

mag. Milan Selan  
Marko Jurečič

Generalni sekretariat Vlade  
RS

milan.selan@gov.si  
marko.jurecic@gov.si

Marko Hartman

Urad predsednika RS  
marko.hartman@up-rs.si

## Ocena tveganj klasičnih arhivov z uporabo metodologije ocene tveganj računalniško podprtih informacijskih sistemov

### Izvleček

Avtorji se čudijo veliki skrbi po varnosti elektronskih arhivov, zlasti zahtevi po nadzoru Arhiva RS celotnega življenjskega cikla elektronskega dokumenta, od njegovega nastanka do njegove shranitve v elektronsko stalno zbirko oziroma v elektronski arhiv. Avtorji se bolj za šalo (vendar vseeno z namenom vzbujanja slabe vesti arhivarjem oziroma arhivistom) potegnili vzporednico med upravljanjem tveganj v klasičnih arhivih in z Zakonom o varstvu dokumentarnega in arhivskega gradiva predpisanimi za elektronske arhive.

### Ključne besede

Dosegljivost, zaupanja vredno, celovitost informacij, informacijsko varnostna politika, klasični arhivi, elektronski arhivi, arhivska zakonodaja, analiza groženj, upravljanje tveganj

### Abstract

The authors wonder at the great attention paid to the security applied to the electronic archives, wonder especially at the expressed requirement to supervise the whole life cycle of the electronic documents of the National Archives, from their creation to when they are being saved in the Electronic Permanent Collection of Documents or in the Electronic Archives. More by way of a joke than seriously (nevertheless, however, to make the archivists' conscience bother them just a little), the authors have traced a parallel between the risk management in the classical type of Archives and the Law on Protection of Documentary and Archives' Records that rules the electronic archives.

### Keywords

Availability, Confidentiality, Integrity, Information Security Policy, Traditional archives, electronic archives, archives' legislation, threats analysis, risk management

## UVOD

K pisanju članka so nas spodbudile občasne jutranje debate ob kavi, ko smo v arhivu Generalnega sekretariata Vlade RS (GSV) premlevali posledice sprejetega Zakona o varstvu dokumentarnega in arhivskega gradiva in arhivih (ZVDAGA) z uredbo in Enotnimi tehničnimi zahtevami (ETZ) Arhiva Republike Slovenije (ARS), ki se bodo odrazile na naš načrtovani prehod na popolnoma elektronske arhive. Še posebej so nas v ETZ zmotila številna kontrolna vprašanja, ki se v celoti nanašajo le na informacijsko varnostno politiko. Mnenja smo bili, da je treba informacijsko varnost, oziroma, zagotavljanje delovanja procesov podprtih z informacijsko tehnologijo, gledati kot celoto, ne pa parcialno, kot nanjo gleda

sprejeta področna zakonodaja. Seveda nas je zmotilo tudi dejstvo, da arhivi nikdar niso ravno sloveli po visoki ravni informatizacije in velikem številu informatikov ter da ena, sicer vrhunska (informatijska in informacijsko-varnostna) strokovnjakinja, ne bo zmožna nadzirati izvajanje zahtev ETZ.

Moramo reči, da nas je prijetno presenetila načrtovana sprememba ZVDAGA (Zakon o spremembah in dopolnitvah ZVDAGA), ki z 10. členom dopolnjuje 19. člen ZVDAGA s četrtem odstavkom, ki se glasi:

» Ne glede na določbo prvega odstavka tega člena se skladnost notranjih pravil ne preverja v tistem delu, za katerega ima oseba s strani pristojnega organa ali neodvisne organizacije izdano potrdilo o skladnosti z veljavnimi predpisi ali mednarodnimi standardi kakovosti, informacijske varnosti in drugimi standardi, ki jih določi vlada.«

S sprejetjem tega dopolnila bo skladnost z mednarodnimi standardi za informacijsko varnost presojala informatijska, na pa arhivska stroka. Glede na to, da je del avtorske ekipe tega članka pomirjen s temi dopolnili, si vseeno nismo mogli zadržati, da z informacijskega vidika ne pokažemo na arhivske varnostne luknje. Seveda, ker je celovita ocena tveganj kompleksno dejanje in preobsežno za članek, smo izpostavili le tri kriterije, in sicer:

- celovitost (Integrity) in dostopnost/dosegljivost (Availability) dokumentarnega in arhivskega gradiva zaradi posledic katastrofe – bodisi naravne ali teroristične akcije posameznikov, in
- zaupanje (Confidentiality) v informacijo oziroma v vsebino dokumenta v njegovem celotnem življenjskem ciklu.

## CELOVITOST IN DOSTOPNOST DOKUMENTARNEGA GRADIVA

23. člen ZVDAGA pravi:

»Dokumentarno gradivo se hrani v ustreznih prostorih in opremi, v ustreznih klimatskih pogojih, zavarovano pred vlomom, požarom, vodo, biološkimi, kemičnimi, fizikalnimi in drugimi škodljivimi vplivi, ter zagotavlja dostopnost, kar pomeni varovanje pred izgubo in stalno zagotavljanje dostopa zgolj pooblaščenim uporabnikom ves čas trajanja hrambe, in celovitost, kar obsega nespremenljivost in neokrnjenost ter urejenost tega gradiva«.

Je z doslednim izvajanjem določb tega člena zakona v celoti poskrbljeno za varnost in koliko so v praksi skrbniki dokumentarnega in arhivskega gradiva (DAG) zares poskrbeli za varnost. Verjetno lahko pravi odgovor dà republiški inšpektor za kulturo in medije? Arhivi so pri državnih organih še vedno v kletih – v poplavnem območju, po možnosti v stenah arhivskih prostorov potekajo še odtočne (kanalizacijske) in vodovodne cevi, zanimiva pa bi bila še ocena potresne varnosti, glede na to, da je večina arhivov na »zanimivi« tevtonski prekladi.

Kako pa je zahtevana in zagotovljena trajnost samega gradiva. Ali ZVDAGA predpisuje, republiški inšpektor pa kontrolira, ali se DAG izpisuje na ustrezen, arhivski papir<sup>80</sup>, je tiskalnik, s katerim se izpisuje DAG ustrezno akreditiran in ali je črnilo (toner) primerno za

<sup>80</sup> Uporaba papirja s kakovostjo trajnega zapisa je omenjena v Uredbi o upravnem poslovanju (UUP; člen 189/6), mednarodni standard ISO 11108 (standard kakovosti arhivskega papirja) pa v Uredbi o varstvu dokumentarnega in arhivskega gradiva (UVDAG), kaj bolj zavezujoča navodila pa so morda v kakšnih tehničnih navodilih, na katere pa se predpisi, kot UUP ali ZVDAGA, ne sklicujejo.

dolgoročno hrambo DAG? Kolikor so nam poznana javna naročila, je kriterij naročanja najnižja cena, zahtev o kislosti, brezlesnosti in trajnosti papirja pa nismo zasledili.

Na posvetu arhivarjev in arhivistov letos v Radencih, je eden od avtorjev, malo za šalo, malo zares, predstavil »dobro« prakso nekaterih državnih in pokrajinskih arhivov ter arhivov v nekaterih drugih državnih organih, ki so zaradi nenadnega udara (v Koelnskem arhivu so letos izgubili 17 km gradiva z območja srednje Evrope od X. stol. dalje – kakšna je dejanska škoda ni kaj dosti zapisanega, novinarje je pač zanimalo le štetje pogrešanih in trupel)), poplave v občinskem arhivu (zaradi uničenega dokumenta prosilec ni mogel uveljaviti prizidka pri hiši) in v primorskem arhivu, številnih požarov (v Egipčanskem arhivu zaradi pomanjkanja vode požara niso mogli pogasiti), ali pa se je dokumentarno, oziroma arhivsko gradivo preprosto »izgubilo«, še preden je dobilo ta status (npr. »dogovor« Karadžiča s Holbrookom) – če nas spomin ne vara, tudi ZPIZ je imel ob koncu 60-tih let prejšnjega stoletja določene težave z ohranjanjem dokumentacije, še danes pa imajo nekateri težave pri upokojevanju – izgubili precejšnje zaupanje v celovitost in dostopnost DAG.

Varnost ni absolutna kategorija, zato je treba upoštevati Murphyjevo načelo »če gre lahko kaj narobe, bo zagotovo šlo« in vzpostaviti take mehanizme, ki bodo omogočili ohranitev vsaj vsebine DAG, če že ne izvirnega nosilca (papir). Kakršnokoli potres, poplava, požar (pa naj gre za malomarnost, načrtno teroristično dejanje (pri oceni ogroženosti bi bilo morda treba upoštevati tudi to, da se lahko, konec koncev, kakšnemu zaposlenemu »utrga« in arhiv zakuri, in vzpostaviti postopke za preprečitev te možnosti – npr.: kontrola vžigalic, vnetljivih tekočin, vstop v arhivske prostore le v paru ...) ali za delovanje narave – npr. udar strele), trpi tako načelo popolnosti, kot dostopnosti.

## **ZAUPANJE V VSEBINO DAG**

ETZ se tako rekoč nanašajo na celoten življenjski cikel dokumenta, saj se zahteva akreditacija sistemov za upravljanje elektorskih dokumentov, informacijske komunikacijske infrastrukture, sistemov za digitalizacijo dokumentov ipd. Če se del akreditacijskih postopkov nanaša na varnost in zanesljivost hrambe elektronskih dokumentov, se del nanaša tudi na avtentičnost elektronskih dokumentov. O možnostih ravnanja z elektronskimi dokumenti, o pravni veljavnosti elektronsko podpisanih dokumentov in o tem, da so vsi e-dokumenti tako rekoč izvirniki, govori že davno sprejeti Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP). Elektronsko podpisan elektronski dokument z možnostjo preverjanja podpisa zagotavlja, da v fazi od podpisa do naslovnika dokument ni bil potvorjen.

V državni upravi v tem trenutno poteka proces prenove elektronskega podpisa, saj se je prvotno e-podpisovanje z Entrustom izkazalo za precej nerodnega za širšo uporabo, predvsem pa se je pokazalo kot nesprejemljivo za osebno e-vročanje državljanom. Prenovljeni e-podpis z uporabo spletnega certifikata, podpisovanjem dokumentov v za dolgoročno arhivsko hrambo primerni različici oblike PDF zapisa ter možnostjo preverjanja e-podpisa z brezplačnim Acrobat Readerjem, bo zagotovo dokončno odprl pot široki uporabi elektronsko podpisanih dokumentov.

Če (praktično) dokumenta, potem, ko je bil elektronsko podpisan – se pravi, od trenutka dalje, ko besedilo postane dokument – ni moč potvoriti, pa poglejmo, kako varna je vsebina dokumenta v papirnati obliki v njegovem celotnem življenjskem ciklu. Naj navedemo le dva možna primera:

#### a.) Izguba zaupanja ob podpisovanju dokumentov

Če se dokument izpisuje v dveh ali več izvodih, podpisnik prebere verjetno le prvi izvod, druge izvode zgolj avtomatično podpiše. V času tipkanja s pisalnim strojem je bila kopija skoraj zagotovo enaka prvemu izvodu – kdo bi se mučil s pretipkavanjem (tudi vizualno bi bilo vložnega precej napora zadeti novo kopijo) – pri izpisu elektronskega dokumenta pa lahko pride do napake zaradi malomarnosti (enkrat npr. pomotoma izpišemo staro verzijo) ali namerne potvorbe vsebine (npr.: kakšnemu znesku 1 spremenimo v 7). Verjetno je izvod poslan naslovniku pravi (sicer bi ugovarjal), »arhivski« izvod pa napačen. Javni uslužbenec dokument vložijo v zadevo, zadeve se »znebijo« v glavni pisarni, glavna pisarna pa nima izvoda za primerjavo, saj je bil pravi dokument odposlan že davno prej. Če pa upoštevamo še vidik dostopnosti in neokrnjenosti – en izvod dokumenta morda nikoli ne vidi glavne pisarne, saj je ostal ali se izgubil v predalu javnega uslužbenca.

Da prvi izvod ni bil enak drugemu, imamo primer še iz letošnjega leta, ko so v arhivirani sodni odločbi nekega primorskega sodišča manjkali ključni deli dokumenta.

#### b.) Izguba zaupanja v dokumente v stalni zbirki ali arhivu

23. člen ZVDAGA zahteva »zagotavljanje dostopa zgolj pooblaščenim uporabnikom ves čas trajanja hrambe«, pri ocenjevanju tveganja, da lahko gre kaj narobe, nas zanima, kdo in na kakšen način se kontrolira pooblaščen osebe – je urejen nadzor, da iz arhiva ne odnašajo posamezne zanimive dokumente, je urejen nadzor, da pooblaščen osebe ne vnašajo »zanimiv« dokumentov v arhiv, je celo vzpostavljen mehanizem, ki preprečuje možnost postavitve fotokopirnega stroja v arhivske prostore in ustvarjati »nove« dokumente?

### **VARNOSTNO KOPIRANJE DOKUMENTARNEGA IN ARHIVSKEGA GRADIVA**

Če se za elektronski arhiv zahteva 200 ali celo 300% varnost, oziroma, na kolikor lokacijah že pač morajo biti shranjeni elektronski dokumenti, govorimo pri klasičnem arhivu vedno le o izvorniku. Zavest o možni izgubi te edine verzije dokumenta nas logično pripelje do razmišljanja, da je treba tudi v klasičnem arhivu zagotoviti »backup« vsakega dokumenta in kopijo hraniti na drugi lokaciji. Naj gre pri tem za odločitev o mikrofilmanju ali o digitalizaciji izvornega DAG ni pomembno, zadnje pri tem naj igra sklicevanje na ekonomsko »računico« in/ali na krčenje proračuna.

S pravočasnim izdelovanjem kopij DAG lahko zadostimo vsem trem kriterijem, ki jih predpisuje že 23. člen ZVDAGA – dostopnost, celovitost, nespremenljivost in neokrnjenost DAG – seveda pa moramo zadostiti še kriteriju, da se kopija(e) nahajajo na oddaljeni lokaciji.

### **PRIMER DOBRE PRAKSE**

V Generalnem sekretariatu Vlade RS, nekdanjem Izvršnem svetu SRS je bil že ob koncu 70-tih let prejšnjega stoletja vzpostavljen informacijski sistem za podporo delu Izvršnega sveta RSR (ISPD IS SRS). Urejen je bil celoten življenjski cikel dokumenta, od oblikovanja (originating) novega dokumenta – že leta 1979 so se začeli dokumenti zajemati računalnikom (Display Writer (pra-osebni računalnik) in Display Write (prvi urejevalnik besedila)), do razmnoževanja, diseminacije, dokumentalistične obdelave, informacijske podpore meta

podatkom do končne hrambe trajnega gradiva v priročnem arhivu Generalnega sekretariata., oziroma predaje arhivskega gradiva Arhivu Republike Slovenije. Seveda so bila v procesu obdelave dokumentov upoštevane zahteve tedaj veljavnega pravilnika o ravnanju z dokumentarnim gradivom (se pravi: razvrščanje po vsebini v zadeve, dodeljevanje zadev v reševanje, reševanje in zaključevanje zadev, izdelava popisov, itd.).

Bistvena komponenta IS pa je bila ureditev mikrofilmanja celotnega dokumentarnega in arhivskega gradiva, z namenom:

- zagotoviti hitrejša in enostavnejša iskanja ter ponovno uporabo že rešenih in v stalno zbirko prenesenih zadev (mikrofilmane zadeve se hranijo v žepkih);
- zagotoviti, da v Generalnem sekretariatu ostanejo dostopni (mikrofilmani) dokumenti, ki so bili sicer predani v Arhiv RS v izvorniku;
- zagotoviti javno vero tudi mikrofilmanim dokumentom;
- zagotoviti varnost dokumentarnega in arhivskega gradiva (varnostne kopije na mikrofilmskih trakovih se hranijo na oddaljeni lokaciji).

Prav varnostna komponenta je bila izpostavljena že na začetku projekta, tako je na mikrofilm presneto celotno gradivo od leta 1965 do konca mandata leta 2000, skupno več kot 6 milijonov strani.

Kritične faze zagotavljanja dosegljivosti, celovitosti in javne vere, če z vidika zahtev ETZ potegnemo vzporednico med klasičnim in elektronskim arhivom, so bile vse faze do mikrofilmanja – zadeve v reševanju v (lesenih) omarah pri javnem uslužbencu, zadeve v (kovinskih) omarah v tekoči zbirki in popisovanje zadev v Glavni pisarni, priprava zadev za mikrofilmanje v arhivu – rabili bi samo en »dober« požar, pa bi v nič lahko šlo nekaj deset metrov dokumentarnega in arhivskega gradiva..

Od konca leta 2000 dalje je že večino dokumentov v elektronski obliki in smo, skladno s projektom o vzpostavitvi elektronskega arhiva v GSV, začeli vzpostavljati popolnoma elektronsko zbirko dokumentarnega in arhivskega gradiva Vlade RS in GSV.

## ZAKLJUČEK

(Informacijska) varnost arhivov se ni začela šele z oblikovanjem elektronskih arhivov, ampak velja tudi za klasične arhive saj požar, potres, vplivi okolja, teroristični napadi, kraje in potvarjanje dokumentov ne vplivajo zgolj na z informacijsko tehnologijo podprte poslovne procese. Z izdelavo varnostnih kopij, bodisi na mikrofilmu ali v digitalizirani obliki, zagotovimo po eni strani za varnost vsebin, za katero skrbijo pooblaščen organi, po drugi strani pa enostavnejšo in učinkovitejšo uporabo DAG.

Pustimo, da nosilce izvornih vsebin raziskujejo strokovnjaki za materiale, obstojnost in barve ter restavradorji, razni raziskovalci zgodovine pa naj se za obdelavo podatkov in informacij zadovoljijo s kopijami.

## VIRI IN LITERATURA

- Frank Lezaja: Študija upravičenosti digitalizacije papirnatih dokumentov na MNZ (interno gradivo MNZ, 1992),

- Mag. Milan Selan, Marko Hartman, Marko Jurečič: Od klasičnega arhiva k elektronskemu – primer iz prakse (DOK\_SIS 2008, Kranjska gora),
- Mag. Milan Selan in sodelavci: Projekt vzpostavitve elektronskega arhiva (interno gradivo GSV, 2006–2007),
- Mag. Milan Selan in sodelavci: Pravilnik o ravnanju in hrambi dokumentarnega in arhivskega gradiva GSV (Notranja pravila; interno gradivo GSV, 2007–2008, gradivo je še v dopolnjevanju),
- Uredba o upravnem poslovanju
- Uredba o varstvu dokumentarnega in arhivskega gradiva
- Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih
- Zakon o elektronskem podpisu in elektronskem poslovanju
- Zakon o tajnih podatki
- Zakon o varstvu dokumentarnega in arhivskega gradiva in arhivih,
- Zakon o dopolnitvah in spremembah Zakona varstvu dokumentarnega in arhivskega gradiva in arhivih (delovno gradivo).

### Avtorji

**mag. Milan Selan** je v Generalnem sekretariatu zaposlen kot vodja Sektorja za informatiko. Odgovoren je za razvoj ključnih projektov, npr. eArhiva in IS za podporo odločanju o zakonodajnih in drugih aktih Sveta Evropske unije (EU-portal), pripravlja pa tudi Notranja pravila in Informacijsko varnostno politiko GSV. Z informatiko se ukvarja od leta 1972. Magistriral je s področja informacijske podpore evropskim zakonodajnim postopkom.

#### **Marko Hartman**

dipl. univ. pol. je zaposlen v Uradu predsednika republike Slovenije kot pomočnik generalnega sekretarja za informatiko. Z informatiko se intenzivno ukvarja od leta 1986 in v tem času je sodeloval pri postavitvi in predvsem implementaciji številnih informacijskih sistemov v delo državne in javne uprave.

#### **Marko Jurečič**

Je zaposlen v Generalnem sekretariatu kot arhivar – vodja arhiva. Z arhiviranjem se ukvarja od leta 1976, s klasičnim mikrofilmom pa od leta 1979.

# media.doc