Edvin Buršić
Financijska agencija
Zagreb

Hrvoje Stančić
Filozofski fakultet u Zagrebu
Zagreb

SIGURNOST POHRANE ARHIVSKIH ZAPISA U RAČUNALNOME OBLAKU

UDK: 004.08:930.251

Pregledni znanstveni rad

Arhivski zapisi u elektroničkome obliku sve se više pohranjuju u neki oblik računalnoga oblaka (engl. cloud storage*). S obzirom na to da je tada najčešće riječ o ugovaranju usluge s trećom stranom – pružateljem usluge pohrane u oblaku (engl.* cloud service provider*) – potrebno je razumjeti slojevitost pitanja sigurnosti u tome kontekstu. Ona su važna za sve arhiviste koji će biti nadležni za pohranu i dugoročno čuvanje takvih zapisa jer će morati procijeniti kvalitetu usluge koju pojedini pružatelji nude kako bi mogli donijeti ispravnu preporuku kojega odabrati. Potom će morati procijeniti potencijalne sigurnosne rizike i formulirati zahtjeve kako ih smanjiti ili otkloniti te konačno postaviti zahtjeve i provesti postupke dugoročnoga očuvanja kada se za njimapojavi potreba i slično. Sve navedeno utječe na sigurnost pohranjenih zapisa, njihovu autentičnost, pouzdanost, iskoristivost te njihov integritet. Stoga autori u ovome radu analizirajuzahtjeve za sigurnošću pohrane arhivskih zapisa u računalnome oblaku, predlažu konkretne mjere za smanjenje potencijalnih rizika koji se pritom pojavljuju te zaključujuo tome kako sve to utječe na arhivsku praksu i obrazovanje arhivista.*

Ključne riječi: *arhivski zapisi, računalni oblak, pohrana, sigurnost, rizik*

Uvod

U skladu s, danas već zastarjelom, kustodijalnom paradigmom arhivi su mjesta gdje se čuva arhivsko gradivo. Suvremena, postkustodijalna paradigma uzima u obzir da suvremeno arhivsko gradivo nastaje u elektroničkome obliku i da je potrebno pomoći samim stvarateljima da ga ispravno čuvaju u svojim informatičkim sustavima. Uloga je arhiva, prema ovome konceptu, savjetodavna. No, od nedavno se pojavljuje i treća strana koja postaje itekako relevantna, a to su pružatelji usluga pohrane u oblaku (engl. *cloud service provider*, *cloud storage*). Naime, stvarateljima gradiva postaje financijski isplativije pohranjivati gradivo u nekome podatkovnom centru i u nekome obliku rješenja u oblaku, nego održavati vlastitu računalno-programsku infrastrukturu, brinuti se o njezinu ispravnome radu i održavanju, obrazovanju IT stručnjaka i slično. Mogućnosti ovdje ne staju jer pružatelji usluga u oblaku ne nude samo neki oblik prostora za pohranu, nego i programska rješenja u oblaku. Tako stvaratelji gradiva više ne moraju plaćati brojne programske licencije,nego mogu ista ta programska rješenja plaćati prema korištenju. U kontekstu dugoročne pohrane i postkustodijalne paradigme, možda bismo ju mogli nazvati i „postkustodijalnom paradigmom 2.0“, arhivi sada moraju ne samo savjetovati stvaratelje gradiva kako čuvati elektroničko arhivsko gradivo u vlastitim sustavima, nego ih moraju savjetovati i kako procijeniti koji pružatelj usluga nudi usluge koje su prilagođene arhivističkim principima, a s druge strane ostvariti korektnu komunikaciju i sa samim pružateljima usluga kako bi oni oblikovali i ponudili upravo takve usluge.[1] Iz toga je sada posve jasno zašto je ranije spomenut ulazak treće strane.

Pohrana u oblaku

O modelima pohrane u oblaku, IaaS, PaaS, SaaS,[2] te vrstama oblaka, javni, privatni, društveni, hibridni,[3] već se u stručnoj literaturi govorilo. No, manje je poznato, a najnovija istraživanja na projektu InterPARES Trust upravo to i pokazuju,

[1] Više u: Stančić, H., Rajh, A., Milošević, I. *"Archiving-as-a-Service". Influence of Cloud Computing on the Archival Theory and Practice*. U: *The Memory of the World in the Digital Age: Digitization and Preservation*. Duranti, L., Shaffer, E. (ur.). UNESCO, 2013. Str. 108–125. URL: http://bib.irb.hr/datoteka/618924.Stancic_Rajh_Milosevic_-_Influence_of_Cloud_Computing_on_the_Archival_Theory_and_Practice.pdf (10. 6. 2015.).

[2] IaaS – *Infrastructure-as-a-Service*, PaaS – *Platform-as-a-Service*, SaaS – *Software-as-a-Service*.

[3] Engl. *Public, Private, Community* i *Hybrid Cloud*

da je razlog prelaska s vlastite računalno-programske infrastrukture na rješenja u oblaku isti kao i razlog odustajanja od rješenja u oblaku i povratka na vlastitu infrastrukturu – financijski. Koliko god je ovo neočekivan rezultat, istraživanja doista pokazuju da je tako. Dok s jedne strane prelazak u oblak osigurava manje troškove iz već spomenutih razloga, on ujedno osigurava skalabilnost, pouzdanost i sigurnost podataka uz jednostavniju mogućnost suradničkoga rada na istome dokumentu. Ipak, s druge strane, stvaratelji se moraju odlučiti za neki model rješenja u oblaku. Za koji se god model odlučili, vrlo je teško unaprijed procijeniti hoće li on biti dovoljan. Premda je uslugu lako moguće proširiti, često se događa da djelatnici iskoriste više nego što je nekim paketom zakupljeno, a ti troškovi tada nisu mali. Uz rizik povećanoga i nepredvidljivoga troška, Duranti navodi i druge rizike, počevši od pouzdanosti, sigurnosti, kontrole, transparentnosti pa sve do rizika povezanoga s privatnošću.[4] Sve navedeno dovodi do toga da su se financijski razlozi nametnuli i kao glavni razlog prestanka korištenja rješenja u oblaku.

Upravo zbog takve situacije iznimno je važno da svi arhivisti razumiju prednosti i nedostatke korištenja rješenja u oblaku da bi mogli s jedne strane savjetovati stvaratelje gradiva, a s druge pružatelje usluga u oblaku kako da organiziraju sigurnu dugoročnu pohranu u oblaku usklađenu s potrebnim arhivskim standardima. Stoga se u nastavku objašnjavaju sve one situacije na koje je potrebno skrenuti pozornost stvarateljima i savjetovati ih kako da u njima postupe. Konkretno, razrađuju se rizici korištenja rješenja u oblaku, ne zbog toga da bi se nekoga odvratilo od takvih rješenja, nego,naprotiv, s namjerom da se uputi na složenost teproblematike gledajući iz arhivske perspektive te osigura da stvaratelji, ali i arhivisti razumiju rizike te spriječe ili smanje mogućnost njihova ostvarivanja.

Rizici pohrane u oblaku

Veći financijski troškovi od planiranih

S obzirom na to da su već spomenuti, najbolje je odmah započeti s financijskim troškovima. Istraživanje korisnika provedeno u okviru projekta *Zapisi u*

[4] Duranti, L. *Preservation in the Cloud: Towards an International Framework for a Balance of Trust and Trust worthiness.* U: APA/C-DAC International Conference on Digital Preservation and Development of Trusted Digital Repositories, New Delhi, India, 5.–6. February 2014. URL: https://www.academia.edu/11328013/Preservation_in_the_Cloud_Towards_an_International_Framework_for_a_Balance_of_Trust_and_Trustworthiness (8. 9. 2015.).

oblaku[5] pokazalo je da prijenos svih podataka u oblak, kao i uspostava svih potrebnih kontrolnih mehanizama, poslovnih procesa i kriptiranja podataka može uključivati dodatne, ranije nepredviđene troškove. Neki pružatelji usluga u oblaku ograničavaju količinu pristupa na otprilike 5% svih pospremljenih zapisa mjesečno, a troškovi korištenja više od 5% znaju biti vrlo visoki. Ustanovama koje stvaraju arhivsko gradivo ponekad je teško predvidjeti koliko će gradiva nastajati na mjesečnoj osnovi pa je i u tome slučaju rizik od prelaska neke, unaprijed dogovorene mjesečne količine, prisutan.

Kršenje regulatornih propisa

Nacionalni arhivi Australije (NAA)[6] kao prvi od više spomenutih rizika navode upravo rizik od kršenja regulatornih propisa. Naime, bilo koja ustanova koja prelazi na rješenja u oblaku mora biti sigurna da pravna regulativa, koja može biti specifična za pojedinu ustanovu ili tijelo državne ili javne uprave, mora biti dosljedno provedena i prilikom korištenja rješenja u oblaku. Moguće je da određeni dokumenti i zapisi moraju biti pohranjeni isključivo u nekome formatu, a moguća je i potreba propisivanja u kojim situacijama takvi zapisi obavezno nastaju i tko ih smije vidjeti. Sve su to neka ograničenja koja bi trebala biti striktno provedena, jer prelaskom na rješenja u oblaku stvaratelj i dalje ima obvezu osigurati da su arhivski zapisi odgovorno stvarani, da se njima tako upravljalo i činilo ih se dostupnima te izlučivalo. Da bi se smanjio rizik od kršenja regulatornih propisa, NAA sugeriraju stvarateljima da najprije odrede koji će zapisi biti prebačeni u oblak i koja je pravna regulativa za njih relevantna. Nadalje, potrebno je osigurati primjereno upravljanje podatcima u oblaku, kako onima koje je stvorio sam stvaratelj tako i onima koje, povezano s tim gradivom, stvara pružatelj usluge. Konačno, potrebno je osigurati da pružatelj usluge razumije svoju odgovornost u odnosu na zapise stvaratelja.

Nepoznata fizička lokacija pohrane i neautorizirano korištenje

Iako pružatelj usluge pohrane u oblaku može pravno djelovati na teritoriju pojedine države te tamo imati fizički prisutan podatkovni centar, postavlja se pitanje

[5] Pan, W.; Rowe, J.; Barlaoura, G. User Survey Report / Records in the Cloud project, 23. listopada 2013. URL: http://www.recordsinthecloud.org/assets/documents/RiC_Oct232013_User_Survey_Report.pdf (20. 7. 2015.).

[6] Outsourcing digital data storage / National Archives of Australia. 2015. URL: http://www.naa.gov.au/records-management/agency/secure-and-store/outsourcing-digital-data/index.aspx (22. 7. 2015.).

gdje se nalaze pričuvne kopije, odnosno jesu li zapisi raspršeno pohranjeni na više fizičkih lokacija od kojih ne moraju sve biti na teritoriju iste države. Za određene vrste arhivskoga gradiva izuzetno je važno da ono cijelo vrijeme ostaje u pravnoj nadležnosti neke države. Za druge vrste arhivskoga gradiva to je od strateške važnosti, dok za treće to možda uopće nije važno. Svjetski poznata rješenja u oblaku poput Google Drivea, DropBoxa, Microsoft Clouda, iClouda i slično posve sigurno ne pohranjuju podatke isključivo na teritoriju Republike Hrvatske. Pravo rješenje za tijela državne i javne uprave bila bi izgradnja državnoga oblaka, kao što se to, primjerice, predviđa Strategijom razvoja javne uprave za razdoblje od 2015. do 2020.[7] No, stvaratelji bi, napose oni koji neće moći pohranjivati svoje arhivsko gradivo u državni oblak, trebali voditi računa o tome gdje je ono fizički smješteno, koristi li se pružatelj usluge podugovarateljima i, ako se njima koristi, gdje oni pohranjuju gradivo. U slučaju pohrane arhivskoga gradiva kod pružatelja usluga koji ne pohranjuju gradivo, primjerice, na teritoriju RH-a ili EU-a, potrebno je voditi računa čiji je pravni okvir mjerodavan kako ne bi došlo do nepredviđenih pravnih aktivnosti. Na primjer, američka Nacionalna sigurnosna agencija (NSA) smije bez posebnoga pitanja ostvariti uvid u gradivo koje prolazi preko servera američkih pružatelja usluga. Stoga je potrebno voditi računa o tome gdje se elektroničko arhivsko gradivo fizički pohranjuje kada se koristi nekom od usluga u oblaku kako ne bi došlo do neautoriziranoga korištenja. U tu je svrhu važno ugovorom propisati da pružatelj usluga mora bilježiti i čuvati informacije (engl. *log files*) o tome tko je i kada pristupao gradivu i što je s njime činio. Bilježenje tih, nazovimo ih, servisnih podataka, važno je u kontekstu autentikacije, tj. provjere pristupnih prava korisnika i njihova propuštanja u sustav i dalje do gradiva, i autentifikacije, tj. potvrđivanja autentičnosti nekoga gradiva.

Smanjena evidencijska vrijednost gradiva

Elektroničko gradivo koje se dugoročno čuva treba ostati vjerodostojno. Vjerodostojno je gradivo ono gradivo koje je tijekom očuvanja zadržalo svojstva autentičnosti, pouzdanosti, integriteta i upotrebljivosti. Posve je realno očekivati da će pružatelj usluge pohrane u oblaku unapređivatiračunalno-programsku okolinu u koju se gradivo pohranjuje ili ujedno u njemu i nastaje. Pritom neki formati zapisa više

[7] Strategija razvoja javne uprave za razdoblje od 2015. do 2020., usvojena na 17. sjednici Sabora 12. lipnja 2015. URL: https://vlada.gov.hr/UserDocsImages/Sjednice/2015/229%20sjednica%20Vlade/229%20-%202.pdf (30. 8. 2015.).

neće biti čitljivi pa će ih se konvertirati u noviji format, mediji će zastarijevati i biti mijenjani suvremenijima, a gradivo migrirati sa starijih medija na nove. Sve ove promjene moraju biti pomno testirane i zabilježene kako bi gradivo i dalje ostalo vjerodostojno. Također, treba voditi brigu i o tome tko će, kada i u kojim slučajevima inicirati, primjerice, konverziju gradiva u novi format i što će se učiniti s gradivom u zastarjelome formatu. Naime, ako je proces konverzije automatski, a gradivo se u starome formatu nastavlja čuvati, onda se može dogoditi da stvaratelj odjednom ima duplo više gradiva i mora platiti duplo više prostora za njegovu pohranu u oblaku. Stoga bi svaki postupak unapređenja računalno-programske okoline trebao biti najavljen ili zatražen te pomno testiran kako bi se smanjio rizik da gradivo izgubi vjerodostojnost, odnosno da njegova evidencijska vrijednost bude smanjena.

Neadekvatno upravljanje metapodatcima i sigurnosno brisanje

U kontekstu konverzije zapisa u noviji format i migracije gradiva na nove medije važno je regulirati tko je vlasnik metapodataka o provedenome postupku – vlasnik gradiva ili pružatelj usluga. Naime, konverzija ili migracija ponekad može biti i automatska. Primjerice, ako dođe do kvara jednoga od diskova povezanih u polje diskova, on može bez gubitaka podataka biti zamijenjen novim, čak i tijekom rada sustava za pohranu. Podatci su pritom replicirani na druge diskove pa nema gubitaka, no informacija o zamjeni diska svakako bi trebala biti zabilježena. Ako je sustav pritom pohranjivao arhivsko gradivo s tajnim zapisima, pokvareni disk mora biti propisno uništen. Taj je postupak povezan i s redovitom zamjenom starijih diskova ili drugih medija za pohranu novima te s izlučivanjem gradiva. U obamaje slučajevima potrebno dogovoriti s pružateljem usluga pohrane u oblaku točnu proceduru sigurnosnoga brisanja podataka za svaku kategoriju tajnosti zapisa ili proceduru fizičkoga uništenja medija.[8] Pritom treba imati na umu kako je potrebno obaviti sigurnosno brisanje i na zamjenskoj, udaljenoj lokaciji kojom se pružatelj usluge koristi za spremanje pričuvnih kopija.Procedure sigurnosnoga brisanja važne su i u slučajevima prelaska s usluga jednoga pružatelja usluga na one drugoga.Metapodatke o svim obavljenim postupcima (brisanju, brisanju zamjenskih podataka, uništavanju

[8] Više o sigurnosnome brisanju podataka u: Golubić, K., Stančić, H. *Clearing and Sanitization of Media Used for Digital Storage: Towards Recommendations for Secure Deleting of Digital Files*. U: *Central European Conference on Information and Intelligent Systems 23rd International Conference*. Hunjak, T., Lovrenčić, S., Tomičić, I. (ur.). Varaždin : Faculty of organization and informatics, 2012. URL: http://www.ceciis.foi.hr/app/public/conferences/1/papers2012/iss6.pdf (20. 7. 2015.).

medija te prelasku na usluge drugoga pružatelja) potrebno je čuvati i nakon provođenja spomenutih postupaka i biti siguran da su oni u vlasništvu stvaratelja.

Prestanak rada pružatelja usluge u oblaku

Pružatelji usluga u oblaku mogu prestati s radom. Hoće li stvaratelji biti u mogućnosti prenijeti svoje gradivo u drugu okolinu? Hoće li moći gradivo izvesti u nekome otvorenom formatu i kako će to utjecati na njegovu vjerodostojnost? Hoće li imati nadzor nad time gdje će završiti mediji na kojima su njihovi podatci bili zapisani? Hoće li im se pružiti mogućnost otkupa računalno-programske okoline u kojoj je njihovo gradivo bilo pohranjeno? Sve su ovo pitanja koja bi trebala biti primjereno dotaknuta u ugovoru o pružanju usluge (engl. *Service-Level Agreement*, *SLA*). Stvaratelji gradiva također bi se trebali zapitati koliko će trajati prijenos gradiva u novu okolinu ili kod nekoga drugog pružatelja usluga jer se brzine pohrane u oblak i preuzimanje s njega ponekad mogu bitno razlikovati, pogotovo ako pružatelj usluga prestaje s radom i svi korisnici odjednom žele čim prije preuzeti svoje gradivo. Odabir pružatelja usluga koji ove situacije ima jasno i precizno definirane u svojim internim pravilnicima, institucijskim politikama i ugovoru o pružanju usluge, time će sasvim sigurno odavati sliku stabilnoga i pouzdanoga partnera.

Prema arhivskoj pohrani u oblaku

Analizirani rizici koji se pojavljuju prilikom pohrane arhivskoga gradiva u oblaku sagledani su iz perspektive stvaratelja arhivskoga gradiva i arhiva čija je zadaća savjetovati stvaratelje, ali i pružatelje usluga pohrane u oblaku kako ispravno i prema svim važećim arhivskim normama dugoročno očuvati arhivsko gradivo u digitalnome obliku. Ta analiza trebala bi s jedne strane pomoći stvarateljima prilikom procjene kvalitete ponuđene usluge u oblaku, a s druge pomoći pružateljima usluge da ju oblikuju i čim više usklade s potrebnim normama i zakonodavnim okvirom. U tome smislu pružatelji usluga trebali bi težiti tomu da postanu pružatelji usluga od povjerenja, tj. da umjesto usluge pohrane u oblaku ponude uslugu arhivske pohrane u oblaku. No, ovdje je ta problematika tek započeta i postoji čitav niz dodatnih parametara koje je potrebno uspostaviti da bi se postigao status arhivske pohrane u oblaku, a ulazak u njihovu dublju analizu premašio bi okvire ovoga rada.

Hibridni model

Iz dosadašnje rasprave proizlazi, slično kao i kod svakoga složenijeg sustava, da oba promatrana rješenja – pohrana digitalnoga gradiva u informatičku infrastrukturu u vlasništvu institucije i pohrana u oblaku – imaju svoje prednosti i nedostatke. Stoga se nameće logičko pitanje – nije li hibridni model najbolje rješenje? U nekim slučajevima moglo bi doista tako i biti pod uvjetom da se odaberu one povoljnije strane iz obaju rješenja. Tako bi se, primjerice, u oblak moglo preseliti sustav za upravljanje dokumentima i uredske programe, a pohranu digitalnih zapisa smjestiti u vlastitu, nadziranu informatičku infrastrukturu. Pritom se sigurnosna kopija može kriptirati i dislocirati pohranom u oblak. Naravno, ne znači da bi takav pristup bio optimalan za sve stvaratelje. Izbor najboljega rješenja ne ovisi samo o tome koliko arhivskoga gradiva nastaje kod nekoga stvaratelja i kakvo je to gradivo u smislu ograničenja dostupnosti, nego i o mnogim drugim faktorima kao što su to, primjerice, broj zaposlenika, razina dostupnoga financiranja, starost postojeće računalno-programske okoline, utemeljenje poslovanja na arhivskim zapisima kao izvorima informacija za praćenje trendova i donošenje budućih poslovnih odluka, važnosti osiguranja kontinuiteta poslovanja i stalne dostupnosti zapisa itd.

Zaključak

Stvarateljima arhivskoga gradiva danas se pružaju različite mogućnosti korištenja tehnoloških rješenja pohrane u oblaku – od usluga softvera u oblaku, što se plaća prema korištenju, a ne prema broju licencija, tj. prema broju radnih mjesta, preko usluga zakupa računalne platforme u oblaku, pri čemu se ne mora brinuti o održavanju računalne opreme, pa sve do zakupa infrastrukture u oblaku koja kao model usluge pruža najviši stupanj slobode, ali ujedno zahtijeva vrlo stručna znanja. Zakup pojedine usluge u oblaku relativno je jednostavan i privlači korisnike brojnim pogodnostima – od nižih financijskih troškova, okupljanja svih sadržaja na jednome mjestu, njihove stalne dostupnosti pa sve do umrežene kolaboracijske radne okoline koja omogućava zajednički istovremeni rad na dokumentima i njihovo korištenje s raznih, fiksnih i mobilnih, uređaja dokle god oni imaju osiguran pristup internetu. Unatoč svemu tome, ovaj se rad fokusirao na rizike prelaska na usluge u oblaku sagledane s arhivističkoga stajališta. On objašnjava zašto je potrebno kritički

procijeniti pojedinu uslugu pohrane u oblaku te skreće pozornost na to da se u postkustodijalnoj paradigmi pojavljuje novi faktor, a to su pružatelji usluga pohrane u oblaku, koji stvaratelji arhivskoga gradiva moraju uzeti u obzir baš kao i arhivi. Upravo stoga je potrebno da arhivisti dobro razumiju potencijalne probleme povezane s pohranom arhivskoga gradiva u računalni oblak jer bez dobro uspostavljene usluge, usklađene s arhivskim normama, može vrlo lako doći do narušavanja vjerodostojnosti zapisa, tj. do gubitka autentičnosti, pouzdanosti, iskoristivosti ili integriteta digitalnih zapisa, ali i pravnih problema povezanih s time. Stoga se iz analiziranih rizika mogu lako izvesti konkretne mjere za njihovo smanjenje ili potpuno uklanjanje pa je potpuno jasno da se arhivisti, napose oni koji jesu ili će biti nadležni za pohranu i dugoročno čuvanje digitalnih zapisa, a takvih će trebati sve više, moraju čim prije i čim bolje upoznati s tom problematikom, dobro ju razumjeti i biti sposobni savjetovati kako stvaratelje tako i pružatelje usluga u oblaku o tome.

Literatura

1. Department of Defense (DoD)Cloud ComputingSecurity Requirements Guide (SRG) / Developed by theDefense Information Systems Agency (DISA) for theDepartment of Defense (DoD). Version 1, Release 1, 12. siječnja 2015. URL: http://info.publicintelligence.net/DoD-CloudSecurity.pdf (20. 2. 2015.).
2. Duranti, L. *Preservation in the Cloud: Towards an International Framework for a Balance of Trust and Trustworthiness*.U:*APA/C-DAC International Conference on Digital Preservation and Development of Trusted Digital Repositories*,New Delhi, India 5.–6.February 2014. URL: https://www.academia.edu/11328013/Preservation_in_the_Cloud_Towards_an_International_Framework_for_a_Balance_of_Trust_and_Trustworthiness (8. 9. 2015.).
3. Golubić, K., Stančić, H. *Clearing and Sanitization of Media Used for Digital Storage: Towards Recommendations for Secure Deleting of Digital Files*.U: *Central European Conference on Information and Intelligent Systems 23rd International Conference*. Hunjak, T., Lovrenčić, S.; Tomičić, I. (ur.). Varaždin : Faculty of organization and informatics, 2012.http://

www.ceciis.foi.hr/app/public/conferences/1/papers2012/iss6.pdf (20. 7. 2015.).

4. Key Factors to Consider when hosting DAM in the Cloud / Cognizant 20-20 insights. Studeni 2014. http://www.cognizant.com/InsightsWhitepapers/key-factors-to-consider-when-hosting-dam-in-the-cloud-codex1028.pdf (3. 2. 2015.).
5. On Premise vs. Cloud-based solution / Whitepaper. GFI Software. 2010. URL:http://www.gfi.com/whitepapers/Hybrid_Technology.pdf (3. 2. 2015.).
6. Outsourcing digital data storage / National Archives of Australia. 2015. URL:http://www.naa.gov.au/records-management/agency/secure-and-store/outsourcing-digital-data/index.aspx (22. 7. 2015.).
7. Pan, W., Rowe, J., Barlaoura, G. User Survey Report / Records in the Cloud project. 23. listopada 2013. URL: http://www.recordsinthecloud.org/assets/documents/RiC_Oct232013_User_Survey_Report.pdf (20. 7. 2015.).
8. Stančić, H., Rajh, A., Milošević, I. *"Archiving-as-a-Service". Influence of Cloud Computing on the Archival Theory and Practice*.U: *The Memory of the World in the Digital Age: Digitization and Preservation*. Duranti, L., Shaffer, E. (ur.).UNESCO, 2013. Str. 108–125. URL: http://bib.irb.hr/datoteka/618924.Stancic_Rajh_Milosevic_-_Influence_of_Cloud_Computing_on_the_Archival_Theory_and_Practice.pdf (10. 6. 2015.).
9. Strategija razvoja javne uprave za razdoblje od 2015. do 2020., usvojena na 17. sjednici Sabora 12. lipnja 2015.URL: https://vlada.gov.hr/UserDocsImages/Sjednice/2015/229%20sjednica%20Vlade/229%20-%202.pdf (30. 8. 2015.).

Summary

THE SAFETY OF STORING ARCHIVES IN THE CLOUD STORAGE

The archives in the electronic form are increasingly stored in some form of cloud storage. Due to the fact that in such cases it is mostly the matter of contracting the service

with a third party i.e. a cloud service provider, it is necessary to understand the multi-layered nature of the question of safety in that context. They are important for all the archivists that will be responsible for storage and long-term preservation of such archives, because they will have to evaluate the quality of the service offered by certain providers in order to be able to give the right recommendation about which one to choose, to evaluate potential safety risks and formulate demands on how to reduce or eliminate them. They will also have to make requests and see through the procedures of the long-term preservation when the occasion arises, etc. All this influences the safety of the stored records, their authenticity, reliability, usefulness and integrity. The authors in this paper, hence, analyse the demands for safety of storage of archives in the cloud storage, they suggest the specific measures for reducing potential risks that appear thereat and draw conclusions about how all this affects the archival practice and the education of the archivists.

***Keywords:** archives, cloud storage, storage, safety, risk*

Translated by Marijan Bosnar