

1.02 Pregledni znanstveni članek

UKD 930.25:004.9:504.4(497.4)

Prejeto: 30. 10. 2024

Varstvo arhivskega gradiva v digitalni obliki pred naravnimi nesrečami

ŽIGA KONCILIJA

dr. zgodovinskih znanosti, višji svetovalec – arhivist za gradivo uprave po letu 1945

Arhiv Republike Slovenije, Poljanska cesta 40, SI-1000 Ljubljana

e-pošta: ziga.koncilija@gov.si

Izvleček

Varstvo arhivskega gradiva pred naravnimi nesrečami je ključno za zagotavljanje dostopnosti, trajnosti in integritete hranjenih podatkov. Naravne nesreče, kot so poplave, požari, potresi in nevihte, lahko povzročijo poškodbe ali celo izgubo, ne samo arhivskega gradiva v fizični obliki, temveč vedno bolj tudi v digitalni obliki. Zato morajo vsak ustvarjalec javnega arhivskega gradiva in tisti, ki takšno gradivo hranijo, pripraviti in sprejeti celovit pristop k varstvu arhivskega gradiva. Avtor v prispevku predstavi ključno orodje za zagotavljanje varne hrambe dolgoročne hrambe gradiva v digitalni obliki, in sicer oceno tveganj kot ključni integralni del notranjih pravil za zajem in hrambo gradiva v digitalni obliki. V prispevku so ponujena tudi nekatera temeljna izhodišča za pripravo ocene tveganj in ukrepov za obvladovanje tveganj, s poudarkom na obvladovanju okoljskih tveganj.

Ključne besede:

arhivsko gradivo
v digitalni obliki,
digitalno gradivo,
naravne nesreče,
notranja pravila,
ocena tveganja

Abstract

PROTECTION OF DIGITAL ARCHIVAL MATERIALS FROM NATURAL DISASTERS

Protection of archival materials from natural disasters is crucial for ensuring the accessibility, durability and integrity of stored data. Natural disasters such as floods, fires, earthquakes and storms can cause damage or even loss, not only of archival materials in physical form, but increasingly also in digital form. Therefore, every creator of public archival materials and those who store such materials must prepare and adopt a comprehensive approach to the protection of archival materials. In the article, the author presents a key tool for ensuring the safe long-term preservation of materials in digital form, namely risk assessment as a key integral part of internal rules for the capture and storage of materials in digital form. With a focus on environmental risk management, the article also provides some fundamental starting principles for creating a risk assessment and risk management measures.

Key-words:

archival materials
in digital form,
digital materials,
natural disasters,
internal rules,
risk assessment

Uvod

Naravne nesreče so izredni dogodki, ki jih lahko povzročijo naravne sile, kot so to na primer potresi, zemeljski plazovi, nevihte, poplave, suše, požari, pomebe, toča, žled, sneg in drugo. Vendar vseh naravnih nesreč vendarle ne moremo pripisati naravnim procesom, ki se odvijajo v ali okoli Zemlje. Nekatere naravne nesreče v zadnjih desetletjih imajo že izdatne antropogene vzroke, torej so posledica človekovega pretiranega in nepremišljenega poseganja v naravo. Najočitnejše se to izraža zlasti ob globalnem segrevanju ozračja. Vse pogostejše se pojavljajo, ponekod tudi prvič v takšnem obsegu, obsežne poplave, hujša neurja, suše in požari ter druge naravne katastrofe, ki ogrožajo življenja ljudi in povzročajo večjo ali manjšo materialno škodo.

Ko pomislimo na posledice naravnih nesreč, se nam pred očmi slikajo podobe porušenih, požganih ter poplavljenih mest, vasi in pokrajin. Nam, arhivistom, pa se nehote prikazujejo podobe poplavljenega, požganega ali kako drugače uničenega arhivskega gradiva. Le bežen prelet tovrstnih dogodkov nam ponudi množico primerov naravnih nesreč in, trenutno sicer še, primerov ogrožanja arhivskega gradiva v fizični obliki. Pred kratkim, junija 2024, je na primer strela na Barbadosu zanetila požar, v katerem je zgorelo arhivsko gradivo mestnih svetov, glavnih bolnišnic in drugo, za državo izjemno pomembno arhivsko gradivo.¹ Bližje nam je primer, ko je, sicer kot posledica človeških dejanj, ob demonstracijah v Sarajevu 7. februarja 2014 požar pogoltnil večjo količino neprecenljivega arhivskega gradiva iz obdobja Avstro-Ogrske.² Med njimi tudi dokumentov, ki se nanašajo na atentat na nadvojvodo Franca Ferdinanda, ki je sprožil prvo svetovno morijo. 24. aprila 2014 je bil, v požaru arhivskega gradiva v Portorožu, med drugim izgubljen tudi arhiv Obalnih galerij Piran.³

6. februarja 2023 je Turčijo, predvsem provinco Gaziantep, prizadel silovit potres, v katerem je bila porušena tudi glavna upravna stavba province.⁴ Uničeno upravno dokumentarno gradivo je posledično zavrlo številne upravne, sodne in druge postopke. Nam najbližja in najbolj uničujoča je bila vsekakor naravna katastrofa v obliki poplav, ki so 4. avgusta 2023 prizadele večji del Slovenije in poleg velike gmotne škode prizadele tudi precej arhivskega gradiva na različnih lokacijah po Sloveniji.⁵

Iz le nekaj primerov lahko hitro razberemo, kako uničujoč in kompleksen vpliv imajo lahko naravne nesreče na arhivsko gradivo v fizični obliki, ki ga sicer poskuša zavarovati 36. člen Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih (dalje ZVDAGA).⁶ Ta določa, da se mora »... arhivsko gradivo v fizični obliki trajno in strokovno neoporečno hraniti v ustreznih prostorih in opremi, v ustreznih klimatskih pogojih, zavarovano pred vlomom, požarom, vodo, biološkimi, kemičnimi, fizikalnimi in drugimi škodljivimi vplivi (materialno varstvo)«.

Vendarle moramo v trenutnih razmerah, ko prihaja do eksponentne rasti digitalnih zapisov oziroma podatkov, pozornost nekoliko spremeniti ter bistveno več časa in pozornosti nameniti tudi varstvu gradiva v digitalni obliki. Digitalno gradivo je hranjeno na različnih nosilcih digitalnih podatkov, bodisi na prenosnih bodisi statičnih nosilcih. Ti tako postajajo ključni subjekti varovanja in različnih varnostnih ukrepov oziroma politik ter strategij, torej tudi subjekti varovanja pred naravnimi nesrečami. Arhivska zakonodaja je v ta namen uvedla

¹ Fleary: Caribbean historical archives destroyed in fire.

² Bešić: Nakon stradanja građe u požaru 2014.

³ Cek: Zgoreli so katalogi in del arhiva.

⁴ Turkey's quake trials blocked due to archive lost in hastily demolished municipality building.

⁵ Več o tem glej npr. v zborniku: *Arhivi v primežu narave in tehnologije*.

⁶ Zakon o varstvu dokumentarnega in arhivskega gradiva ter o arhivih.

instrument notranjih pravil za zajem in hrambo digitalnega gradiva,⁷ ki vključuje oceno in upravljanje tveganj. Pomemben vidik tega procesa je tudi ocena tveganj pred naravnimi nesrečami.

Arhivsko gradivo v digitalni obliki in podatkovni nosilci

Toda še prej razjasnimo pojme, kaj arhivska zakonodaja sploh razume pod pojmom arhivsko gradivo v digitalni obliki. ZVDAGA v 2. členu opredeli nekatere izmed osnovnih pojmov. Dokumentarno gradivo so vse vrste in oblike zapisov, ki so nastali ali bili prejeti pri poslovanju pravnih in fizičnih oseb. Medtem, ko je arhivsko gradivo tisti del dokumentarnega gradiva, ki ima trajen pomen za zgodovino, druge znanosti in kulturo ali trajen pomen za pravni interes pravnih in fizičnih oseb. ZVDAGA opredeljuje, da se lahko dokumentarno, in s tem torej tudi arhivsko gradivo, nahaja v več različnih pojavnih oblikah, in sicer v fizični, analogni, digitalni ter elektronski obliki.

Gradivo v fizični obliki je tisto, ki je hranjeno na fizičnem nosilcu zapisa. Gradivo v elektronski obliki je gradivo tako v analogni kot digitalni obliki. Analogno gradivo je v analognem zapisu shranjeno na strojno berljivem nosilcu zapisa (npr. mikrofilm, vinilne plošče, kompaktne avdio kasete, VHS-kasete). Gradivo v digitalni obliki je na strojno berljivem nosilcu zapisa zapisano v binarni⁸ obliki zapisa. Nas v članku bolj specifično zanima slednje, torej arhivsko gradivo v digitalni obliki, oziroma če smo natančni, digitalno gradivo na nosilcih in v formatih, primernih za učinkovito dolgoročno hrambo.⁹ Digitalno ohranjanje arhivskega gradiva, če dejavnost razumemo kot »... *aktivno upravljanje digitalnih vsebin skozi čas z zagotavljanjem dolgoročnega dostopa*«, je, in predvsem bo v prihodnosti, tudi ena izmed osnovnih dejavnosti vseh arhivov.¹⁰

Z vidika varovanja arhivskega gradiva je ključna tudi izvirnost digitalnega gradiva. Glede na izvor digitalnega gradiva ločimo digitalizirano gradivo in izvorno digitalno gradivo. Digitalizirano gradivo je tisto, ki je bilo iz analogne ali fizične oblike pretvorjeno v digitalno oziroma binarno obliko zapisa. Izvorno digitalno gradivo (angl. *born-digital archival materials*) označuje gradivo, ki je bilo ustvarjeno neposredno v digitalni obliki in nikoli ni obstajalo v fizični obliki. Takšno gradivo vključuje zapise, ki so bili ustvarjeni, shranjeni in uporabljeni izključno v digitalnih formatih. Razlikovanje med tema dvema vrstama gradiva je ključno za razvoj ustreznih strategij za njihovo dolgoročno hrambo in varovanje.

Pravilnik o enotnih tehnoloških zahtevah za zajem in hrambo gradiva v digitalni obliki (dalje PETZ) v 3. členu¹¹ podrobneje opredeli vrste arhivskega gradiva v digitalni obliki, in sicer kot: besedilne in mešane dokumente, filmsko in avdiovizualno gradivo, spletne strani, elektronsko pošto, podatkovne zbirke in uradne evidence ter prostorske podatke.

Med najpogostejše oblike izvorno digitalnega arhivskega gradiva sodijo sporočila in priponke, ki so poslani in prejete po elektronski pošti. Sem spadajo tudi zapisi oziroma datoteke, ustvarjene z različnimi namenskimi programi, kot so: urejevalniki besedil (npr. Microsoft Word, Google Docs, Open Office, PDF),

⁷ Več glej npr. v: Antončič: Vzorčna notranja pravila? O čem pravzaprav sploh govorimo, str. 465–480.

⁸ Binarni ali dvojiški sistem, znan tudi kot binarna koda, je način zapisovanja podatkov z uporabo dveh simbolov: 0 in 1. V binarni kodi so v najosnovnejši obliki zapisani vsi procesi, ki jih računalnik obdeluje in izvaja.

⁹ Več o tej problematiki glej npr.: Hajtnik: Pretvorba e-dokumentov v formate za dolgoročno hrambo na osnovi standarda ISO 13008.

¹⁰ Corrado in Moulaison Sandy: *Digital preservation for libraries, archives and museums*, str. 3.

¹¹ Pravilnik o enotnih tehnoloških zahtevah.

preprostejši urejevalniki podatkovnih baz (npr. Excel, Microsoft Access) in programska oprema za ustvarjanje predstavitev (npr. PowerPoint, Canva, Slides). Pomembno kategorijo digitalnega arhivskega gradiva predstavljajo tudi digitalne fotografije, bodisi posnete z digitalnimi fotoaparati ali s pametnimi telefoni bodisi zajete z drugimi digitalnimi napravami. Te fotografije so shranjene v različnih formatih, med najpogostejšimi so JPEG, TIFF, GIF. Še posebej prostorsko zahtevna kategorija digitalnega gradiva vključuje podatke geografskih informacijskih sistemov (GIS) v različnih vektorskih in rasterskih formatih ter množico avdio in zlasti video zapisov. Slednji so lahko posneti z digitalnimi kamerami, s pametnimi telefoni ali ustvarjeni z računalniško programsko opremo, pri čemer so med najpogostejšimi formati VAW, MOV, MP4 ali MP3. Med digitalno gradivo sodijo tudi spletne strani in vsebine, objavljene na spletnih straneh, blogih, forumih in družbenih omrežjih, pri čemer se uporabljajo različni formati, kot so HTML, CSV, JSON, XML ali drugi specifični formati, ki se uporabljajo za strukturiranje in prikaz podatkov na spletnih straneh. Še ena ključna kategorija digitalnih podatkov so zbirke podatkov, ustvarjene in shranjene v digitalni obliki. Te zbirke podatkov se pogosto upravljajo s sistemi za upravljanje podatkovnih zbirk,¹² kot so Microsoft SQL, Oracle in različne NoSQL-rešitve.

Zbirka vseh znanih formatov digitalnega gradiva je sicer zbrana v tehničnem registru britanskega nacionalnega arhiva, imenovanem PRONOM.¹³ Medtem ko je Arhiv Republike Slovenije pripravil dokument, ki vsebuje priporočljive formate digitalnega gradiva, primerne za dolgoročno hrambo.¹⁴

Podatkovni nosilci,¹⁵ na katerih se arhivsko gradivo v digitalni obliki fizično nahaja, so raznovrstni in številni. Med zgodnje oblike podatkovnih nosilcev spadajo luknjaste kartice, ki so se uporabljale od 50. let 20. stoletja. Kasneje so jih nadomestili bolj sofisticirani pomnilniki, kot so HDD (*Hard Disk Drive*) ali »trdi«¹⁶ diski, kjer so podatki zapisani z magnetno tehnologijo na plošče iz aluminija ali stekla. Danes so razširjeni SSD-diski (angl. *Solid State Drive*), ki ne vsebujejo gibljivih delov in temeljijo na polprevodniški tehnologiji za zapisovanje binarnih podatkov. Kot prenosne medije poznamo iz preteklosti različne diskete, zlasti velikosti 5,25 in 3,5 palca, ki so omogočale magnetni način zapisa podatkov. Te so kasneje zamenjali optični diski, kot so CD (angl. *Compact Disc*), DVD (angl. *Digital Video Disc*) in BD (angl. *Blu-ray Disc*), ki uporabljajo lasersko tehnologijo za zapisovanje. V sodobnem času prevladujejo prenosni pomnilniki, kot so USB-ključki (angl. *Universal Serial Bus*), SD-pomnilniške kartice (angl. *Secure Digital*) in druge oblike kompaktnih pomnilnikov. Za dolgoročno hrambo arhivskega gradiva se pogosto uporabljajo tehnologije, kot je LTO (angl. *Linear Tape-Open*), ki omogoča zapis podatkov na trakove v posebnih podatkovnih postajah. Tovrstno tehnologijo na primer uporablja Slovenska javna arhivska služba. V zadnjem času so za dolgoročno hrambo podatkov vse bolj prisotne rešitve podatkovnih skladišč, zlasti tiste v obliki oblčnih storitev. Te vključujejo državne računalniške oblake, kot je slovenska različica državnega računalniškega oblaka,¹⁶ hibridne in zasebne računalniške oblake, ki jih ponujajo največja tehnološka podjetja, kot so Google, Amazon in drugi.¹⁷

¹² *Data Base Management Systems*. Gre za zahtevnejše programe za vodenje podatkovnih zbirk, ki omogočajo večjo stopnjo programabilnosti in urejanja dostopnih pravic.

¹³ Tehnični register PRONOM.

¹⁴ Seznam oblik zapisa, primernih za dolgoročno hrambo gradiva v digitalni obliki.

¹⁵ Več o tej problematiki glej npr. Hribar: Pomembnost nosilcev podatkov digitalnega gradiva v arhivistiki.

¹⁶ Državni računalniški oblak (DRO) predstavlja računalniško infrastrukturo za neposredne proračunske uporabnike in jim nudi shranjevalne, razvojne, poslovne in druge zmogljivosti v obliki storitev ter možnost, da z uporabo koncepta računalništva v oblaku hitro dosežejo svoje poslovne cilje.

¹⁷ Več o tem glej Beagrie: How Cloud Storage can address the needs of public archives in the UK.

Vsak nosilec digitalnih podatkov ima svoje prednosti in slabosti, tako z vidika prenosljivosti, hrambe in dostopnosti kot z vidika varnosti (vključno z zaščito pred naravnimi nesrečami) in učinkovite dolgoročne hrambe.¹⁸ Premišljena izbira ustreznega nosilca je tako ključna za učinkovito in varno ohranjanje digitalnega gradiva.

Izzivi dolgoročne hrambe digitalnega arhivskega gradiva in okoljska tveganja

Izvorno digitalno in digitalizirano arhivsko gradivo predstavlja vse večji delež gradiva, ki ga ustvarjajo in hranijo sodobni ustvarjalci javnega arhivskega gradiva in arhivi.¹⁹ Hkrati so izzivi dolgoročne hrambe nekoliko drugačni in bolj zapleteni kot izzivi varovanja fizičnega arhivskega gradiva, saj zahtevajo posebne pristope ter tehnologije za zagotavljanje dolgoročne hrambe in dostopnosti.²⁰

Digitalni zapisi so podvrženi tehnološkemu staranju in nenehnim spremembam formatov, zato je treba skrbno načrtovati krovne politike dolgoročne hrambe, procesov pretvorbe formatov in migracije podatkov. Zagotavljati je treba, da digitalno gradivo ostaja ves čas hrambe dolgoročno celovito, avtentično in nespremenjeno, kar je ključnega pomena za ohranitev vrednosti podatkov in njihovo pravno veljavnost. Zagotoviti je treba, da je digitalno gradivo dostopno ves čas hrambe, kljub spremembam tehnologij, informacijskih sistemov in programske opreme. Ustvarjanje in vzdrževanje ustreznih metapodatkov sta prav tako ključni za organizacijo, predvsem z vidika iskanja in razumevanja digitalnih zapisov. Zaščititi je treba informacijske sisteme, podatke in nosilce podatkov pred izgubo, krajo ali nepooblaščenim dostopom. In navsezadnje, podatke in nosilce podatkov, sisteme in prostore, kjer se nosilci podatkov nahajajo (npr. diskovna polja, strežniške sobe), je treba zaščititi pred celotnim spektrom okoljskih tveganj.

Arhivi in drugi ustvarjalci arhivskega gradiva uporabljajo različne prakse za učinkovito upravljanje in dolgoročno hrambo digitalnega gradiva. Med najpogostejše ukrepe spada standardizacija formatov, torej uporaba odprtih in standardiziranih formatov, ki so odpornejši proti tehnološkim spremembam (npr. PDF/A za dokumente, TIFF za fotografije itn.). Pomembni sta tudi načrtovanje in izvajanje rednih migracij podatkov na nove formate ali nosilce, ko obstoječi postanejo zastareli. S tem se zagotavlja ohranjanje dostopnosti in uporabnosti gradiva skozi čas. Praksa vključuje tudi izvajanje rednih varnostnih kopiranj ter shranjevanje digitalnih zapisov na več fizično ločenih in ustrezno oddaljenih lokacijah (npr. najmanj na treh, med seboj oddaljenih lokacijah).

Ključnega pomena je uporaba ustreznih arhivskih informacijskih sistemov, ki omogočajo dolgoročno hrambo arhivskih zapisov, upravljanje njihovih metapodatkov in dostopanje do hranjenega digitalnega arhivskega gradiva. Priporočljiva je uporaba specializiranih podatkovnih skladišč za upravljanje digitalnih arhivskih zapisov, kot so Fedora,²¹ DSpace,²² Archivematica²³ ali Pre-

¹⁸ Povzeto po Legget: *Digitization and digital archiving: a practical guide for librarians*, str. 63–129.

¹⁹ Več o vlogi Arhiva Republike Slovenije na področju vzpostavljanja elektronskega arhiva glej Hajtnik: Učinkovito dolgoročno ohranjanje arhivskega gradiva v Arhivu RS.

²⁰ Malak: 10 Challenges of Digital Preservation.

²¹ Fedora je družina orodij, zasnovanih na operacijskem sistemu Linux, ki je v uporabi tudi v Slovenski javni arhivski službi.

²² DSpace je odprtokodni informacijski sistem, ki omogoča hrambo in dostopanje do vseh vrst digitalnega gradiva.

²³ Archivematica je odprtokodna družina programskih orodij, ki omogočajo obdelavo in hrambo arhivskega gradiva skladno z OAIS-referenčnim modelom.

servica.²⁴ Poleg tega je koristna tudi uporaba orodij za organizacijo, iskanje in upravljanje digitalnih dokumentov (npr. SharePoint, Alfresco, mSef) in sistemov za upravljanje metapodatkov (npr. scopeArchiv),²⁵ ki omogočajo ustvarjanje, shranjevanje in upravljanje metapodatkov hranjenega digitalnega arhivskega gradiva. Za dolgoročno uspešno upravljanje je priporočljiva implementacija arhivskih in drugih digitalnih standardov, kot sta OAIS²⁶ (angl. *Open Archival Information System*) in PREMIS (angl. *Preservation metadata*).²⁷ Za ohranjanje celovitosti oziroma avtentičnosti gradiva je ključno vzdrževanje revizijskih sledi vseh opravljenih postopkov, povezanih z upravljanjem digitalnega gradiva, kar omogoča transparentnost in sledljivost vseh izvedenih dejavnosti.

Kot smo v uvodu, sicer pretežno na primerih fizičnega arhivskega gradiva, že nakazali, predstavljajo enega izmed ključnih in najbolj destruktivnih tveganj, v prihodnosti tudi za arhivsko gradivo v digitalni obliki, ravno naravne nesreče.²⁸ Naravne nesreče spadajo v skupino t. i. okoljskih tveganj, ki vključujejo:

- Splošne naravne nesreče, kot so potresi, poplave in požari,
- naravne nesreče, ki so neposredna posledica človeških dejavnosti, na primer nesreče, in sicer zaradi industrijskih procesov,
- naravne nesreče, ki so posledica podnebnih sprememb oziroma posrednih človeških posegov v naravno okolje, kot so naraščajoče ekstremne vremenske razmere, taljenje ledu ali dvig morske gladine.

Učinki okoljskih tveganj so raznovrstni in uničujoči. Od širših vplivov na celotno družbo, državo in politike do ožjih vplivov na gospodarstvo in posamezne družbene sektorje. Vpliv na arhivski sektor je prav tako lahko občuten in potencialno uničujoč. Naravne nesreče lahko prizadenejo arhive kot celoto. Ogrožajo lahko nepremičnine in prostore, kjer se hrani arhivsko gradivo. Poškodovana energetska infrastruktura lahko posredno vpliva na dobavo elektrike ali drugih energentov. Lahko sta ogroženi življenje in zdravje zaposlenih. Navsezadnje, naravne nesreče neposredno ogrožajo delovanje informacijskih sistemov in nosilcev podatkov kot takšne, s čimer so ogroženi tudi arhivski digitalni zapisi.

Nenadno tresenje tal lahko povzroči veliko škode na nepremičninah in energetski infrastrukturi, kar lahko posledično vodi do poškodb in uničenja digitalnih arhivskih zapisov. Čezmerna količina vode, ki preplavi prostore in energetska infrastrukturo, lahko uničujoče ogrozi digitalno arhivsko gradivo. Enako destruktiven do prostorov, infrastrukture in neposredno digitalnega arhivskega gradiva je lahko tudi ogenj.

Učinkovito upravljanje okoljskih tveganj je tako ključno ter zahteva celovit pristop, ki vključuje sodelovanje celotne države in vodstev, zakonodaje, energetskega in informacijsko-tehnološkega sektorja, ustvarjalcev arhivskega gradiva, ponudnikov storitev in opreme ter neposredno arhivov oziroma zaposlenih v kulturni in arhivski dejavnosti. Za varstvo digitalnega arhivskega gradiva, tako pri ustvarjalcih kot v arhivih, je slovenska arhivska zakonodaja uvedla eno izmed ključnih orodij za zaščito gradiva v digitalni obliki, in sicer notranja pravila ter znotraj njih oceno in upravljanje tveganj.

²⁴ Preservica zagotavlja zanesljivo hrambo in dostopanje do hranjenega gradiva ne glede na vrsto formatov.

²⁵ ScopeArchiv je namensko programsko orodje, ki ga uporablja Slovenska javna arhivska služba, namenjeno strokovni obdelavi arhivskega gradiva, konkretno urejanju metapodatkov arhivskega gradiva, ki so dodani v procesu strokovne obdelave.

²⁶ Več glej Kavčič-Čolić: Teoretični model digitalnih arhivov, str. 63–75.

²⁷ PREMIS je mednarodni standard oziroma baza metapodatkov za podporo dolgoročne hrambe digitalnih objektov in za zagotovitev uporabljivosti teh.

²⁸ Več o tem glej Natek: Temeljni termini v geografiji naravnih nesreč, str. 73–101.

Notranja pravila kot ključen varnostni mehanizem varovanja gradiva v digitalni obliki

Naravnih nesreč seveda ne moremo preprečiti, vendar pa lahko zmanjšamo vpliv, ki ga imajo na arhivsko gradivo v digitalni obliki.²⁹ ZVDAGA (39. člen) določa, da morajo, »... javnopravne osebe skrbeti za ohranjanje, materialno varnost, celovitost in urejenost dokumentarnega gradiva, ki ga prejemajo ali nastaja pri njihovem delu, dokler ni iz tega gradiva odbrano arhivsko gradivo«. To se seveda nanaša tudi na gradivo v digitalni obliki.

Kot ključna orodja za varstvo gradiva v digitalni obliki sicer arhivska zakonodaja od ustvarjalcev javnega arhivskega gradiva zahteva, da mora biti uporabljena strojna in programska oprema certificirana³⁰ pri Arhivu Republike Slovenije, prav tako morajo biti certificirane najete storitve povezane z digitalnim gradivom in navsezadnje, javnopravna oseba mora imeti sprejeta ali potrjena notranja pravila, ki jih mora tudi dokazljivo izvajati in posodabljalati.

Notranja pravila so, glede na 2. člen ZVDAGA, pravila, »... ki jih kot svoj interni pravni akt sprejme oseba glede izvajanja zajema in dolgoročne hrambe svojega dokumentarnega in arhivskega gradiva v digitalni obliki ter spremljevalnih storitev, ali ponudnik storitev glede izvajanja zajema in dolgoročne hrambe oziroma spremljevalnih storitev«. Glede na to, kdo jih je pripravil in čigavo je gradivo, katerega upravljanje urejajo, ločimo pravila za lastno poslovanje, notranja pravila za izvajanje storitev ali vzorčna notranja pravila.

Notranja pravila morajo, glede na 18. in 19. člen ZVDAGA, sprejeti vse javnopravne osebe, ki zajemajo ali hranijo gradivo v digitalni obliki, ter ponudniki storitev, medtem ko jih morajo v potrditev Arhivu Republike Slovenije predložiti vse javnopravne osebe, razen organov državne uprave.

Notranja pravila so ključnega pomena, saj omogočajo ureditev in usklajitev ravnanja z digitalnim gradivom skladno z zakonskimi zahtevami, vključno z varovanjem podatkov pred naravnimi nesrečami. Z njihovo pomočjo se zagotavlja učinkovita in varna hramba gradiva v digitalni obliki, kar omogoča ohranitev njegove pravne ali druge veljavnosti. Kot določa 31. člen ZVDAGA, »... se vsaka enota varno hranjenega gradiva v digitalni obliki šteje za enako posamezni enoti izvirnega gradiva, če sta bila zajem in varna hramba opravljena v skladu s tem zakonom, njegovimi podzakonskimi predpisi, pri državnem arhivu potrjenimi notranjimi pravili«. S tem notranja pravila zagotavljajo pravni okvir za pravilno hrambo in varovanje gradiva ter prispevajo k dolgoročni zaščiti in veljavnosti digitalnih zapisov.

Kot ključno orodje varstva pred naravnimi nesrečami v notranjih pravilih med drugim predstavlja ocena tveganj. V 6. členu Uredba o varstvu dokumentarnega in arhivskega gradiva (dalje UVDAG)³¹ določa, da mora vsaka javnopravna oseba v zvezi z varstvom dokumentarnega in arhivskega gradiva v digitalni obliki določiti obseg poslovanja, ki bo urejen z notranjimi pravili, popisati vrste in vire dokumentarnega in arhivskega gradiva v digitalni obliki, izvesti oceno veljavnega informacijskega sistema in informacijske varnosti, določiti zahteve za zajem, hrambo in spremljevalne storitve, pripraviti načrt za zajem, hrambo in spremljevalne storitve ter »... pripraviti oceno tveganj in ukrepe za njihovo upravljanje«.

PETZ v 57. členu podrobneje določa, da so osnovni sestavni deli ocene

²⁹ Več o zagotavljanju varne e-hrambe glej npr. Hajtnik: Vse, kar mora vodstvo organizacije vedeti o e-hrambi.

³⁰ Certifikacija je, glede na 86. člen ZVDAGA, postopek, v katerem Arhiv Republike Slovenije preverja skladnost opreme in storitev zajema, hrambe in spremljevalnih storitev z ZVDAGA. Pridobljen certifikat ponudnikom omogoča poslovanje z javnim sektorjem, pri čemer hkrati uporabnikom zagotavlja večjo varnost pri uporabi opreme in storitev.

³¹ Uredba o varstvu dokumentarnega in arhivskega gradiva.

tveganj; »... popis informacijskih sredstev in njihovi skrbniki, nevarnosti, prepoznane za posamezne skupine informacijskih sredstev, ranljivosti, prepoznane za posamezne skupine informacijskih sredstev, ocena verjetnosti in škode, če se nevarnost uresniči, ocena stopnje tveganja ter vrednotenje in ocena sprejemljive ravni tveganja«.

Pravilnik v istem členu nadalje določa, da mora ocena tveganj »... vključevati tveganja, povezana z lokacijami hrambe digitalnega gradiva, in sicer glede na potresno in poplavno ogroženost«. Po pravilniku se tudi določi odgovorna oseba, ki na podlagi dokumentirane in sprejete metodologije izdela in vzdržuje oceno tveganj, v kateri so prepoznana in obvladovana vsa tveganja, ki ogrožajo dostopnost, uporabnost, celovitost in avtentičnost³² gradiva v digitalni obliki. Odgovorna oseba za upravljanje tveganj »... vzdržuje dokument načrt za upravljanje tveganj, s katerim se za vsako prepoznano tveganje določi skrbnika tveganja in ukrepe za njegovo obvladovanje ter spremlja roke za uvedbo ukrepov«. Ocena tveganja se lahko dokumentira v več dokumentih in se ti vzdržujejo v okviru celotne dokumentacije notranjih pravil.

58. člen PETZ določa še, da mora odgovorna oseba za upravljanje tveganj zagotoviti, da sta »... ocena tveganj in načrt za upravljanje tveganj najmanj enkrat letno in ob spremembah tveganja posodobljena tako, da izražata dejansko stanje«. Arhivska zakonodaja na tak način že ponuja ustrezne temelje za varstvo digitalnega arhivskega gradiva oziroma za obvladovanje tveganj, povezanih z naravnimi nesrečami.

Ocena tveganj kot ključen element notranjih pravil

Ocena tveganj je proces, s katerim ocenjujemo potencialne nevarnosti in tveganja, ki bi lahko negativno vplivali na ljudi, premoženje, okolje ali poslovanje, povezano z digitalnim arhivskim gradivom. Ta proces je torej ključen tako za prepoznavanje in analizo tveganj kot za določanje ustreznih ukrepov za njihovo obvladovanje ali zmanjšanje. Ocena tveganja je dinamičen proces, ki zahteva stalno spremljanje in prilagajanje glede na spreminjajoče se okoliščine in nove informacije. Ta pristop se opredeljuje kot upravljanje tveganj, ki organizacijam omogoča učinkovitejše obvladovanje tveganj in posledično zmanjševanje njihovih negativnih vplivov.

Ključni koraki pri izvedbi ocene tveganj so: popis sredstev, identifikacija njihovih ranljivosti, identifikacija groženj in na podlagi tega ocena tveganj.³³

Popis sredstev je specifičen za vsako organizacijo posebej. Ključna so zlasti tista sredstva, ki jih želimo v kontekstu varstva digitalnega gradiva najbolje zaščititi. Običajno obsega popis zaposlenih (ključni so zlasti zaposleni, ki so vpleteni v postopke zajema in hrambe digitalnega gradiva), popis nepremičnin in prostorov (v kontekstu varstva digitalnega arhivskega gradiva pomembni prostori, npr. kjer se nahajajo strežniški prostori, diskovna polja, UPS³⁴-postaje itn.), popis celotne infrastrukture (električna napeljava, strojna oprema, komunikacijska oprema, varnostna oprema) in informacijskih sistemov (programska oprema, zlasti informacijski sistemi za zajem, obdelavo ter hrambo digitalnega gradiva in metapodatkov), vsi podatkovni nosilci ter navsezadnje popis vrst dokumentarnega in arhivskega digitalnega gradiva, ki nastaja ali je prejet pri določeni organizaciji. V oceno tveganja morajo biti zajete tudi morebitne zunanje

³² Gre za t. i. DUCAT – osnovna načela varne hrambe digitalnega gradiva: dostopnost, uporabnost, celovitost, avtentičnost in trajnost, ki izhajajo iz kombinacije osnovnih načel informacijske varnosti (t. i. CIA-triada) ter temeljnih načel ZVDAGA v členih 3. do 7.

³³ Glej npr. Metodologija obvladovanja tveganj informacijske varnosti v državni upravi.

³⁴ *Uninterruptible Power Supply*. Gre za sisteme za neprekinjeno napajanje, ki so ključni v primerih okvar električne infrastrukture.

najete storitve, povezane z zajemom in s hrambo digitalnega gradiva, kakor to določata 83. člen³⁵ in 82. člen PETZ.³⁶

Po opravljenem popisu sredstev sledi korak identifikacije nevarnosti oziroma groženj. Torej tistih groženj, ki lahko potencialno ogrožajo naša predhodno identificirana sredstva. V pomoč pri definiranju vrst groženj so nam lahko številni standardi, kot je npr. standard ISO 18128,³⁷ ki se osredotoča na kontekste groženj, ki lahko vplivajo na način upravljanja organizacije z dokumenti oziroma zapisi.

Kot prvo kategorijo standard razlikuje kontekste zunanjih groženj, ki so lahko posledica širših družbeno-političnih sprememb (npr. zakonodajne spremembe, nastajanje novih standardov, upad ugleda ali zaupanja v organizacijo, reorganizacije uprave). Grožnje, ki so lahko posledica kontekstov gospodarskih sprememb (reorganizacije, spremembe v ciljih organizacije). Nadalje standard loči kontekste groženj v obliki naravnih nesreč (potresi, orkani, cunamiji, poplave, požari, suše)³⁸ ter zunanjih varnostnih groženj v obliki nepooblaščenih dostopov, vdorov v sistem, fizičnih vdorov v prostore, uporabe zlonamerne programske opreme in DDoS³⁹ napadov.

Drugo kategorijo groženj predstavljajo »notranji« konteksti, ki so povezani z organizacijo kot takšno (npr. notranje reorganizacije, nove sistemizacije delovnih mest), s tehnološkimi spremembami (npr. spremembe delovnih postopkov, novi načini zajema in hrambe digitalnega gradiva), z zaposlenimi in njihovimi kompetencami (npr. odhajanje kadra, neprimerne kompetence), ter grožnje, povezane z zagotavljanjem zadostnih finančnih sredstev.

Tretjo kategorijo predstavljajo konteksti groženj, uperjeni neposredno proti informacijskim sistemom za upravljanje z zapisi. Sem sodijo grožnje, ki so povezane s strukturo sistema kot takšno (npr. sprememba sistemov mimo naših potreb, vdori v sistem, spreminjanje formatov za dolgoročno hrambo zapisov), s primernim vzdrževanjem in kontinuiteto sistema ter s primerno usposobljenostjo zaposlenih (sistemskih administratorjev in uporabnikov sistema).

Četrta kategorija kontekstov groženj je usmerjena neposredno na digitalne zapise oziroma podatke ter njihove metapodatke (npr. nepooblaščen dostopanje, spreminjanje ali uničevanje podatkov iz strani zaposlenih). Posledice neupoštevanja kontekstov in identifikacije vseh groženj so lahko uničenje, izguba ali poškodovanje dokumentov, ki tako niso več uporabni, zanesljivi, avtentični, celoviti in kot taki ne izpolnjujejo več namena, zaradi česar so bili ustvarjeni.

Potem, ko smo identificirali vsa sredstva in grožnje, sledi identifikacija ranljivosti obstoječih sredstev, torej pomanjkljivosti, ki jih lahko grožnje »izkoristijo« za uničenje ali za povzročitev škode. V tem koraku je treba izdelati seznam ranljivosti za vsako skupino ali za vsako specifično sredstvo, ki smo ga identificirali v prvem koraku. Npr. ranljivosti, ki lahko ogrozijo prostor za strežnike, vključujejo neustrezno lokacijo prostora (npr. izpostavljenost poplavam), neustrezno infrastrukturo in opremo (npr. odsotnost požarnih aparatov, slaba električna instalacija) ter pomanjkanje urejenega sistema pooblaščenega dostopanja do prostora. Ranljivosti dokumentnega sistema lahko zajemajo neustrezno dodeljevanje dostopnih pravic, odsotnost določenih tehničnih ali

³⁵ 83. člen PETZ – določa, kako in na kakšen način se pogodbeno uredi naročanje storitev pri zunanjem izvajalcu.

³⁶ 82. člen PETZ – določa, kako in na kakšen način ponudnik in naročnik pred podpisom pogodbe o opravljanju storitev izvedeta skupno oceno tveganj.

³⁷ ISO 18128:2024 – Information and documentation – Risk assessment for records processes and systems.

³⁸ ISO 18128:2024 – Risk assessment for records processes and systems, str. 6.

³⁹ DDoS (*Distributed denial of service*) so distribuirani napadi z zavrnitvijo storitev, pri čemer poskušajo napadalci s preobremenitvijo spletnih mest in strežnikov onemogočiti delovanje napadenih informacijskih sistemov.

vsebinskih skrbnikov, slabo upravljanje gesel in odsotnost politik varnostnega kopiranja. Popis ranljivosti se običajno začne na najvišji ravni celotne organizacije, pri čemer so pogosto največje ranljivosti povezane z odsotnostjo ali neustreznostjo varnostnih politik in odsotnostjo notranjih pravil.

Šele ob ustreznem popisu sredstev, njihovih ranljivosti in potencialnih groženj sledi končna ocena tveganj. V tem koraku se pripravi kalkulacija tveganj, ki pogosto vključuje uporabo t. i. vročičnih tabel. Pri vsaki grožnji in ranljivosti določenega sredstva si zastavimo dve ključni vprašanji:

1. Kakšna je verjetnost, da se določena grožnja uresniči (npr. velika, srednja, majhna)?
2. Kakšen vpliv bi imela realizacija grožnje na določeno sredstvo (npr. nepomemben, majhen, sprejemljiv, nesprejemljiv ali celo katastrofalen)?

S primerjavo verjetnosti realizacije grožnje in ocene njenega vpliva na določeno sredstvo ovrednotimo posamezna tveganja. Načelo je preprosto: višja, kot sta vpliv in verjetnost, večje je tveganje. Zbiru izvedenih omenjenih korakov in ovrednotenju posameznih tveganj tako rečemo ocena tveganj.⁴⁰

Ukrepi za zagotavljanje varne hrambe gradiva v digitalni obliki

Poleg izvedbe ocene tveganj, torej popisa sredstev, identifikacije ranljivosti, identifikacije groženj in na podlagi tega vrednotenja tveganj, so ključni obvladovanje tveganj ter določanje in izvajanje ukrepov za zmanjšanje verjetnosti ali vpliva tveganj. Ukrepi lahko vključujejo preprečevanje tveganj, zmanjševanje njihovih posledic, prenos tveganj na druge ali sprejemanje tveganj. Poleg tega sta nujni tudi redno spremljanje tveganj in učinkovitosti sprejetih ukrepov ter prilagajanje strategij obvladovanja tveganj, kadar je to potrebno. Če povzamemo, ključno za ustvarjalce javnega arhivskega gradiva je, da vzpostavijo ustrezne varnostne politike in sprejmejo ukrepe za varstvo gradiva, o čimer sicer govorita tudi že omenjena 57. in 58. člen PETZ.

Ukrepi za zagotavljanje varne hrambe digitalnega gradiva so raznovrstni, večslojni in kompleksni, kar je glede na količino in kompleksnost groženj tudi razumljivo.⁴¹ Segajo od sprejema krovnih informacijsko-varnostnih politik do načrtov za neprekinjeno poslovanje, ki med drugim vključujejo tudi varnostne politike pred naravnimi nesrečami in postopke za obnovo podatkov po naravnih nesrečah. Za organizacijo sta poleg sprejetja formalnih krovnih politik nujni tudi izvajanje rednih vaj in simulacij z namenom, da se osebje seznani z načrti in s postopki za ravnanje v primeru naravnih nesreč, ter izvajanje rednih revizij varnostnih postopkov oziroma preverjanje učinkovitosti varnostnih ukrepov.

Z vidika informacijske varnosti so ključni ukrepi uporaba in vzdrževanje zanesljivih informacijskih sistemov za zajem in hrambo ter vzpostavitev politik rednih varnostnih kopiranj. Prav tako so pomembni redno posodabljanje in uporaba protivirusne programske opreme za zaščito pred škodljivimi vdori in programi. Za varnost digitalnega gradiva je ključen ukrep geografske razpršenosti hrambe podatkov in varnostnih kopij na različnih lokacijah, ki so dovolj oddaljene druga od druge, da bi se izognili izgubi podatkov v primerih lokalnih naravnih nesreč. Vedno bolj priporočljiva je tudi implementacija tehnologije oblačne hrambe, saj ta zagotavlja visoko raven redundance in odpornosti proti naravnim nesrečam.

Za organizacijo sta prav tako nujna ustrezna fizična zaščita strojne opre-

⁴⁰ Več o tem glej npr. Hajtnik: Ocena in obvladovanje tveganj pri dolgoročni e-hrambi s pomočjo programskega orodja.

⁴¹ Glej npr. Metodologija obvladovanja tveganj informacijske varnosti v državni upravi, str. 8–16.

me in prostorov ter definiranje politik dostopov. Zagotoviti je treba, da so strežniki in druge pomembne naprave nameščene v prostorih, ki so odporni proti potresnim sunkom. Nujna je uporaba protipožarnih sistemov, kot so gasilni aparati s CO₂, ki v primeru implementacije ne poškodujejo strojne opreme. Postavitve strojne opreme na višje lokacije je priporočljiva za zaščito pred poplavami. Dostopanje do infrastrukture, sistemov in podatkov mora biti ustrezno regulirano in dokumentirano. Pri implementaciji ukrepov je priporočljivo sodelovanje z varnostnimi strokovnjaki za oceno tveganj, ki so specializirani za področje naravnih nesreč. Smiselno je tudi ukrep zavarovanja strojne opreme in podatkov proti naravnim nesrečam ter skladno s tem dokumentiranje izvedenih postopkov za varovanje podatkov in strojne opreme.

Tako kot je priporočljiva uporaba uveljavljenih standardov pri identifikaciji groženj, je smiselna tudi pri pripravi varnostnih politik. Uveljavljen splošni standard s področja obvladovanje tveganj predstavlja ISO 31000⁴² in konkretno s področja informacijske varnosti standard ISO 27001,⁴³ ki definira sisteme za upravljanje informacijske varnosti. Slednji standard predvideva za organizacije, ki vpeljujejo sistem informacijske varnosti, štiri (4) sklope kontrol (organizacijske, človeške, fizične, tehnološke) s 93 kontrolami. Kot eno izmed kontrolnih področij standard predvideva uvedbo kontrol z namenom varstva pred fizičnimi in okoljskimi tveganji, kot so to npr. naravne nesreče ali druge namerne ali nenamerne fizične grožnje.

Zaključek

Varstvo arhivskega gradiva v digitalni obliki pred naravnimi nesrečami je izjemnega pomena za zagotavljanje dostopnosti, uporabnosti, celovitosti, trajnosti in avtentičnosti podatkov, tako za ustvarjalce arhivskega gradiva kot za arhive kot takšne. Naravne nesreče, kot so poplave, požari, potresi in nevihte, lahko povzročijo hude poškodbe ali celo izgubo digitalnega gradiva, zato mora vsak ustvarjalec javnega arhivskega gradiva, in navsezadnje tudi arhivi, pripraviti in sprejeti celovit pristop k varstvu in zaščiti arhivskega gradiva v digitalni obliki.

Arhivska zakonodaja je predvidela enega izmed ključnih instrumentov za zagotavljanje učinkovite in dolgoročno varne hrambe gradiva v digitalni obliki. In sicer oceno tveganj kot ključni integralni del notranjih pravil za zajem in hrambo gradiva v digitalni obliki oziroma drugih informacijsko-varnostnih politik.

Ocena tveganj je na kratko proces, s katerim ocenjujemo nevarnosti in tveganja, ki bi lahko negativno vplivali na naše digitalno arhivsko gradivo. Proces je zato ključen za prepoznavanje, analizo in oceno tveganj ter za določanje ustreznih ukrepov za njihovo obvladovanje ali zmanjšanje. Ocena tveganja je, podobno kot notranja pravila, dinamičen proces, ki zahteva stalne revizije, spremljanje in prilagajanje zaradi spreminjajočih se okoliščin. Učinkovita ocena tveganja, ki naj bi bila cilj, je tako tista, ki omogoča organizacijam boljše obvladovanje tveganj in zmanjševanje njihovih negativnih vplivov.

Čeprav slovenska arhivska zakonodaja (ZVDAGA, UVDAG in PETZ) že predvideva ustrezne moderne pristope k varstvu digitalnega gradiva, tudi pred naravnimi nesrečami, vendarle lahko opazimo še precej pomanjkljivosti pri realizaciji tovrstnih določb. Posamezni organi, zlasti v javni upravi, se srečujejo s številnimi izzivi, tako v postopkih priprave notranjih pravil za zajem in hrambo gradiva v digitalni obliki kot pri pripravi ocen tveganj in izvajanju ukrepov.

⁴² ISO 31000: 2018 – Risk Management – Guidelines

⁴³ ISO 27001: 2022 – Information security, cybersecurity and privacy protection – Information security management systems.

Varstvo digitalnega gradiva zahteva vodstvo organizacij, ki je odloženo rešiti vprašanje notranjih pravil in upravljanj s tveganji ter ustrezno strokovno znanje pripravljavcev ocen tveganj in notranjih pravil. Proces je kompleksen in zahteva celovit pristop, saj vključuje tako tehnične kot organizacijske ukrepe celotne organizacije. Le s takšnim pravilnim načrtovanjem, z uporabo ustreznih politik in rednim preverjanjem bomo lahko zmanjšali različna tveganja (tudi okoljska) za uničenje ali izgubo digitalnega arhivskega gradiva.

VIRI IN LITERATURA

ZAKONODAJA

Pravilnik o enotnih tehnoloških zahtevah za zajem in hrambo gradiva v digitalni obliki. V: *Uradni list RS*, št. 118/2020.

Uredba o varstvu dokumentarnega in arhivskega gradiva. V: *Uradni list RS*, št. 42/2017.

Zakon o varstvu dokumentarnega in arhivskega gradiva ter o arhivih. V: *Uradni list RS*, št. 30/2006 in 51/2014.

STANDARDI

ISO 18128: 2024 – Information and documentation – Risk assessment for records processes and systems. Geneva, 2024.

ISO 27001: 2022 – Information security, cybersecurity and privacy protection – Information security management systems. Geneva, 2022.

ISO 31000: 2018 – Risk Management – Guidelines. Geneva, 2018.

SPLETNI VIRI

Beagrie, Charles: How Cloud Storage can address the needs of public archives in the UK: <https://cdn.nationalarchives.gov.uk/documents/archives/cloud-storage-guidance.pdf> (dostop: 16. 10. 2024).

Bešić, Vesna: Nakon stradanja građe u požaru 2014: Arhiv BiH uspijeva godišnje obraditi 4.000 dokumenata, potrebna im je pomoć: <https://www.aa.com.tr/ba/balkan/nakon-stradanja-gra%C4%91e-u-po%C5%BEaru-2014-arhiv-bih-uspijeva-godi%C5%A1nje-obraditi-4000-dokumenata-potrebna-im-je-pomo%C4%87/3247842#> (dostop: 25. 9. 2024).

Cek, Daniel: Zgoreli so katalogi in del arhiva: <https://primorske.svet24.si/2014/04/24/zgoreli-so-katalogi-in-del-arhiva> (dostop: 25. 9. 2024).

Fleary, Sinai: Caribbean historical archives destroyed in fire. <https://www.voice-online.co.uk/news/world-news/2024/06/21/caribbean-historical-archives-destroyed-in-fire/> (dostop: 25. 9. 2024).

Malak, Haisam Abdel: 10 Challenges of Digital Preservation: <https://theecmconsultant.com/challenges-of-digital-preservation/> (dostop: 16. 10. 2024).

Metodologija obvladovanja tveganj informacijske varnosti v državni upravi: <https://www.gov.si/assets/ministrstva/MDP/DI/Informacijska-varnost/Metodologija-obvladovanja-tveganj-informacijske-varnosti-v-drzavni-upravi.pdf> (dostop: 20. 12. 2019).

The National Archives, UK. Tehnični register PRONOM: <https://www.nationalarchives.gov.uk/pronom/> (dostop: 11. 10. 2024).

Turkeys quake trials blocked due to archive lost in hastily demolished municipality building: <https://www.duvarenglish.com/turkeys-quake-trials-blocked-due-to->

-archive-lost-in-hastily-demolished-municipality-building-news-64416 (dostop: 25. 9. 2024).

Seznam oblik zapisa, primernih za dolgoročno hrambo gradiva v digitalni obliki: <https://www.gov.si/assets/organi-v-sestavi/Arhiv-RS/Zakonodaja/Pravilnik-o-enotnih-tehnoloskih-zahtevah-za-zajem-in-hrambo-gradiva-v-digitalni-obliki/Seznam-oblik-zapisa-za-dolgorocno-hrambo-ver-1.0.pdf> (dostop: 21. 10. 2024).

LITERATURA

Antončič, Marjan: Vzorčna notranja pravila? O čem pravzaprav sploh govorimo. V: *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja. Popisovanje arhivskega gradiva [Elektronski vir]: zbornik mednarodne konference, Radenci, 13.–15. april 2016* (ur. Nina Gostenčnik). Maribor: Pokrajinski arhiv, 2016, str. 465–480.

Arhivi v primežu narave in tehnologije: knjiga povzetkov: Mednarodna konferenca Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: 15.–17. maj 2024, Radenci, Slovenija (ur. Nina Gostenčnik). Maribor: Pokrajinski arhiv, 2024.

Corrado, Edward M., Moulaison Sandy, Heather: *Digital preservation for libraries, archives and museums*. Lanham: Rowman & Littlefield, 2017.

Hajtnik, Tatjana: Ocena in obvladovanje tveganj pri dolgoročni e-hrambi s pomočjo programskega orodja. V: *Uporabnikom prijazni arhivi: knjiga povzetkov: Mednarodna konferenca Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: 11.–13. maj 2022, Radenci, Slovenija* (ur. Nina Gostenčnik). Maribor: Pokrajinski arhiv, 2022, str. 54.

Hajtnik, Tatjana: Pretvorba e-dokumentov v formate za dolgoročno hrambo na osnovi standarda ISO 13008. V: *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja. Digitalno in digitalizirano. Arhivsko gradivo včeraj, danes in jutri [Elektronski vir]: zbornik mednarodne konference, Radenci, 5.–7. april 2017* (ur. Nina Gostenčnik). Maribor: Pokrajinski arhiv, 2017, str. 27–47.

Hajtnik, Tatjana: Učinkovito dolgoročno ohranjanje arhivskega gradiva v Arhivu RS. V: *Knjižnica: revija za področje bibliotekarstva in informacijske znanosti* 56 (2012), št. 3, str. 55–70.

Hajtnik, Tatjana: Vse, kar mora vodstvo organizacije vedeti o e-hrambi. V: *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: 10. zbornik referatov dopolnilnega izobraževanja s področij arhivistike, dokumentalistike in informatike v Radencih od 6.–8. april 2011* (ur. Slavica Tovšak et al.). Maribor: Pokrajinski arhiv, 2011, str. 475–495.

Hribar, Luka: Pomembnost nosilcev podatkov digitalnega gradiva v arhivistiki. V: *Arhivi v službi človeka - človek v službi arhivov: relevance v raziskavah arhivske znanosti: 8. znanstvena konferenca z mednarodno udeležbo Za človeka gre: relevance znanosti in izobraževanja: zbornik recenziranih prispevkov: Maribor, 14. 3. 2020* (ur. Zdenka Semlič Rajh). Maribor: AMEU – ECM, Alma Mater Press, 2020, str. 139–152.

Kavčič-Čolić, Alenka: Teoretični model digitalnih arhivov. V: *Knjižnica: revija za področje bibliotekarstva in informacijske znanosti* 48 (2004), št. 4, str. 63–75.

Legget, Elizabeth R.: *Digitization and digital archiving: a practical guide for librarians*. Lanham: Rowman & Littlefield, 2014.

Natek, Karel: Temeljni termini v geografiji naravnih nesreč. V: *Dela – Oddelek za geografijo Filozofske fakultete v Ljubljani*, št. 35 (2011), str. 73–101.

SUMMARY

PROTECTION OF DIGITAL ARCHIVAL MATERIALS FROM NATURAL DISASTERS

The protection of archival material in digital form against natural disasters is of utmost importance for ensuring accessibility, usability, integrity, sustainability, and authenticity of data. For the archives themselves as well as for the creators of archival materials. Natural disasters such as floods, fires, earthquakes and storms can cause significant damage or even loss of digital records, so every creator of public archival materials, and not least the archives themselves, have to plan and implement a comprehensive approach to the preservation and protection of archival material in digital form.

One of the most essential instruments for guaranteeing the efficient and long-term safe storage of digital content is provided by archival legislation. Particularly, the risk assessment, which is a crucial component of internal rules for the capture and preservation of digital content or other information security policies.

In short, risk assessment is the process by which we assess the hazards and risks that could adversely impact our digital archival materials. The process is therefore crucial for identifying, analysing and assessing risks and for determining appropriate measures to manage or reduce them. However, risk assessment, like internal rules, is a dynamic process that requires constant revisions, monitoring and adjustment due to changing circumstances. Therefore, a risk assessment that enables organisations to more effectively handle risks and reduce their negative effects is considered effective. Although the Slovenian archival legislation already foresees appropriate modern approaches to the protection of digital material, including against natural disasters, we can still observe a number of shortcomings in implementation. Individual bodies, at least in the administration, encounter numerous challenges, both in the procedures for preparing internal rules for the capture and storage of material in digital form, and in the implementation of risk assessments.

Protecting digital content requires organisational leadership that is determined to address the issue of internal rules and risk management. The process is complex and all-encompassing, as it includes both technical and organizational measures. Only with such correct planning, deployment of appropriate technology and routine inspections will we be able to reduce the risks of destruction or loss of digital archival material.