integrity dat atd. Výsledný blok dat o pevné velikosti – otisk (hash), se typicky udává v bitové délce např. 128, 256, 512 bitů. Známými zástupci hashovacích funkcí je např. MD5, SHA atd. V rámci elektronického podepisování, pečetění a aplikace časových razítek je to právě vypočítaný hash (otisk) daného dokumentu (a nikoliv dokument samotný), který se stává předmětem kryptografických operací při vytváření uvedených rozšířených vlastností dokumentu či při jejich zpětném ověřování.

transakční protokol – obecně centrální chronologický zápis všech či všech významných aktivit v informačním systému. Transakční protokol hraje zásadní roli při udržování důvěryhodnosti elektronického infomačního systému. Např. občanský zákoník formuluje presumpci důkazní spolehlivosti elektronických písemností, u nichž se prokáže, že jsou součástí systému mající evidenci operací a ochranu proti změnám, tedy přesně to, co plní transakční protokol: § 562

odst. 2, první věta, zákona č. 89/2012 Sb.: „*Má se za to, že záznamy údajů o právních jednáních v elektronickém systému jsou spolehlivé, provádějí-li se systematicky a posloupně a jsou-li chráněny proti změnám*. Prokáže-li tedy ten, kdo písemností argumentuje, že systém, v němž se písemnost nachází, tyto parametry má, přesouvá se důkazní břemeno na toho, kdo tvrdí nedostatek její pravosti. V prostředí elektronické spisové služby (dále jen eSSL), je transakční protokol důvěryhodný zápis informací o operacích provedených v eSSL, které ovlivnily nebo změnily entity nebo eSSL. Tyto informace umožňují dohledání, identifikaci, rekonstrukci a kontrolu těchto operací, stavu entit v minulosti a činnosti uživatelů. Denní obsahy transakčního protokolu jsou povinně ztvárněny, uloženy, opatřeny elektronickými zajišťujícími prvky a evidovány jako dokumenty eSSL, jsou pak následně vybírány za archiválie. Zároveň eSSL musí podporovat export dat transakčního protokolu pro konkrétní entity spisové služby, který se tak stává historickým záznamem aktivit dotýkajících se každé entity. Takový připojený export z transakčního protokolu obohacuje metadata dané entity a zvyšuje tak její důvěryhodnost a schopnost archivace.

elektronická pečeť – elektronický autentizační prvek založený na datech v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu. Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce rozlišuje tři druhy elektronických pečetí:

1. kvalifikovaná elektronická pečeť založená na kvalifikovaném certifikátu vytvářená kvalifikovaným prostředkem (USB token, čipová karta, HSM modul, vzdálená služba prostřednictvím kvalifikovaného poskytovatele služeb vytvářejících důvěru) a to pro právní jednání veřejnoprávního podepisujícího a jiné právnické osoby, jedná-li při výkonu své působnosti, pokud jiný právní předpis nestanoví podpis nebo tato náležitost nevyplývá z povahy právního jednání (§ 8 cit. zákona)

2. uznávaná elektronická pečeť v podobě zaručené elektronické pečeti založené na kvalifikovaném certifikátu pro elektronickou pečeť nebo kvalifikovaná elektronická pečeť, a to pro právní jednání vůči veřejnoprávnímu podepisujícímu nebo jiné osobě v souvislosti s výkonem jejich působnosti (§ 9 cit. zákona)

3. elektronická pečeť pro právní jednání jiné než výše uvedeným způsobem (soukromoprávní subjekty).

Platí, že veřejnoprávní podepisující připojí kvalifikovanou elektronickou pečeť ke každému dokumentu, s kterým se právně jedná, ke kterému nebyl připojen elektronický podpis. Pečetí lze vyjádřit pouze vztah pečetícího k dokumentu, tzn. nelze jím například zajistit dokument jiného původu, který vlastník pečeti obdržel.

elektronická značka – obdoba elektronického podpisu dle zákona č. 227/2000 Sb. Jednalo se o údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které splňují následující požadavky:

1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu,

2. byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,

3. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.

V podobě uznávané elektronické značky, tedy založené na kvalifikovaném certifikátu, bylo možné užít k označování dokumentů v podobě datové zprávy, jehož prostřednictvím se činí úkon vůči a) státu, b) územnímu samosprávnému celku, c) právnické osobě zřízené zákonem, zřízené nebo založené státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem, d) právnické osobě neuvedené v písmenech a) až c) a vykonávající působnost v oblasti veřejné správy, týká-li se dokument této působnosti a e) fyzické osobě vykonávající působnost v oblasti veřejné správy, týká-li se dokument této působnosti. Elektronická značka je nahrazena v Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES institutem elektronické pečeti. Elektronickou značkou bylo možné označit i dokumenty doručené držiteli značky, což bylo využíváno v praxi elektronických spisových služeb.

elektronické časové razítko – elektronický autentizační prvek prokazující spojení data a času s daty takovým způsobem, aby byla přiměřeně zamezena možnost nezjistitelné změny dat. Je založeno na zdroji přesného času, který je spojen s koordinovaným světovým časem; je podepsáno s použitím zaručeného elektronického podpisu, opatřeno zaručenou elektronickou

pečetí kvalifikovaného poskytovatele služeb vytvářejících důvěru (též certifikační autorita) nebo označeno jinou rovnocennou metodou (u kvalifikovaného časového razítka).

eIDAS – nařízení Evropského parlamentu a rady (EU) č. 910/2014 ze dne 23.července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a zrušení směrnice 1999/93/ES (eIDAS). Toto nařízení zrušilo směrnici Evropské unie 1999/93/EC. Vstoupilo v platnost 17. září 2014, jeho účinnost je rozložena v čase dle čl. 52. Nařízení je závazné a přímo použitelné ve všech členských státech EU, tzn. má přednost před národní úpravou, byla-li by tato národní úprava s nařízením v nesouladu. Nařízení definuje podmínky pro elektronickou identifikaci osob a důvěryhodné služby pro elektronické transakce na vnitřním trhu Evropské unie. Nařízení v rámci kapitoly tři upravuje zejména tyto služby vytvářející důvěru – elektronické podpisy, elektronické pečetě, elektronická časová razítka, elektronické doporučené doručování, autentizace internetových stránek. Nařízení eIDAS v páté kapitole pak stanoví, že elektronickému dokumentu nesmí být upírány právní účinky a tento nesmí být odmítán jako důkaz v soudním a správním řízení. Nařízení EIDAS upravuje na evropské úrovni pravidla pro bezpečné transakce přes hranice elektronickou cestou bez užití tradičních metod, jako je např. pošta. Stanoví standardy pro elektronické podpisy, kvalifikované digitální certifikáty, elektronické pečeti, časová razítka a další způsoby ověření autentizace. Ty umožňují, aby elektronická transakce měla stejné právní postavení jako transakce prováděná v papírové podobě. Členské státy EU jsou povinny vytvořit společný rámec pro rozpoznávání elektronické identity z jiných členských států EU spolu s ověřením pravosti a bezpečnosti (interoperabilita). Na základě nařízení vzniká také veřejně přístupný seznam důvěryhodných služeb, které mohou být použity v rámci centralizovaného podpisu (transparentnost). Nařízení vytváří právní prostředí pro zaručený elektronický podpis (technicky navazuje na normy XAdES, PAdES nebo CAdES pro digitální podpisy, které byly specifikovány organizací ETSI (European Telecommunications Standards Institute/ Evropský ústav pro telekomunikační normy) a uznávaný elektronický podpis, kvalifikovaný digitální certifikát a důvěryhodnou elektronickou službu. V ČR pro oblast služeb vytvářejících důvěru doplňuje nařízení zákon o službách vytvářejících důvěru pro elektronické transakce č. 297/2016 Sb. včetně doprovodného pozměňovacího zákona č. 298/2016 Sb. a dále pak zákon o elektronické identifikaci č. 250/2017 Sb.

DOPLŇUJÍCÍ LITERATURA

POLČÁK, Radim a kol. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018.

LECHNER, Tomáš. *Elektronické dokumenty v právní praxi*. Praha: Leges, 2013.

4.-5. Vývoj a současný stav eGovernmentu, základní projekty, komparace se zahraničím, dopad na spisovou službu a archivní činnost.

OBECNÉ CÍLE

1. Získat přehled o vývoji e-Governmentu v České republice a jeho dopadu na veřejnou správu.
2. Získat přehled o základních nástroje informatizace veřejné správy a jejich vlivu na dokumenty.

LECHNER, Tomáš. Elektronické dokumenty v právní praxi. Praha: Leges, 2013. 255 s. Praktik. ISBN 978-80-87576-41-0.

MATES, Pavel a SMEJKAL, Vladimír. E-government v České republice: právní a technologické aspekty. 2., podstatně přeprac. a rozš. vyd., V nakl. Leges vyd. 1. Praha: Leges, 2012. 464 s. Teoretik. ISBN 978-80-87576-36-6.

POLČÁK, Radim a kol. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018.

Národní architektonické dokumenty. Dostupné na https://archi.gov.cz/start

Ministerstvo vnitra: GDPR https://www.mvcr.cz/gdpr/

Zákon č. 365/2000 Sb. o informačních systémech veřejné správy.
Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů.
Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby.
Zákon č. 300/2008 Sb.,o elektronických úkonech a autorizované konverzi dokumentů.
Vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů.
Vyhláška č. 194/2009 Sb.,o stanovení podrobností užívání a provozování informačního systému datových schránek.
Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
Zákon 298/2016 Sb. (účinný od 19.9.2016), kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce

eIDAS Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES

Nařízení Evropského parlamentu a Rady (EU) č. 679/2016 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů

Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů

Zákon č. 261/2021 Sb. -Zákon, kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

Zákon č. 111/2009 Sb., o základních registrech.

Zákon 250/2017 Sb. o elektronické identifikaci.

DÍLČÍ ÚKOLY

1. **Jaké je postavení Ministerstva vnitra ČR v rámci rozvoje informatizace veřejné správy?**
2. **K čemu slouží Portál občana?**
3. **Jaké přímé a nepřímé dopady mělo zavedení informačního systému datových schránek a konverze dokumentů na obor archivnictví?**
4. **K čemu slouží základní registry?**
5. **Jaká je souvislost mezi rozvojem eGovernmentu a digitálním archivnictvím?**
6. **Je systém elektronické spisové služby významným informačním systémem veřejné správy?**
7. **Jak systém datových schránek ovlivnil komunikaci s úřady?**

VYBRANÉ POJMY

eGovernment – využívání komunikačních a informačních technologií při výkonu veřejné správy s cílem přispět k naplnění doktríny dobré správy, tedy především k zajištění efektivní, transparentní a nestranné služby veřejnosti, obecně informatizace veřejné správy.

datová schránka – elektronické úložiště podle zákona 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, které je určeno k doručování orgány veřejné moci, provádění úkonů vůči orgánům veřejné moci, dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob. Datové schránky zřizuje a spravuje Ministerstvo vnitra. K datové schránce se přistupuje přes speciální webové rozhraní provozované Ministerstvem vnitra ČR na adrese https://www.mojedatovaschranka.cz/as/login?uri=https%3a%2f%2fwww.mojedatovaschranka.cz%2fportal%2fISDS%2f&status=NCOO a také s využitím webových služeb. Velikost datové schránky není omezena, ale je omezena doba, po kterou jsou zprávy v datové schránce uloženy. Doručování digitálních dokumentů prostřednictvím datových schránek je legislativně favorizovaným způsobem komunikace mezi orgány veřejné moci i komunikace od orgánů veřejné moci k ostatním držitelům datových schránek.

Komunikace systémem datových schránek:

<table>
<tr><td></td><td colspan="4">OD KOHO</td></tr>
<tr><td rowspan="4">KOMU</td><td>Komunikace zdarma
(ISDS placeno z rozp.
MV ČR)</td><td>Orgán veřejné moci</td><td>Právnická osoba</td><td>Fyzická osoba včetně podnikající</td></tr>
<tr><td>Orgán veřejné moci</td><td>Povinně* a výlučně**</td><td>Dobrovolně, pokud má DS</td><td>Dobrovolně, pokud má DS</td></tr>
<tr><td>Právnická osoba</td><td>Povinně*, pokud má DS</td><td colspan="2" rowspan="2">Dobrovolně, pokud obě strany mají DS – „privátní“ komunikace založená smluvně (PDZ, ODZ, DDZ) za úplatu</td></tr>
<tr><td>Fyzická osoba včetně podnikající</td><td>Povinně* pokud má DS</td></tr>
</table>

*Pokud to umožňuje povaha dokumentu nebo není určeno jinak jiným právním předpisem (např. nedoručuje-li se na místě či veřejnou vyhláškou)
**Pokud z bezpečnostních důvodů není zavedena jiná forma elektronické komunikace

informační systém veřejné správy – funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Zahrnuje data, která jsou uspořádána tak, aby bylo možné

jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností. Základním obsahem jsou datové prvky (jednotka dat jednoznačně definovaná a v rámci kontextu systému nedělitelná, např. adresa, rodinný stav) a číselníky (přípustné hodnosty datového prvku, např. svobodný). Systémy vedou zejména orgány centrální státní správy a územně samosprávných celků. Ústředním orgánem je Ministerstvo vnitra, které ISVS koordinuje, kontroluje a zpracovává koncepce rozvoje.

ISVS mohou být akreditovány a atestovány pověřenými atestačními středisky. Dělí se na veřejné (obchodní rejstřík, katastr nemovitostí ad.) a neveřejné (matriky, evidence rejstříku trestů ad.). Zákon o kybernetické bezpečnosti rozlišuje druhy informačních systémů, u nichž jsou příslušné orgány a osoby povinny zavést a provádět bezpečností opatření a vést o nich bezpečností dokumentaci:

1) Kritická informační infrastruktura, což je prvek nebo prvek infrastruktury v odvětví komunikačních a informačních systémů v oblasti kybernetické bezpečnosti. Zahrnuje zejména informační systémy základní služby, jejichž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém ze stanovených odvětví ,např. energetika, doprava, bankovnictví atd.),
2) Významný informační systém spravovaný orgánem veřejné moci, který není systémem dle 1), ale u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci, mezi takové systémy se řadí např. e-mailový klient provozovaný OVM nebo elektronický systém spisové služby.

Mezi informační systémy veřejné správy dle uvedeného zákona se naopak nepočítají provozní informační systémy zajišťují činnosti nutné pro vnitřní provoz příslušného orgánu, například účetnictví, správu majetku, nesouvisející bezprostředně s výkonem veřejné správy.

centrální místo služeb – zajišťuje vzájemné, řízené a bezpečné propojování subjektů veřejné a státní správy a komunikaci subjektů veřejné a státní správy s jinými subjekty ve vnějších sítích (např. internet). Zároveň tvoří jediné logické místo propojení jednotlivých operátorů telekomunikačních infrastruktur poskytujících služby pro komunikační infrastrukturu veřejné správy. Vytváří vyhrazené a zabezpečené prostředí jako základní stavební prvek celé komunikační infrastruktury veřejné správy.

komunikační infrastruktura veřejné správy – představuje sjednocenou datovou síť subjektů veřejné a státní správy ČR. Středobodem této komunikační infrastruktury je systém CMS, který tvoří jediné místo propojení státních síťových infrastruktur a telekomunikačních infrastruktur komerčních operátorů. KIVS slouží k bezpečné, garantované a auditovatelné výměně informací mezi jednotlivými orgány veřejné správy.

informační systém základních registrů – obsahem základních registrů jsou aktuální, právně závazné referenční údaje o subjektech těchto údajů. Cílem je sbírat a využívat spolehlivě stanovené informace v celé veřejné správě dálkovým přístupem bez nutnosti neustále nového předkládání potřebných dokladů prokazujících tyto informace. K údajům v základních registrech má přístup pouze ten, kdo k tomu má zákonné oprávnění a každý přístup je zaznamenán. V základních registrech jsou pak pouze aktuálně platné údaje bez historie. Referenční údaje jsou uloženy ve čtyřech základních registrech a nad nimi funguje tzv. ORG (správcem je ÚOOÚ) - převodník identifikátorů, který jako jediný dokáže propojit data v jednotlivých registrech, přičemž pro zajištění maximální ochrany osobních údajů využívá vygenerovaný bezvýznamový identifikátor místo rodného čísla. Samotné sdílení dat zajišťuje Informační systém základních registrů, který zároveň kontroluje oprávnění k přístupu k datům. O provoz a bezpečnost základních registrů se stará Správa základních registrů (https://www.szrcr.cz/cs/).

Registr osob (správcem je Český statistický úřad) - obsahuje základní identifikační údaje o subjektech, které mají IČO (právnické, podnikající fyzické osoby apod.), jejich provozovnách a statutárních zástupcích.

Registr obyvatel (správcem je Ministerstvo vnitra ČR) - obsahuje referenční údaje o fyzických osobách, které žijí na území ČR (občané ČR i cizinci) a to konkrétně jméno a příjmení, datum a místo narození (a případně úmrtí), adresa místa pobytu, státní občanství, čísla elektronicky čitelných identifikačních dokladů, ID datové schránky.

Registr práv a povinností – obsahuje údaje o vykonávaných agendách a údaje o oprávněních k přístupu k údajům v ostatních registrech.

Registr územní identifikace, adres a nemovitostí (správcem je Český úřad zeměměřický a katastrální) - slouží k evidenci územního členění státu. Vede referenční údaje o stavebních objektech, pozemcích, ulicích, katastrálních územích atd.

Národní identitní autorita (Národní identitní bod)- informační systém veřejné správy ve smyslu zákona č. 365/2000 Sb. o informačních systémech veřejné správy. Systém slouží jako nástroj pro agendy podle Nařízení evropského parlamentu a rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS), a Prováděcího rozhodnutí komise (EU) 2015/1984 ze dne 3. listopadu 2015, kterým se stanoví okolnosti, formáty a postupy pro oznamování podle čl. 9 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trh, Prováděcího rozhodnutí komise (EU) 2015/296 ze dne 24. února 2015, kterým se stanoví procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace podle čl. 12 odst. 7 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a souvisejících národních právních předpisů. Národní identitní autorita (dále jen „NIA“) zprostředkovává služby důvěryhodných poskytovatelů identit (Identity provider) jednotlivým důvěryhodným poskytovatelům služeb (Service Provider) vyžadujícím důvěryhodnost autentizací přistupujících subjektů (uživatelů). Součástí NIA je podpora administrativních procesů nutných k registraci důvěryhodných poskytovatelů identit (Identity Provider) a důvěryhodných poskytovatelů služeb (Service Provider) a navázání jejich důvěry. Úvodní stránka NIA Portál, který je umístěn na webových stránkách eidentita.cz. Představuje pro uživatele rozcestník mezi službami pro občany a službami pro poskytovatele služeb (Service Provider). Uživatel přistupující v roli občana může po úspěšném ověření provést správu vlastních údajů (správa SDÚ uživatelem), správu souhlasů pro výdej atributů vybranému poskytovateli služeb nebo správu svého profilu. Uživatel přistupující jako zástupce organizace může po úspěšném ověření provést registraci organizace nebo v rámci již registrované organizace konfigurovat či rušit jednotlivé poskytovatele služeb. NIA vytváří národní část uzlu EIDAS dle čl. 9, udržuje vazbu mezi základní elektronickou identitou fyzické

osoby (záznam v Registru obyvatel) a instancemi elektronické identity této osoby u poskytovatelů důvěryhodných služeb identifikace a autentizace

Czech Point – Podací Ověřovací Informační Národní Terminál (POINT) je asistované místo výkonu veřejné správy, umožňující komunikaci se státem prostřednictvím jednoho místa. Vznikl mj. za použití prostředků z Integrovaného operačního programu Evropského fondu pro regionální rozvoj. Systém kontaktních míst veřejné správy je v provozu od 1. 7. 2008 provozuje jej Ministerstvo vnitra. Cílem projektu Czech POINT je vytvořit garantovanou službu pro komunikaci se státem prostřednictvím jednoho univerzálního místa, kde je možné získat a ověřit data z veřejných i neveřejných informačních systémů veřejné správy, úředně ověřit dokumenty a listiny, převést písemné dokumenty do elektronické podoby a naopak, získat informace o průběhu správních řízení ve vztahu k občanovi a podat podání pro zahájení řízení správních orgánů. Jde tedy o maximální využití údajů ve vlastnictví státu tak, aby byly minimalizovány požadavky na občany. Systém Czech POINT poskytuje pro veřejnost výpisy z informačních systémů veřejné správy (např. z bodového hodnocení řidiče, z insolvenčního rejstříku, z Katastru nemovitostí, z Obchodního rejstříku, z Rejstříku trestů, z Rejstříku trestů právnických osob, z Živnostenského rejstříku, ze seznamu kvalifikovaných dodavatelů) či výpisy ze základních registrů (z registru obyvatel, z registru osob a výpisy o využití údajů z těchto registrů), podání vůči státní správě (např. podání do registru účastníků provozu modulu autovraků ISOH), konverze dokumentů v listinné podobě do dokumentu obsaženého v datové zprávě nebo datovém souboru a naopak, založení a správu datové schránky, zprostředkovanou identifikaci účastníka obchodu a další. Jednotlivé úkony těchto kontaktních míst veřejné správy jsou upraveny dílčími právními předpisy. Služby jsou poskytovány na tzv. kontaktních místech veřejné správy, která jsou opatřena modrým logem Czech POINT. Kontaktními místy veřejné správy jsou notáři, krajské úřady, obecní úřady, úřady městských částí nebo městských obvodů, ale také zastupitelské úřady (velvyslanectví) v zahraničí. Kontaktní místa provozuje rovněž Česká pošta, Hospodářská komora a také banky, kterým Ministerstvo vnitra udělilo autorizaci.

digitální služba – úkon vykonávaný orgánem veřejné moci vůči uživateli služby v rámci agendy a vedený v katalogu služeb jako úkon v elektronické podobě; za digitální službu se považuje i

úkon vykonávaný vůči uživateli služby kontaktním místem veřejné správy v rámci agendy. Rozlišujeme službu informační, kdy jsou poskytnuty informace o možnostech vyřízení konkrétní životní situace; službu transakční, kdy je možno elektronicky vyřídit celý proces služby a službu asistovanou, kdy je elektronická služba poskytnuta na kontaktním místě veřejné správy s asistencí úředníka.

Portál občana – spuštěn 8.7.2018 jako nadstavba a rozšíření Portálu veřejné správy, která zprostředkovává přístup k elektronickým službám státu. Dostupný na https://obcan.portal.gov.cz/ . Je centrální elektronické místo vstupu pro komunikaci občanů s úřady ČR. Jde o osobní prostor ve vztahu ke službám orgánů veřejné moci, nabídne občanovi zejména realizaci úplného elektronického podání, zajištění výstupů z informačních systémů veřejné správy, informace o stavu jednotlivých úkonů, které občan učinil vůči konkrétním orgánům veřejné moci, a dále například osobní archiv dokumentů. Občané mohou vstupovat do Portálu občana prostřednictvím přístupu se zaručenou elektronickou identitou např. e-občankou, datovou schránkou nebo jednorázovým heslem, a to buď samoobslužně (pomocí počítače, tabletu a mobilu) nebo zprostředkovaně z kontaktních míst veřejné správy.

Portál veřejné správy – informační systém veřejné správy zajišťující přístup k informacím veřejných orgánů a komunikaci s veřejnými orgány. Dostupný na https://portal.gov.cz/ . Správcem portálu veřejné správy je ministerstvo vnitra, před tím jím bylo od 6.10.2003 Ministerstvo informatiky. Portál veřejné správy zajišťuje přístup k informacím získaným na základě informační činnosti veřejných orgánů zejména v oblasti sociálního zabezpečení, zdravotnického zabezpečení, správy veřejných financí, dotací, veřejných zakázek, státní statistické služby, evidence a identifikace osob, jejich součástí a práv a povinností těchto osob či jejich součástí a tvorby a publikace právních předpisů. Portál veřejné správy zajišťuje komunikaci s veřejnými orgány prostřednictvím datových schránek, prostřednictvím přístupu se zaručenou identitou do informačních systémů veřejné správy nebo elektronických aplikací spravovaných těmito veřejnými orgány a prostřednictvím kontaktních míst veřejné správy. Portál veřejné správy dále zajišťuje přístup k informacím fyzických osob a právnických osob, zejména k formulářům v elektronické podobě těchto osob, a komunikaci s fyzickými osobami a právnickými osobami. Portál veřejné správy zajišťuje přístup k informacím fyzických osob a právnických osob na základě písemné smlouvy mezi správcem portálu veřejné správy a

fyzickou osobou, k jejímž informacím je zajištěn přístup, nebo právnickou osobou, k jejímž informacím je zajištěn přístup; písemná smlouva se nevyžaduje, stanoví-li fyzické osobě nebo právnické osobě povinnost zpřístupnit informaci prostřednictvím portálu veřejné správy zákon. Fyzická osoba, k jejímž informacím je zajištěn přístup, a právnická osoba, k jejímž informacím je zajištěn přístup, hradí za zajištění tohoto přístupu úplatu; to neplatí, stanoví-li fyzické osobě nebo právnické osobě povinnost zpřístupnit informaci prostřednictvím portálu veřejné správy zákon. Úplata je příjmem státního rozpočtu, vybírá ji správce portálu veřejné správy. Správce portálu veřejné správy stanoví podmínky, za kterých budou informace fyzických osob nebo právnických osob prostřednictvím portálu veřejné správy zpřístupněny, a pravidla pro stanovení výše úplaty a způsob její úhrady a zveřejní je na portálu veřejné správy. Portál veřejné správy umožňuje fyzické osobě zápis dokladu, průkazu, osvědčení nebo jiné veřejné listiny za účelem zasílání informace o končící platnosti této veřejné listiny na kontaktní údaj a zápis sériového čísla, vydavatele a platnosti kvalifikovaného certifikátu pro elektronický podpis.

konverze – v prostředí správy dokumentů je konverzí v užším smyslu změna (datových) formátů dokumentu v digitální podobě, resp. proces transformace jedné nebo více komponent tohoto dokumentu do jiného formátu (též formátová migrace). V širším pojetí pak pojem zahrnuje i převedení dokumentu v analogové podobě do dokumentu v digitální podobě a naopak. Výsledkem převedení i změny formátu dokumentu v prostředí elektronické spisové služby je ztvárnění. Autorizovanou konverzí se pak dle předpisu o autorizované konverzi dokumentů rozumí úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě nebo datovém souboru (dokumentu v digitální podobě) způsobem zajišťujícím shodu obsahu těchto dokumentů a připojení doložky o provedení konverze nebo úplné převedení dokumentu obsaženého v datové zprávě nebo datovém souboru (v digitální podobě) do dokumentu v listinné podobě způsobem zajišťujícím shodu obsahu těchto dokumentů a připojení doložky. Dokument, který provedením převodu vznikl – výstup, má stejné právní účinky jako dokument, z něhož vznikl – vstup. Neautorizovanou konverzí, též archivní či konverzí dle archivního zákona, je převod dokumentu v analogové podobě na dokument v digitální podobě a naopak a provedení změny datového formátu dokumentu v digitální podobě postupem zaručujícím věrohodnost původu dokumentu, neporušitelnost obsahu, čitelnost dokumentu a bezpečnost procesu převádění nebo změny formátu.

Dokument vzniklý převodem je opatřen doložkou a má právní účinky ověřené kopie dokumentu, jehož převedením nebo změnou datového formátu vznikl. Jinou konverzí se nejčastěji označuje prosté vytištění digitálního nebo digitalizace analogového dokumentu bez jakéhokoliv procesu ověření shody, doložení výsledku činnosti a právního účinku, méně často je i nesprávně zaměňována s pojmem neautorizované konverze.

ztvárnění – ve spisové službě se jím rozumí výsledek konverze nebo změny datového formátu. Změnou datového formátu je transformace dokumentu nebo komponenty při použití jednoho nebo více formátů odlišných od původních formátů. Ztvárnění se zpravidla vytvářejí pro uchování dokumentů v digitální podobě za účelem minimalizace rizika ztráty přístupu k jejich obsahu v čase. Například dokumenty vyhotovené v proprietárním datovém formátu musí být uloženy jako ztvárnění ve výstupním datovém formátu stanoveném prováděcím právním předpisem upravujícím podrobnosti výkonu spisové služby (například PDF/A). Výsledkem konverze nebo změny datového formátu dokumentu je ztvárnění některých nebo všech jeho komponent. Po konverzi nebo změně datového formátu může mít dokument stejný nebo rozdílný počet komponent jako před jejím provedením. Ztvárněna jako dokument mohou být také metadata nebo transakční protokol.

DOPLŇUJÍCÍ LITERATURA

DONÁT, Josef, Martin MAISNER a Robert PIFFL. *Nařízení eIDAS. Komentář*. Praha: Nakladatelství C. H.Beck, 2017.

Digitální Česko v digitální Evropě. Mladá Boleslav 2019. https://www.vlada.cz/assets/evropske-zalezitosti/aktualne/Digitalni_Cesko_FINAL-ONLINE-VERSION.pdf

6. Národní standard pro elektronické spisové služby.

OBECNÉ CÍLE

1. Chápat význam národního standardu pro elektronické spisové služby v rámci předarchivní péče archivu a jeho význam pro veřejnoprávní původce.

STUDIJNÍ MATERIÁLY

BÁRTA, Stanislav (red.) – BRZOBOHATÁ, Hana – ČERVENÁ, Radana – JELÍNEK, Jiří – STODŮLKA, Zbyšek - ZEMÁNKOVÁ, Michaela. Digitální archivnictví. FF MU : Brno, 2018.

KUNT Miroslav – LECHNER Tomáš. *Spisová služba*. 2. aktualizované vydání. Praha 2017.

Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů ve znění zákona č. 250/2014 Sb.

Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby v posledním znění, ve znění pozdějších předpisů.

Národní standard pro elektronické systémy spisové služby, Věstník ministerstva vnitra částka 57/2017 (část II)

Metodický návod pro kontrolu výkonu spisové služby vedené prostřednictvím elektronického systému spisové služby u veřejnoprávních původců. MV ČR, dostupný na https://www.mvcr.cz/clanek/spisova-sluzba-metodiky.aspx, citováno dne 29. 06. 2020.

DÍLČÍ ÚKOLY

1. **K čemu slouží národní standard pro elektronické spisové služby?**
2. **Kdo jej vydává a jak je zveřejněn?**
3. **Jak souvisí národní standard s činností archivářů v oblasti předarchivní péče?**

VYBRANÉ POJMY

elektronický systém spisové služby – informační systém určený ke správě dokumentů dle legislativních požadavků. Může se jednat o funkční součást informačního systému spravujícího dokumenty, která plní úkoly stanovené zákonem.

informační systém pro správu dokumentů – obecný pojem pro systémy, které spravují dokumenty, ať se již jedná o eSSL či samostatnou evidenci dokumentů.

předarchivní péče – soubor činností a vztahů mezi archivy a původci od vzniku dokumentů až do okamžiku ukončení skartačního nebo mimo skartačního řízení a předání archiválií do péče archivu. Představuje důležitou součást fungování archivů, které systematickou činností monitorují podmínky pro umožnění budoucího výběru archiválií. Mění se v čase a je odlišná rovněž v různých typech archivů – oblastních archivech, Národním archivu, archivech územních samosprávných celků. Zahrnuje oblast metodické spolupráce s původci, orientuje se významně na oblast spisové služby jako prostředku pro uchování dokumentů a umožnění výběru archiválií, kontrolu povinností vyplývajících ze zákona o archivnictví a spisové službě a další. Podpůrně zahrnuje vedení seznamů těchto původců, podílí se na šíření informací (legislativy a metodik), projevuje se ve spolupráci s Národním archivem a dalšími archivy. Důležitou roli v tomto ohledu plní soustava archivů a systematická dělba kompetencí s možností využití institutu přenesení působnosti.

Národní standard pro elektronické spisové služby – definuje, co musí splňovat elektronický systém spisové služby. Vycházel původně z evropské normy Moreq2, jeho první znění bylo publikováno ve Věstníku ministerstva vnitra čá. 76/2009, a to na základě zmocnění § 70 odst. 2, které bylo do archivního zákona doplněno jeho novelizací v roce 2009. Původcům, kteří již eSSL používali, bylo uloženo dát tyto systémy do souladu s národním standardem, a to nejpozději do 1. července 2012. Na základě praktických zkušeností jak původců, tak dodavatelů, byl text národního standardu postupně upravován, a to ve shodě s archiváři i výrobci spisových služeb na platformě pracovní skupiny sdružení Co po nás zbude. Poslední, aktuálně platné, znění zveřejněné ve Věstníku ministerstva vnitra čá. 57/2017 je tak již jeho čtvrtou verzí. Má 11 kapitol a je k němu připojeno celkem 6 příloh obsahujících schémata XML (1. – schéma pro výměnu dokumentů a jejich metadat mezi eSSL a jiným informačním systémem pro správu dokumentů, 2. – schéma pro zaznamenání popisných metadat uvnitř

datového balíčku SIP, 3. – schéma pro vytvoření datového balíčku SIP, 4. – schéma pro zasílání seznamu dokumentů a spisů vybraných za archiválie nebo dokumentů a spisů určených ke zničení a pro zaslání identifikátoru digitálního archivu po předání vybraných archiválií do archivu k jeho zaznamenání do eSSL, 5. – schéma pro export a import spisového a skartačního plánu, 6. – schéma pro export a import transakčního protokolu).

S účinností od 1.2.2022 je standard určen pro atestování elektronických systému spisové služby. Ministerstvo vnitra zajistí atestační středisko, které vydá výrobci eSSL písemný atest, že daný systém splňuje požadavky archivního zákona, vyhlášky podle §70 odst. 1 a národního standardu. Veřejnoprávním původcům nesmí být pod hrozbou sankce nabízen žádný systém, který nedisponuje takovým atestem.

kontrola v rámci předarchivní péče – jedná se o kontrolu plnění legislativních požadavků na péči o dokumenty podle archivního zákona (499/2004 Sb.). Řídí zákonem č. 255/2012 Sb., v platném znění (zákon o kontrole) a vykonávají ji především pracovníci specializovaní na předarchivní péči. Konkrétně takovou kontrolu provádí ministerstvo vnitra u Národního archivu, státních oblastních archivů, specializovaných a bezpečnostních archivů zřízených ministerstvy, dalšími ústředními správními úřady, Kanceláří Poslanecké sněmovny, Kanceláří Senátu, Kanceláří prezidenta republiky, Českou národní bankou nebo zpravodajskými službami České republiky a v širším pojetí u všech akreditovaných archivů, dále pak Národní archiv u správních archivů ministerstev a dalších ústředních správních úřadů, právnických osob zřízených zákonem, specializovaných archivů ostatních organizačních složek státu s celostátní působností, jakož i jimi zřízených státních příspěvkových organizací, s výjimkou těch archivů, kde kontrolu provádí ministerstvo, právnických osob zřízených zákonem, Archivu hlavního města Prahy a konečně státní oblastní archivy podle své územní působnosti u správních úřadů a jiných organizačních složek státu s působností na území kraje, okresu nebo obcí a u jimi zřízených státních příspěvkových organizací, specializovaných archivů státních podniků a státních příspěvkových organizací, s výjimkou těch archivů, kde provádí kontrolu Národní archiv, archivů územních samosprávných celků, s výjimkou Archivu hlavního města Prahy, orgánů územních samosprávných celků a jimi zřízených organizačních složek, příspěvkových organizací a jiných právnických osob, soukromých archivů a u zřizovatelů těchto archivů.

SIP (Submission Information Package) – informační balíček, který do archivu OAIS zasílá tvůrce (původce), ať již osoba nebo systém. Je tvořen určitým informačním obsahem a určitými informacemi o uchovávání. Z pohledu české archivní legislativy jsou SIP balíčky využívány při provádění výběru ve skartačním řízení podle § 20 odst. 5 vyhl. č. 259/2012 Sb. Veřejnoprávní původce sestaví z elektronického systému spisové služby nebo ze samostatné evidence dokumentů vedené v elektronické podobě seznam dokumentů určených k posouzení. Tento seznam je tvořen podle schématu XML pro vytvoření datového balíčku SIP stanoveného národním standardem a obsahuje metadata podle schématu XML pro zaznamenání popisných metadat uvnitř datového balíčku SIP stanoveného národním standardem (tj. přílohou č. 2 a přílohou č. 3). Další variantou SIP je balíček vzniklý při výběru z datových souborů mimo eSSL, ať již při výběru ve skartačním nebo výběru mimo skartační řízení s využitím Národního (archivního) portálu.

DOPLŇUJÍCÍ LITERATURA

Národní archiv, INFORMAČNÍ LIST pro otázky elektronické spisové služby a dokumentů v digitální podobě. Dostupné na https://www.nacr.cz/verejnost/2-predarchivni-pece/verejnopravni-puvodci/informacni-list

7. - 9. Překážky dlouhodobého ukládání digitálních dat a jejich řešení. Digitální archivy a digitální archiválie.

OBECNÉ CÍLE

1. Seznámit se s procesem dlouhodobé péče o digitální archiválie a jeho konkrétní aplikací v českém prostředí
2. Pochopit specifika péče o digitální archiválie

STUDIJNÍ MATERIÁLY

BÁRTA, Stanislav (red.) – BRZOBOHATÁ, Hana – ČERVENÁ, Radana – JELÍNEK, Jiří – STODŮLKA, Zbyšek – ZEMÁNKOVÁ, Michaela. Digitální archivnictví. FF MU : Brno, 2018. Dostupné z https://munispace.muni.cz/library/catalog/view/1407/3886/1725-1/0#preview citován.

CUBR, Ladislav. Dlouhodobá ochrana digitálních dokumentů. Praha: Národní knihovna ČR, 2010.

KUNT Miroslav – LECHNER Tomáš. *Spisová služba*. 2. aktualizované vydání. Praha 2017.

Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů ve znění zákona č. 250/2014 Sb.

SULITKOVÁ, Ludmila. *Archivnictví a spisová služba*. Ústí nad Labem: Filozofická fakulta, Univerzita Jana Evangelisty Purkyně v Ústí nad Labem ve spolupráci s nakladatelstvím Scientia, spol. s r.o., 2017. Acta Universitatis Purkynianae Facultatis philosophicae. ISBN 978-80-7561-027-0.; Dostupné též z: http://ff.ujep.cz/archivnictvi/archivni_teorie.pdf, citováno dne 29. 06. 2020.

Vyhláška č. 645/2004 Sb., kterou se provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů.

Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby v posledním znění v posledním znění.

DÍLČÍ ÚKOLY

1. **Jaké jsou překážky dlouhodobého uchovávání digitálních dat?**

2. **K čemu v procesu péče o digitální archiválie slouží metadata?**
3. **Které metadatové standardy jsou nejvíce využívány v procesu péče o digitální archiválie?**
4. **Vysvětlete pojmy SIP, AIP, DIP v procesu ukládání digitálních archiválií. Která norma popisuje SIP používaný v české archivní praxi?**
5. **Jaké jsou odlišnosti výběru archiválií v digitální podobě?**
6. **Jaké nástroje nabízí digitální archiv pro původce?**
7. **K čemu slouží formátová normalizace a jak je realizovaná v české archivní legislativě?**
8. **Která norma slouží celosvětově jako nejpoužívanější pro stavbu digitálních archivů?**
9. **Jakou roli hraje Národní archiv v Praze v procesu dlouhodobého ukládání digitálních dat?**
10. **K čemu slouží národní (archivní) portál?**

VYBRANÉ POJMY

národní digitální archiv – o možnostech digitální archivace se v českém archivnictví začalo uvažovat v polovině devadesátých let 20. století. Následně vznikly konkrétní výzkumné projekty realizované za účasti Odboru archivní správy MV, ČVUT a Národního archivu v letech 2001-2005. Konkrétní podobu úvahy o digitální archivaci dostaly v usnesení vlády č. 11 ze 7. ledna 2004, které uložilo vypracovat projekt dlouhodobého uchovávání a zpřístupňování dokumentů v digitální podobě. Cílem byla nutnost řešit dlouhodobé uchovávání digitálních dokumentů a byl určen postup směřující k vybudování digitálního archivu. Naléhavost řešení dlouhodobého uchovávání byla zdůrazněna rozvojem eGovernmentu, jehož projekty jsou bez vyřešení digitální archivace jen obtížně realizovatelné. Tým pro přípravu digitálního archivu byl v Národním archivu ustaven na konci roku 2005. Společně s vítězným dodavatelem připravil (v období od července 2007 do února 2009) technologický projekt Pracoviště pro dlouhodobé uchovávání a zpřístupňování dokumentů v digitální podobě. V dubnu 2008 vláda

svým usnesením č. 447, k zabezpečení plnění úkolů ve věci vybudování Národního digitálního archivu, schválila čerpání finančních prostředků na vybudování Národního digitálního archivu, které mělo být financováno v rámci Integrovaného operačního programu. Projekt se stal jednou z komponent programu Smart Administration – příloha ke strategii Efektivní veřejná správa a přátelské veřejné služby. Součástí projektu byla i stavební část směřující k vybudování hlavního pracoviště rozšířením budov archivního areálu Chodovec. Realizaci projektu v letech 2011-2013 významně ovlivnily problémy s výběrovým řízením na dodavatele softwarového řešení, od roku 2014 tedy došlo ke změně projektu a vybudování infrastruktury digitálního archivu na základě kanadského open-source LTP systému Archivematica. V roce 2015 proběhlo první výběr a uložení archiválií v digitální podobě v digitálním archivu. V roce 2016 přešlo pracoviště do plnohodnotného provozu, v roce 2017 byl do produkčního provozu spuštěn Národní (archivní) portál, který umožňuje přístup ke službám digitálního archivu. Zvýšení kapacity, robustnosti a rozšíření poskytovaných služeb probíhá od roku 2016 v rámci projektu IROP Národní digitální archiv II

Národnímu archivu dle § 46 odst. 3 archivního zákona:

a) ukládá archiválie v digitální podobě náležející do jeho péče a archiválie v digitální podobě náležející do péče Archivu bezpečnostních složek, státních oblastních archivů a archivů, které nejsou digitálními archivy a neukládají archiválie v digitální podobě na základě písemné dohody v jiném digitálním archivu, b) spravuje národní portál, c) plní pro archivy metodickou a poradenskou funkci v oblasti předarchivní péče o dokumenty v digitální podobě a v oblasti digitalizace archiválií v analogové podobě, d) provádí vědeckou a výzkumnou činnost na úseku životního cyklu dokumentů v digitální podobě, e) poskytuje archivům údaje potřebné pro evidenci archiválií v digitální podobě a služby pro shromažďování a zpřístupňování popisů archiválií v digitální podobě a replik archiválií v digitální podobě, f) vydává závazné stanovisko k žádosti o udělení oprávnění k ukládání archiválií v digitální podobě.

Prostřednictvím Národního portálu pak NDA zajišťuje:

a) výběr a příjem archiválií v digitální podobě a jejich metadat; b) vedení a zpřístupňování evidence Národního archivního dědictví; c) příjem metadat popisů původců; d) příjem metadat popisů archivů a kulturně vědeckých institucí; e) příjem a prezentace archivních pomůcek v digitální podobě; f) přístup k archiváliím v digitální podobě a dokumentům v

digitální podobě vzniklým jako digitální reprodukce z archiválií v analogové podobě; g) ve spolupráci s archivem, do jehož péče archiválie v digitální podobě náleží, vytváření, správu a zpřístupnění skupin metadat obsahujících: a) základní identifikaci archiválie, b) popis archiválie, c) evidenci subjektů oprávněných k přístupu k archiválii včetně rozsahu oprávnění

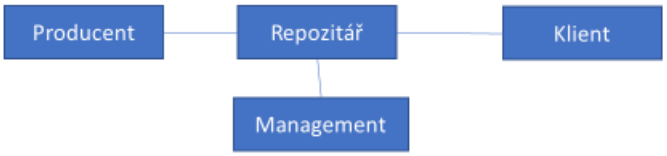
SIP (Submission Information Package) – informační balíček, který do archivu OAIS zasílá tvůrce (původce), ať již osoba nebo systém. Je tvořen určitým informačním obsahem a určitými informacemi o uchovávání. Z pohledu české archivní legislativy jsou SIP balíčky využívány při provádění výběru ve skartačním řízení podle § 20 odst. 5 vyhl. č. 259/2012 Sb. Veřejnoprávní původce sestaví z elektronického systému spisové služby nebo ze samostatné evidence dokumentů vedené v elektronické podobě seznam dokumentů určených k posouzení. Tento seznam je tvořen podle schématu XML pro vytvoření datového balíčku SIP stanoveného národním standardem a obsahuje metadata podle schématu XML pro zaznamenání popisných metadat uvnitř datového balíčku SIP stanoveného národním standardem (tj. přílohou č. 2 a přílohou č. 3). Další variantou SIP je balíček vzniklý při výběru z datových souborů mimo eSSL, ať již při výběru ve skartačním nebo výběru mimo skartační řízení s využitím Národního (archivního) portálu.

Otevřený archivační informační systém (OAIS – ČSN ISO 14721) - standard pro budování dlouhodobých úložišť digitálních dokumentů. Kumuluje znalostní bázi a ověřené postupy ze světa digitální archivace. Popisuje účastníky v oblasti uchovávání digitálního obsahu, jejich role a povinnosti a druhy informací, které jsou předmětem výměny při vkládání a přijímání dat do digitálních úložišť a poskytování dat z digitálních úložišť. OAIS se v rámci definice jednotlivých funkčních modulů zabývá všemi činnostmi, které jsou realizovány v procesu uchovávání archivních informací. Patří sem příjem, uložení do archivu, správa, zpřístupnění a poskytování. Referenční model se věnuje přesunům digitálních informací na nové datové nosiče a převody do nových formátů, datovými modely užívanými k vyjádření informací, funkcí SW při uchovávání informací a výměnu digitálních informací mezi archivy. Popisuje vnitřní a vnější rozhraní funkčních celků archivu a obecné služby těchto rozhraní. OAIS stanovuje, které základní povinnosti musí archiv plnit, aby mohl být označen za archiv typu OAIS. Archiv v souladu s požadavky referenčního modelu OAIS může uživatelům poskytovat také další služby, které přesahují rámec požadavků tohoto modelu. V obecném měřítku je hlavním účelem OAIS

usnadnit pochopení požadavků na dlouhodobé uchovávání a zpřístupňování digitálních informací. Digitální archivy se testují na soulad s tímto standardem.

OAIS v kontextu archivnictví

Model širšího kontextu



V případě archivnictví

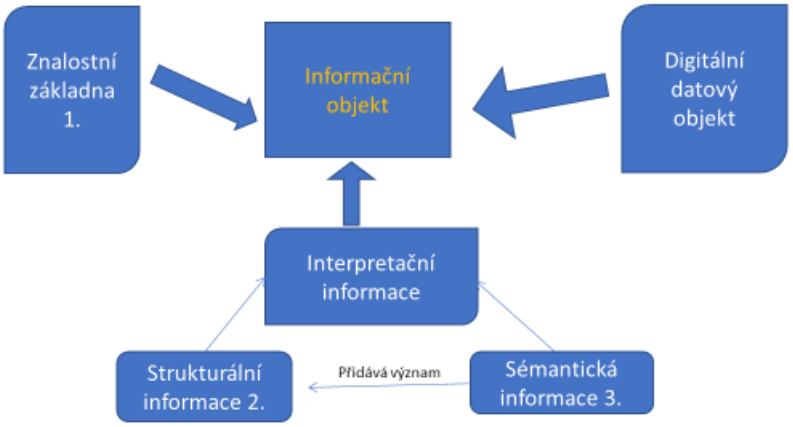
Producent – veřejnoprávní a soukromoprávní původci

Repozitář – Národní digitální archiv, digitální archiv

Management – Národní archiv, archiv zřizující DA

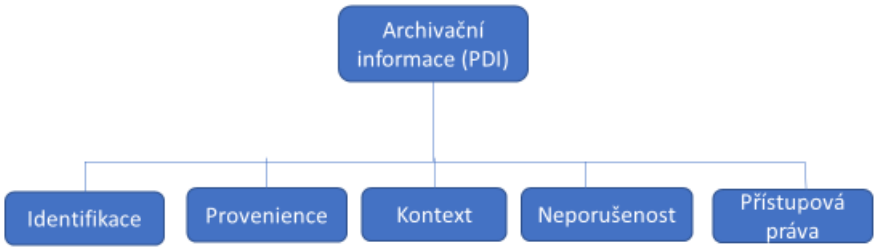
Klient – badatelská veřejnost, původci, archivy, které mají v příslušném Da uložené dig. dokumenty svých původců

Informační model OAIS



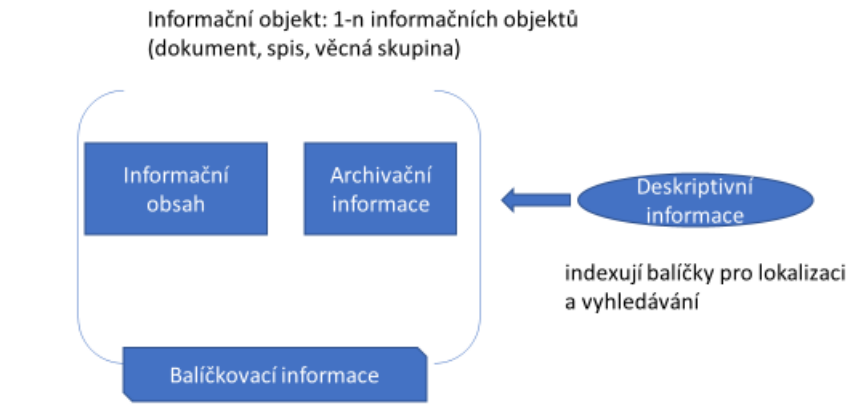
1. např. znalost spisové služby
2. formátová specifikace, využívaný software
3. např. jazyk textu, typ dokumentu, číselník, zkratky

Archivační informace



1. např. trvalý identifikátor
2. např. původce
3. např. spisový a skartační plán
4. např. digitální podpis, kontrolní hash
5. např. autorská práva, vlastnictví

Informační balíček

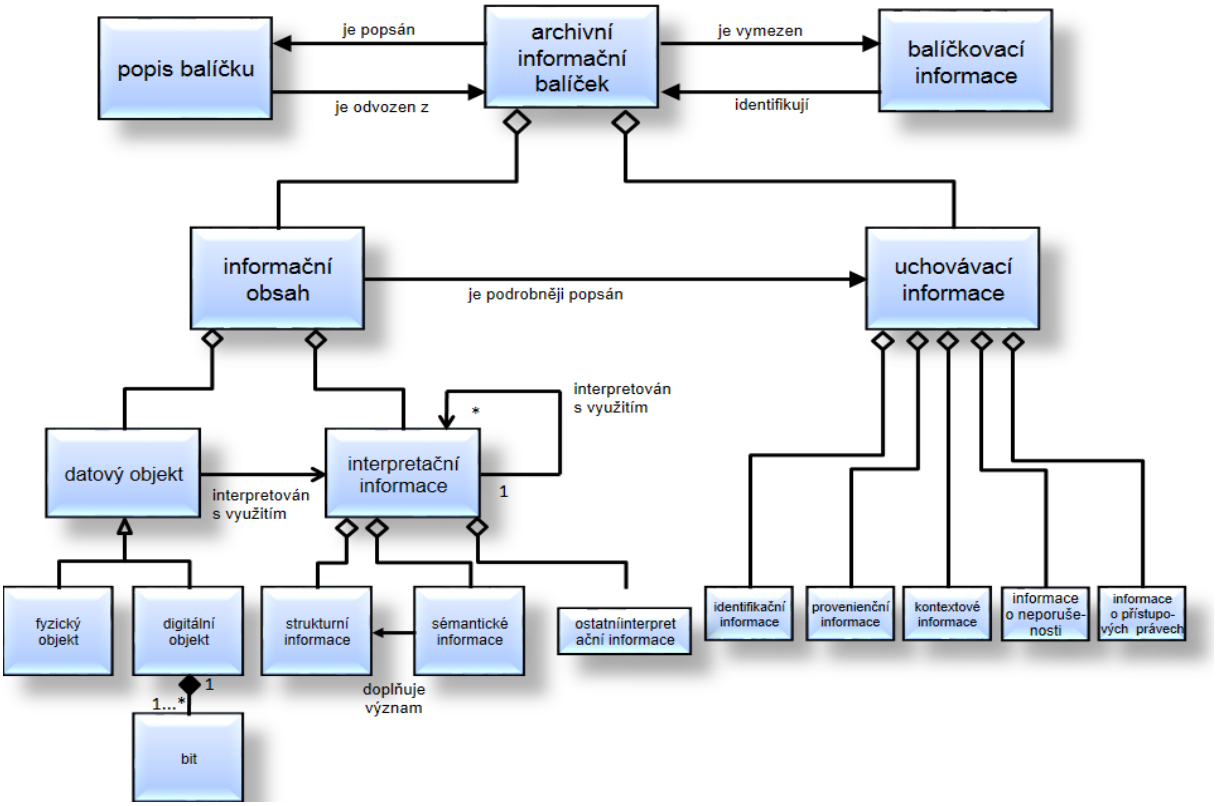


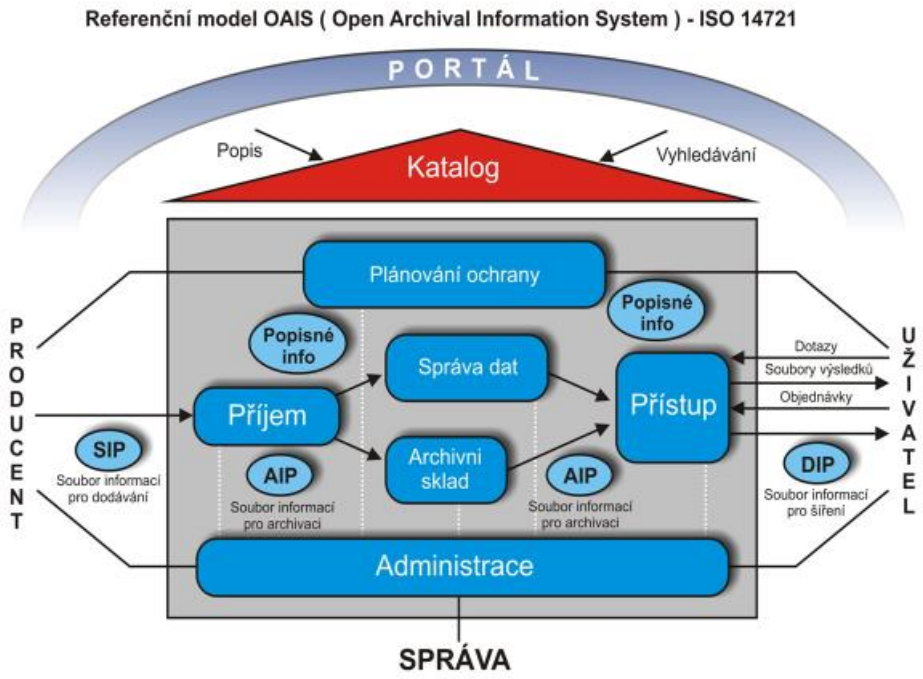
Typy balíčků

SIP – dodávají ERMS veřejnoprávních původců, informační systémy SSP v rozsahu povinností stanovených ArchZ

AIP – archiv dodává archivační (uchovávací, konzervační) metadata identifikátor odkazován do archivních pomůcek i systému ERMS

DIP – balíček pro badatele, pro zpracovatele pomůcek





výstupní datové formáty – v průběhu životního cyklu dokumentů v rámci eSSL se (na příjmu, nebo při odeslání či v okamžiku vyřízení dokumentu/spisu) tyto převádějí do výstupních datových formátů, které stanovuje vyhláška o spisové službě. Jedná se o nucenou formátovou normalizaci, kdy se dokumenty stanou předmětem formátové migrace, tedy nevratného převodu založeným na převodu původního zdrojového formátu na nový cílový formát, v daném případě formát, který je vhodný pro dlouhodobé uložení v digitálním archivu.

Nástroje národního digitálního archivu (dostupné na https://www.nacr.cz/):

Validátor SIP - validátor SIP je pomocný nástroj usnadňující vytvoření datového balíčku SIP. Je určen k ověření SIP určených pro skartační řízení a pro předání do archivu.

Validátor pdf – validuje digitální objekty uložené ve formátu pdf na jejich shodu s verzemi normy pdf/A, která je určena pro formát vhodný pro dlouhodobé ukládání digitálních dat

Národní archivní portál – obecně nástroj pro práci s digitálními archiváliemi, který slouží pro přístup původců, archivářů i badatelů k digitálním archiváliím, viz výše. Jeho součástmi jsou zásadní moduly, jako je např. modul skartačního řízení se samostatnou aplikací eSkartace pro

příjem SIP balíčků či modul mimoskartačního řízení, kdy potřená metadata dodává archivář nahrávající data.

Digitální dědictví - Konference UNESCO 12 v kanadském Vancouveru v roce 2012 konstatovala, že digitální technologie nabízí **bezprecedentní možnosti přenosu a uchování informací**. Dokumenty a data v digitální formě jsou velmi důležitá pro rozvoj vědy, výuky, kultury, ekonomiky i společnosti, ale problém jak zajistit jejich **uchování do budoucna** ještě **není ani zdaleka vyřešen**.

…mnohé **dokumenty již vznikají jako digitální**, ale bez řádného zvážení prostředků pro zajištění jejich trvalé dostupnosti, autenticity, spolehlivého a přesného uchování do budoucna a bez zvážení jejich kompatibility s budoucími technologiemi… **lepší porozumění digitálnímu prostředí** je zásadní pro vytvoření modelů ochrany digitálních dat, které budou respektovat právní principy, stabilizovat přístup k datům soukromé povahy, budou brát ohledy na ekonomickou stránku věci či respektovat vlastnictví…uchovávání digitálních záznamů by mělo být **prioritou a investice** do této činnosti jsou zásadní pro **zajištění důvěryhodnosti** zachovaných digitálních záznamů…musí být vyvinuta vhodná výuka…je tu naléhavá potřeba vytvořit plán, který navrhne **vhodná řešení** a zajistí dohody, které umožní **dlouhodobý přístup** a zároveň **důvěryhodné uchování**.

Schématické pojetí digitálního objetu jako předmětu uchovávání

Konceptuální objekt (obsah) – smysluplná jednotka informace, kterou lidský uživatel dokáže rozpoznat a rozumět jí.

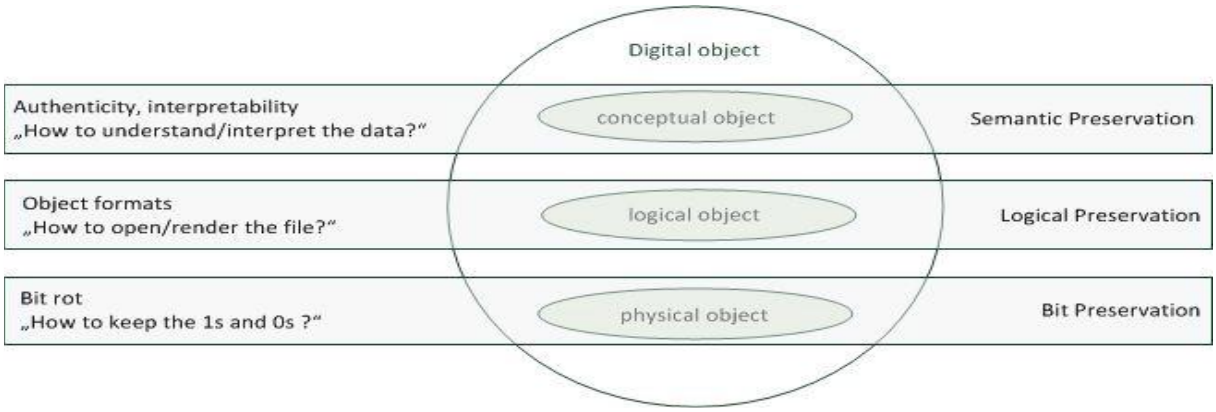
Cíl – srozumitelnost - neliší se příliš od požadavků ochrany dokumentů tradičních, musejí být opatřeny dostatečnou dokumentací, která umožní uživatelům, aby jim rozuměli, aniž by museli vyhledávat takové dodatečné informace, které nejsou široce dostupné

Logický objekt (kontext a struktura) – je rozpoznán a zpracován softwarem, přístup k logickému digitálnímu objektu je možný pouze prostřednictvím příslušných softwarových aplikací

Cíl – zpřístupnitelnost - zachovat adekvátní reprodukci příslušným softwarem, digitální objekt zpracovat určitou softwarovou aplikací a zpřístupnit lidskému uživateli v té podobě, pro jakou byl původně vytvořen

Fyzický objekt (forma) - zápis binárních znaků na konkrétním elektronickém nosiči, technické konvence určují rozhraní mezi systémem reprezentace těchto znaků a fyzickým datovým nosičem, na kterém jsou tyto znaky uloženy

Cíl - uchovávání - procesy soustavného zálohování a údržby nejen digitálních dokumentů, ale také přidružených počítačových technologií a datových nosičů



Zdroj obrázku: D6.6.1 Current state of 3D object digital preservation and gap-analysis report. DURAARK. Royal Danish Academy:2013. Dostupné na https://zenodo.org/record/1115504/files/duraark_d6.6.1_final.pdf

Překážky digitální archivace

Technologická rovina (fyzický objekt) -

a) Degradace nosičů (data decay, data rot, decay of storage media) v důsledku fyzikálních a chemických změn (např. změna magnetizace u magnetických médií, kazy materiálu, škůdci, drobné výboje u polovodičových médii, UV záření, vlhkost, teplo, elektromagnetické pole, kosmické záření ad.)

ochranná opatření: výběr vhodných nosičů a jejich kombinace, pravidelná technologická renovace, bitová ochrana (migrace bez změny bitových posloupností), multiplikace souborů (bitových kopií) na různých typech nosičů

b) Technologická selhání, např. výpadek el. proudu, selhání čtecích zařízení, chybný lidský úkon, selhání např. zálohovacích procesů, poškození virem, přírodní katastrofou

ochranná opatření: vhodné přístupy a plánování v oblasti hardwaru, používání více geograficky vzdálených úložišť

c) Technologická zastaralost (morální zastarávání HW), ukončení podpory ze strany výrobců způsobující ztrátu funkcionality, nečitelnost datových nosičů, nekompatibilita zařízení
ochranná opatření: opět technologická renovace a bitová ochrana formou migrace

Informační rovina (logický objekt) –
a) Formátová rizika – zastaralost formátu v důsledku technologické evoluce a obchodní taktiky vedoucí k ztrátě softwarové podpory
ochranná opatření: výběr vhodných perspektivních formátů pro dlouhodobé uložení dat a migrace dat před jejich uložením do vybraných formátů, v ČR realizováno konceptem výstupních datových formátů v §23 vyhlášky o podrobnostech spisové služby (viz pojem) nebo emulace, tedy použití softwaru umožňující běh počítačových programů na jiné platformě, než pro kterou byly původně vytvořeny, není v současnosti využíváno v praxi spisových služeb
b) Nedostatečná autoreference digitálních objektů – sami o sobě mnoho nevypovídají, jejich autenticita je opřena o použití složitých rozšířených vlastností (elektronický podpis, transakční protokol apod.)
ochranná opatření: metadatový popis objektu, a to strukturovaných způsobem za využití širokého spektra metadat (popisná, strukturální, archivní, technická, administrativní, legislativní) dle příslušných specializovaných standardů.

Institucionální rovina (srozumitelnost, autenticita) – dokumenty a archiválie musí být zajištěny po celou dobu jejich životního cyklu, a to důvěryhodným způsobem všemi jejich držiteli
ochranná opatření: analýza činnosti, vytvoření reálného scénáře stavby digitálního archivu jako instituce, zajištění dlouhodobé ekonomické udržitelnosti projektu, zajištění vnitřních i vnějších auditních nástrojů a certifikací k zajištění veřejné a respektované důvěryhodnosti. Jde o uchování, zpřístupnění, zajištění důvěryhodnosti dokumentů v celém jejich životním cyklu (tzv. digitální kontinuity) a především jejich srozumitelnosti cílové skupině uživatelů. Prostředkem k naplnění těchto cílů je **funkční institucionální archiv**, při jehož vzniku a provozu je třeba přijmout a udržovat v chodu řadu opatření v rovině plánování a řízení, v rovině technologických opatření i v oblasti dalšího využívání digitálních dat formou zajištění

jejich kvalitního metadatového popisu a zpřístupnění formou webových portálů dálkovým přístupem uživatelům. Příkladem takového řešení může být národní digitální archiv.

Metadata – zjednodušeně „data o datech“, označují strukturované informace, které popisují, osvětlují, lokalizují a různými způsoby usnadňují vyhledávání a využívání informačního zdroje. Metadata se v oblasti správy dokumentů a digitální archivace využívají při: 1. popisu informačních objektů; 2. označení vztahu mezi jedním informačním objektem a jinými objekty; 3. stanovení technických vlastností informačních objektů; 4. odpovědnosti za řízení a uchovávání informačních objektů; 5. zajištění vyhledání informačních objektů, bez ohledu na to, kde jsou uloženy; 6. popisu, jak může být informačních objekt využíván (např. právní omezení); 7. popisu požadavků na opětovné zobrazení informačních objektů; 8. zaznamenání historie informačních objektů a 9. doložení autenticity informačních objektů.
Při zajištění výše uvedených činností se obecně rozlišují tyto základní typy metadat:
1. Popisná metadata (descriptive metadata) reprezentují vlastnosti informačních objektů za účelem jejich identifikace a vyhledávání - např. údaje o tvůrci, názvu, vydavateli, roku vydání, evidenci dokumentu ve spisové službě, popisu archiválie v archivní pomůcce atd. Popisná metadata zachycují metadatová schémata Dublin Core, MARC 21, MODS, EAD aj.
2. Administrativní metadata (administrative metadata) zachycují procesy v rámci digitálního repozitáře a umožňují tak správu digitálních objektů. Následující podtypy metadat bývají někdy uváděny i samostatně:
a) Ochranná (též archivační či preservační) metadata (preservation metadata) deklarují procesy související s uchováváním a ochranou digitálních objektů v repozitáři. Jejich úkolem je zajistit integritu a kontext objektu s cílem umožnit jeho zpřístupnění. Slouží také k podpoře odpovídajících opatření při realizaci ochranných činností vycházejících z uchovávací strategie (migrace, emulace atd.). Zahrnuje např. historii objektu, vztahy k dalším informačním objektům, údaje o hardwaru a softwaru potřebném k jeho zobrazení atd. Nejčastěji je pro tyto účely využíván standard PREMIS.
b) Technická metadata (technical metadata) popisují technické vlastnosti digitálních objektů, např. datový formát, velikost, hardware a software sloužící k vytvoření objektu, komunikační protokol, komprese, kontrolní součet atd.). Slouží kupříkladu k vyhledání objektů ve stanoveném formátu, který má být převeden. Tyto metadata zachycuje např. sekce <mets:fileSec> standardu METS.

c) Metadata o možnostech přístupu a duševních právech (rights metadata; access metadata) poskytují informace o omezení přístupu k objektu s uvedením zdroje tohoto omezení (např. omezení přístupnosti archiválie, osobní a citlivé údaje, právo duševního vlastnictví, autorské právo, obchodní tajemství aj.), případně také o podmínkách omezení přístupu uživatelům (kopírování atd.). Tyto údaje pak slouží k automatickému vyhodnocení při přístupu k objektům. K zaznamenání je možné využít kupř. standard PREMIS nebo metadatové schéma METS.

3. Strukturální metadata (structural metadata) reprezentují informace o vztazích či struktuře digitálního objektu nebo více digitálních objektů tvořících komplexní digitální objekt, a to jak pro jeho správu, tak zejména pro jeho zpřístupňování. Slouží k vyjádření struktury fyzické (např. různé reprezentace jednoho objektu) nebo logické (např. entity zatříděné v hierarchii spisového plánu, kapitoly jedné knihy atd.). Ve standardu METS slouží pro zachycení těchto metadat tzv. strukturální mapa v sekci <mets:structMap> (Zbyšek Stodůlka, viz literatura)

výstupní datový formát – legislativně definovaná skupina formátů stanovená s cílem zajistit standardizaci při výkonu spisové služby a dále zajištění udržitelnosti a čitelnosti při střednědobém a dlouhodobém uchovávání. Vyznačují se zejména otevřeností, minimalizací licenčních omezení, funkčností, rozšířením těchto formátů a mírou implementace, dostatečně mírou záznamu informace, relativní složitostí a dostatečným rozsahem vlastního popisu v podobě dokumentace. V případě, že původce vykonává spisovou službu v elektronickém systému spisové služby, zajistí příjem dokumentů minimálně v rozsahu výstupních formátů (nebo formátů dokumentů, které jsou výstupem z autorizované konverze dokumentů obsažených v datové zprávě), v případě, že tak není možné učinit ani ve spolupráci s archivem zajistí jejich převod do analogové podoby a dále převedení dokumentů v digitální podobě do výstupního datového formátu při: a) výstupu z elektronického systému spisové služby, b) ukládání ve spisovně, která je součástí elektronického systému spisové služby, c) při předávání do digitálního archivu. Původce nevykonávající spisovou službu v elektronické podobě v elektronických systémech spisové služby, převede dokument v digitální podobě určený k výběru archiválií mimo skartační řízení do výstupního datového formátu nejpozději při přípravě výběru archiválií mimo skartační řízení, pokud to není možné ani ve spolupráci s archivem, převede je do analogové podoby. Rozlišují se následující kategorie dokumentů:

1) Statické textové dokumenty a statické kombinované textové a obrazové dokumenty:

a) Portable Document Format for the Long-term Archiving (PDF/A, ISO 19005)

2) Statické obrazové dokumenty:

a) datový formát Portable Network Graphics (PNG, ISO/IEC 15948),

b) datový formát Tagged Image File Format (TIF/TIFF, revize 6 – nekomprimovaný),

c) datový formát Joint Photographic Experts Group File Interchange Format (JPEG/JFIF, ISO/IEC 10918)

3) Dynamické obrazové dokumenty:

a) datový formát umožňující uložení komprimovaných dat kódovaných podle standardu Moving Picture Experts Group Phase 2 (MPEG-2, ISO/IEC 13818),

b) datový formát umožňující uložení komprimovaných dat kódovaných podle standardu Moving Picture Experts Group Phase 1 (MPEG-1, ISO/IEC 11172),

c) datový formát Graphics Interchange Format (GIF).

4) Zvukové dokumenty:

a) datový formát umožňující uložení komprimovaných dat kódovaných podle standardu MPEG-1 Audio Layer II nebo MPEG-2 Audio Layer II (MP2),

b) datový formát umožňující uložení komprimovaných dat kódovaných podle standardu MPEG-1 Audio Layer III nebo MPEG-2 Audio Layer III (MP3),

c) datový formát Waveform audio format (WAV), modulace Pulse-code modulation (PCM)

5) Databáze:

a) Extensible Markup Language Document (XML) s popisem jeho struktury pomocí schématu XML

b) Document Type Definition (DTD), o kterém veřejnoprávní původce vede dokumentaci.

6) účetní doklady v elektronické podobě obsahující fakturu:

a) Information System Document (ISDOC) verze 5.2 a vyšší

b) datový formát, který je v souladu s evropskou normou pro sémantický datový model základních prvků elektronické faktury a syntaxí podle směrnice Evropského parlamentu a Rady č. 2014/55/EU ze dne 16. dubna 2014 o elektronické fakturaci při zadávání veřejných zakázek

b1) CII (Cross Industry Invoice) – reprezentované formátem XML

b2) UBL (Universal Business Language) – reprezentované formátem XML

DOPLŇUJÍCÍ LITERATURA

ČSN ISO 14721. Systémy pro přenos dat a informací z kosmického prostoru – Otevřený archivační informační systém - Referenční model. Praha: Český normalizační institut, 2014;

Oznámení Ministerstva vnitra, kterým se zveřejňuje vzorový provozní řád archivu oprávněného k ukládání archiválií v digitální podobě. VMV čá. 65/2012 (část II). Dostupné na https://www.mvcr.cz/soubor/65-vmv-pdf.aspx, citováno 29.6.2020.

HUTAŘ, Jan. Digitalizace, popis pomocí metadat a jejich formáty. Disertační práce. [online] Praha: 2012. [cit. 2021-09-30] Dostupné z: https://is.cuni.cz/webapps/zzp/detail/25756/

Corrado, Edward M. and Heather Lea Moulaison. *Digital Preservation for Libraries, Archives, and Museums*. Rowman and Littlefield, 2014. ISBN: 978-0-8108-8712-1.

10.-11. Specializované archivní programy.

OBECNÉ CÍLE

1. . Seznámit se s nejdůležitějšími specializovanými archivními programy a jejich využitím.

STUDIJNÍ MATERIÁLY

BÁRTA, Stanislav (red.) – BRZOBOHATÁ, Hana – ČERVENÁ, Radana – JELÍNEK, Jiří – STODŮLKA, Zbyšek – ZEMÁNKOVÁ, Michaela. Digitální archivnictví. FF MU : Brno, 2018. Dostupné z https://munispace.muni.cz/library/catalog/view/1407/3886/1725-1/0#preview citováno dne 30.9.2021.

Metodický pokyn č. 1/2021 odboru archivní správy a spisové služby, kterým se vydávají Základní pravidla pro zpracování archiválií ver. 3.0 (č. j. MV- 23313-5/AS-2021), dostupné z https://www.mvcr.cz/clanek/metodiky.aspx?q=Y2hudW09Mw%3D%3D citováno dne 30.9.2021.

Metodický návod č. 1/2012 odboru archivní správy a spisové služby MV k vedení evidence Národního archivního dědictví. dostupné z https://www.mvcr.cz/clanek/metodiky.aspx?q=Y2hudW09Mg%3d%3d citováno dne 30.9.2021.

Centrální Archivní Modul. Dokumentace 1.0, dostupné z https://cam.nacr.cz/doc/index.html.

Elektronické zpracování archiválií. Dokumentace 2.0, dostupné z http://elza-doc.lightcomp.cz/.

Provozní řád informačního systému Evidence Národního archivního dědictví na Národním archivním portálu. Dostupný na https://www.mvcr.cz/soubor/provozni-rad-is-peva-ii.aspx. citováno dne 30.9.2021.

Provozní řád informačního systému Evidence Centrálního archivního modulu. Není doposud oficiálně vydán, jakmile proběhne vydání, bude přístupný v kanálu Týmu Archivistika 4 v univerzitních Teams.

DÍLČÍ ÚKOLY

1. **K čemu slouží program PEvA a jakého prostředí je součástí?**
2. **K čemu slouží programy ELZA a ProArchiv?**
3. **K čemu jsou využívány evidenční jednotky v rámci programu PEvA, ELZA a ProArchiv?**
4. **K čemu slouží program CAM?**
5. **V jakých možných rolích vystupuje archivář, pokud pracuje s programem CAM?**

Praktické ukázky budou provedeny při výuce, studenti obdrží individuální přístupy do vybraných softwarů a k Moodle kurzu ELZA 2021.

DOPLŇUJÍCÍ LITERATURA

SULITKOVÁ, Ludmila. *Archivnictví a spisová služba*. Ústí nad Labem: Filozofická fakulta, Univerzita Jana Evangelisty Purkyně v Ústí nad Labem ve spolupráci s nakladatelstvím Scientia, spol. s r.o., 2017. Acta Universitatis Purkynianae Facultatis philosophicae. ISBN 978-80-7561-027-0.; Dostupné též z: http://ff.ujep.cz/archivnictvi/spisova_sluzba.pdf, citováno dne 29. 06. 2020

Metodický pokyn č. 3/2017 odboru archivní správy MV k vedení evidence původců pomocí programu PEvA ver. 02 (2018), dostupné z https://www.mvcr.cz/clanek/metodiky.aspx?q=Y2hudW09Mg%3d%3d

citováno dne 30.9.2021.

16. Digitální archiv, péče od digitální archiválie.