Doc. dr. Tatjana HAJTNIK
Arhiv Republike Slovenije, Ljubljana
tatjana.hajtnik@gov.si
Izr. prof. dr. Miroslav NOVAK
Pokrajinski arhiv Maribor, Maribor
miroslav.novak@pokarh-mb.si

1.01 ***Izvorni naučni rad/Original scientific article***
UDK/UDC: 930.25:004:004.8:006.3/.8

INFORMACIJSKA SIGURNOST I PROCESI ARHIVSKOG PROFESIONALNOG RADA

Apstrakt: *Osnovna svrha ovog rada je ispitivanje uloge informacijske bezbjednosti u arhivskim praksama, s posebnim fokusom na digitalizaciju arhivskih procesa, integraciju umjetne inteligencije (AI) i drugih tehnoloških rješenja, te upravljanje rizicima povezanima s dugoročnim skladištenjem i očuvanjem arhivskih materijala.*

U svrhu ovog rada korišteni su različiti metodi. Osnovni metod je metoda proučavanja web resursa i deskriptivna metoda za razumijevanje konteksta i definicije pojma "informacijska bezbjednost". Iste metode su korištene za razumijevanje ovog pojma u arhivskom kontekstu i identifikaciju relevantnih ISO standarda. Metoda sažimanja je korištena za predstavljanje sadržaja ISO standarda u oblasti informacijske bezbjednosti. Iskustveni i deskriptivni metodi su korišteni za predstavljanje informacijske bezbjednosti u Slovenskoj javnoj arhivskoj službi.

Nalazi temeljem studije slučaja, tj. dvije inspekcije informacijske bezbjednosti u Slovenskoj javnoj arhivskoj službi, pokazuju zahtjeve za kontinuiranim identifikovanjem rizika u oblasti informacijske bezbjednosti u (javnim) arhivskim službama. Predstavljanje ISO standarda u oblasti informacijske bezbjednosti ukazuje na složenost ove oblasti. Stoga, arhivske institucije moraju trajno provjeravati koji segmenti informacijske bezbjednosti osiguravaju relativno nizak nivo rizika i koji identificirani rizici zahtijevaju posebnu pažnju u najkraćem mogućem vremenu.

Istraživanje pokazuje da se informacijskoj bezbjednosti u arhivima treba pristupiti holistički. Pri tome, arhivisti se ne smiju ograničiti samo na elektronska okruženja, već moraju jednako razmatrati fizička i druga okruženja. U postupcima određivanja nivoa informacijske bezbjednosti arhivskih organizacija, takođe je potrebno testirati aspekte koji nisu tipično arhivski, npr. oblast upravljanja uslugama, oblast digitalne forenzike, oblast odnosa sa dobavljačima itd. Inspekcije bezbjednosti trebaju se provoditi sistematski i periodično. Dobijeni rezultati trebaju se dugoročno upravljati na odgovarajući

način. Svi zaposleni koji su aktivno povezani s njima na bilo koji način moraju učestvovati u eliminaciji rizika informacijske bezbjednosti u arhivima.

Ključne riječi: *Arhivska teorija i praksa, informacijska bezbjednost, umjetna inteligencija, informacione tehnologije, fizički arhivski dokumenti, elektronski arhivski dokumenti, ISO standardi.*

INFORMATION SECURITY AND PROCESSES OF ARCHIVAL PROFESSIONAL WORK

Abstract: *The basic purpose of this paper is to examine the role of information security in archival practices, with a focus on the digitization of archival processes, the integration of artificial intelligence (AI) and other technological solutions, and the management of risks associated with the long-term storage and preservation of archival materials.*

Various methods were used for the purposes of this paper. The basic method is the method of studying web resources and the descriptive method for understanding the context and definition of the concept of "information security". The same methods were used to understand this concept in an archival context and to identify relevant ISO standards. The summary method was used to present the content of ISO standards in the field of information security. Experiential and descriptive methods were used to present information security in the Slovenian Public Archives Service.

Findings based on the case study, i.e. two inspections of information security in the Slovenian Public Archives Service, show the requirements for continuous identification of risks in the field of information security in (public) archive services. The presentation of ISO standards in the field of information security shows the complexity of this field. Therefore, archival institutions must permanently check which segments of information security ensure a relatively low level of risk and which identified risks require special attention in the shortest possible time.

The research shows that information security in archives needs to be approached in a holistic way. In doing so, archivists must not limit themselves to electronic environments but must equally consider physical and other environments as well. In the procedures for determining the level of information security of archival organizations, it is also necessary to test those aspects that are not typically archival, e.g. the field of service management, the field of digital forensics, the field of supplier relations, etc. Safety inspections should be carried out systematically and periodically. The obtained results should be managed in a long-term appropriate manner. All those employees who are actively connected with them in any way must participate in the elimination of information security risks in the archives.

Key words: *Archival theory and practice, information security, artificial intelligence, information technology, physical archival records, electronic archival records, ISO standards*.

Uvod

U savremenom informacijskom društvu sve više procesa i rješenja se odvija isključivo u digitalnom okruženju. Posljedica toga je rapidno povećanje obima prikupljenih podataka, što stvara potrebu za snažnijom informatičkom infrastrukturom i inovativnim rješenjima koja djelomično ili potpuno oslobađaju ljude od upravljanja obimnim podatkovnim korpusima, izvršavanja raznih zadataka i kreiranja novih sadržaja. Sve veća uključenost tehnoloških rješenja u procese savremenog društva usko je povezana s osiguravanjem neprekidnog rada cjelokupnog digitalnog okruženja, što nosi rizike i mogućnosti zloupotrebe, ne samo u uskom informacijskom sektoru, već na razini cijelog informatičkog društva.

Također, (javne) arhivske službe kao dio tog društva prate ove trendove, jer se razvoj digitalnih tehnologija direktno i indirektno odražava i na arhivsku djelatnost. Savremena rješenja, kao što su „usluge u oblaku" i umjetna inteligencija (UI), već su integrisana u arhivsko profesionalno djelovanje. Arhivsko gradivo tokom vremena stiče kulturnu vrijednost i sve veći značaj za pravnu zaštitu pojedinaca ili grupa. U isto vrijeme, postaje izuzetno važno za različite oblasti kao što su obrazovanje, istraživanje, kreativnost i šira društvena upotreba.

Priznavanje arhivskog gradiva kao važnog društvenog dobra je usko povezano s uspješnom digitalizacijom arhivske djelatnosti, što utiče na dostupnost i korisnost arhivskog gradiva putem savremenih komunikacijskih kanala. To se povezuje s dugoročno stabilnim i sistematski usmjerenim radom pojedinih arhivskih institucija, kao i s očuvanjem i prenošenjem sve većeg broja arhivskih sadržaja različitim korisničkim grupama. Opažamo također direktnu relaciju između korištenja arhivskog gradiva i povećanja broja prikupljenih analitičkih metapodataka, posebno onih koji su povezani s popisnim jedinicama nižih nivoa i koji su korisnicima direktno dostupni putem savremenih komunikacijskih kanala.[1]

Za potrebe poslovnih procesa, arhivi se povezuju s različitim informacijskim sistemima, kao što su upravljanje arhivom, posredovanje gradiva za upravno-pravne procese, materijalna zaštita i vrednovanje stvaralaca. Kao i u drugim digitalizovanim organizacijama, stabilno i sigurno funkcionisanje ovih sistema postaje ključno. U tom kontekstu, informacijska sigurnost postaje bitna

[1] M. Novak, Stanje in perspektive vzajemnega metapodatkovnega korpusa slovenske javne arhivske službe. *Moderna arhivistika* 2023, 6 (2), Pokrajinski arhiv Maribor, Maribor 2023, 308–333. Pridobljeno 1. 7. 2024 s spletne strani: https://doi.org/10.54356/MA/2023/MJUO4040.

komponenta arhivske djelatnosti. Nove tehnologije, poput umjetne inteligencije (UI), interneta stvari (IoT) i „usluge u oblaku" rješenja, otvaraju vrata raznim ranjivostima, što pokreće važna stručna pitanja.

Pojam "informacijska sigurnost" postaje ključna komponenta arhivske djelatnosti, što postavlja profesionalna pitanja kao što su: Kako adekvatno definirati informacijsku sigurnost u arhivskom kontekstu kroz različita vremenska razdoblja? Kako je efikasno uključiti u svakodnevni arhivski profesionalni rad i istovremeno se prilagoditi izuzetno brzom razvoju u ovoj oblasti? I kako u arhivima pravovremeno i dugoročno prepoznati i upravljati rizicima koji bi mogli dovesti do uništenja ili neovlaštenih promjena arhivskih podataka ili metapodataka, čime bi se ugrozila načela dostupnosti, upotrebljivosti, cjelovitosti, autentičnosti i trajnosti arhivskog gradiva?

Sigurna pohrana elektronskih dokumenata, u skladu s propisima, zahtijeva preciznu usmjerenost i tehnička rješenja, što se odražava i u novim standardima i praksama u oblasti dugoročne pohrane arhivskog gradiva. Grobelnik i drugi (2023) su istakli ulogu UI u uspostavljanju novih digitalnih procesa i prenosu dobrih praksi iz srodnih institucija u arhive. Njihova otkrića dodatno naglašavaju značaj UI u suočavanju s izazovima sigurnosti i vjerodostojnosti arhivskog gradiva, posebno u elektronskom arhiviranju.

Korištenje UI će igrati ključnu ulogu u poboljšanju efikasnosti i tačnosti arhivskog profesionalnog rada, posebno u digitalizaciji i očuvanju elektronskog gradiva. Međutim, razvoj i integracija ovih tehnologija zahtijevat će promišljeno razmatranje rizika povezanih s pogrešnom upotrebom i zloupotrebama ovih rješenja.

Definicija pojma "informacijska sigurnost"

Pojam "informacijska sigurnost" možemo definirati na više načina, s obzirom na to da se danas često povezuje sa zaštitom podataka unutar sigurne komunikacijsko-informacijske infrastrukture. Primjer takve definicije možemo pronaći u *Rječniku vojnih i srodnih izraza*, gdje je informacijska sigurnost opisana kao *„… zaštita informacija i informacijskih sistema od neovlaštenog pristupa ili promjene informacija, bilo da su u skladištu, obradi ili prenosu, te od uskraćivanja usluga ovlaštenim korisnicima. Informacijska sigurnost obuhvata mjere potrebne za otkrivanje, dokumentovanje i suprotstavljanje takvim prijetnjama. Informacijska sigurnost se sastoji od računalne sigurnosti i sigurnosti komunikacija."*[2]

Sličnu definiciju možemo pronaći i u Gartnerovom rječniku, gdje se informacijska sigurnost definiše kao *„…zaštita informacija i informacijskih*

[2] *Information security.* (n.d) *Dictionary of Military and Associated Terms*. (2005). Pridobljeno 17. 7. 2024 s spletne strani: https://www.thefreedictionary.com/information+security .

sistema od namjernog i nenamjernog neovlaštenog pristupa, ometanja, promjene i uništenja od strane vanjskih ili unutrašnjih aktera."[3]

Informacijsku sigurnost možemo razmatrati eksplicitno s aspekta informacijskog okruženja ili implicitno s aspekta sigurnosti sadržaja. Kao primjer, možemo navesti definiciju iz slovenskog *Zakona o informacijskoj sigurnosti* (ZInfV), gdje je ona opisana kao *„zaštita, očuvanje i obrana informacijskog okruženja od neovlaštenog pristupa, upotrebe, otkrivanja, ometanja, promjene ili uništenja, s ciljem osiguravanja povjerljivosti, autentičnosti, cjelovitosti i dostupnosti"*[4]

Razumijevanje informacijske sigurnosti može biti mnogo šire kada se gleda iz perspektive informacijskog okruženja, jer pored elektronskog obuhvata i fizička i hibridna okruženja. Na primjer, web stranica *Ureda Vlade Republike Slovenije* definiše informacijsku sigurnost kao *„… zaštitu podataka i informacijskih sistema od nezakonitog pristupa, upotrebe, otkrivanja, ometanja, promjene ili uništenja. To uključuje povjerljivost, cjelovitost i dostupnost podataka bez obzira na njihov oblik: elektronski, tiskani ili bilo koji drugi"*.[5]

Sličnu definiciju informacijske sigurnosti možemo pronaći na web stranici IBM, koja je proširena i na zaštitu usmene komunikacije. Ona je definirana kao *„… zaštita važnih informacija organizacije – digitalnih datoteka i podataka, papirnih dokumenata, fizičkih medija, pa čak i ljudskog govora – od neovlaštenog pristupa, otkrivanja, upotrebe ili promjene."*.[6]

Microsoft definira pojam informacijske sigurnosti na osnovu sigurnosnih postupaka i alata kao *„… skup sigurnosnih procedura i alata koji široko štite osjetljive informacije preduzeća od zloupotrebe, neovlaštenog pristupa, ometanja ili uništenja. Informacijska sigurnost obuhvata fizičku i okolišnu sigurnost, kontrolu pristupa i sajber sigurnost."*.[7] Sličnu definiciju možemo pronaći kod kompanije Fortinet, koja također naglašava zaštitu

[3] Gartner Glossary. (n.d). Gartner. Pridobljeno 1. 7. 2024 s spletne strani: https://www.gartner.com/en/glossary .

[4] ZInfV. *Zakon o informacijski varnosti*. (2023). "Uradni list RS", št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23. Pridobljeno 1. 7. 2024 s spletne strani: https://pisrs.si/pregledPredpisa?id=ZAKO7707.

[5] Informacijska varnost. (2024). Pridobljeno 1. 7. 2024 s spletne strani: https://www.gov.si/teme/informacijska-varnost/

[6] Prevod definicije: Informacijska sigurnost ili 'InfoSec' je zaštita važnih informacija organizacije - digitalnih datoteka i podataka, papirnih dokumenata, fizičkih medija, pa čak i ljudske komunikacije - od neovlaštenog pristupa, otkrivanja, upotrebe ili izmjene. *What is information security?* (N.d). IBM. Pridobljeno 14. 7. 2024 s spletne strani https://www.ibm.com/topics/information-security.

[7] Prevod definicije: Informacijska sigurnost, često skraćeno (InfoSec), je skup sigurnosnih procedura i alata koji generalno štite osjetljive podatke preduzeća od zloupotrebe, neovlaštenog pristupa, ometanja ili uništenja. InfoSec obuhvata fizičku i okolišnu sigurnost, kontrolu pristupa i kibernetičku sigurnost. Information Security (InfoSec) defined. (N.d). Microsoft. Pridobljeno 14. 7. 2024 s spletne strani: https://www.microsoft.com/en-au/security/business/security-101/what-is-information-security-infosec.

nedigitalnih okruženja i dodaje dokumentovanje postupaka informacijske sigurnosti.[8]

Elementi informacijske sigurnosti u arhivskoj djelatnosti prisutni su još od samih početaka čuvanja i očuvanja arhivskog gradiva. Posebni sigurni prostori za skladištenje dokumentacije, nadzorovan pristup i upotreba arhivskog gradiva, kao i prepisivanje sadržaja sa starih na nove medije, samo su neki od primjera aktivnosti koje su arhivski stručnjaci provodili kroz vrijeme i prostor. Na toj osnovi su se tokom stoljeća razvile metode i procedure za čuvanje fizičkog arhivskog gradiva, koje danas nazivamo materijalnom zaštitom. Ako posmatramo arhivsko gradivo kroz prizmu informacijske sigurnosti, tada možemo ove aktivnosti, metode, procedure i standarde definirati kao podskup informacijske sigurnosti za fizičko arhivsko gradivo.

Za zaštitu podataka odnosno informacija iz fizičkog arhivskog gradiva uspostavljen je i sistem pravne zaštite. Ovaj sistem određuje koji su sadržaji slobodno dostupni, a koji su zaštićeni ograničenjima pristupa, s posebnim naglaskom na zaštitu ličnih i drugih osjetljivih podataka. Ova oblast arhivske djelatnosti također se može smatrati jednom od podskupina informacijske sigurnosti.

Obje podskupine informacijske sigurnosti - materijalna i pravna zaštita - kroz istoriju arhivske djelatnosti su se mijenjale u skladu s tehnološkim razvojem, pravnim zahtjevima i sviješću o važnosti očuvanja arhivskog gradiva. Stoga se nivo informacijske sigurnosti u oblasti arhivske djelatnosti nikada nije definisao kao apsolutna vrijednost, već uvijek kao relativna, obično koristeći izraze poput "prikladno" i "neprikladno" ili "sigurno" i "nesigurno".

Od sredine osamdesetih godina prošlog stoljeća počela su se otvarati arhivska stručna pitanja o materijalnoj zaštiti strojno čitljivog (digitalnog) arhivskog gradiva. Time se počinje razvijati treća podskupina faktora informacijske sigurnosti u arhivskoj teoriji i praksi. Velikim dijelom, ovom razvoju doprinijela je digitalizacija cijelih ili dijelova arhivskog gradiva u nadležnim arhivskim institucijama, a još više su na te promjene uticale digitalizacija upravljanja procesima s dokumentarnim gradivom kod nadležnih stvaraoca arhivskog gradiva, kao i digitalizacija postupaka arhivskog stručnog rada u nadležnim arhivskim institucijama. Sve to je izazvalo potrebu za novim rješenjima u oblasti sigurnosti.

Četvrtu veliku podskupinu cijele informacijske sigurnosti možemo prepoznati kao faktore digitalne transformacije arhivske djelatnosti. U tom kontekstu, informacijska sigurnost u arhivu postaje središnji stručni izazov savremene arhivske paradigme. Razumijevanje i neposredna implementacija rješenja iz oblasti informacijske sigurnosti u arhivsku djelatnost više nisu problem samo informatičara i informacijskih rješenja u arhivskim institucijama. U praksi, to postaje problem i istovremeno izazov za svakog zaposlenika u

[8] *What Is Information Security?* (2024). Fortinet. Pridobljeno 14. 7. 2024 s spletne strani: https://www.fortinet.com/resources/cyberglossary/information-security.

arhivu, kao i za svakog korisnika arhivskog gradiva koji je u bilo kakvoj interakciji s arhivskim sadržajem i informacijskim rješenjima, posebno ako je to povezano sa širim, pa čak i globalnim arhivskim i drugim informacijskim sistemima.

U arhivskoj struci dobro je poznat pojam „materijalna zaštita". U slovenskoj *Uredbi o zaštiti dokumentarnog i arhivskog gradiva*, *ovaj pojam obuhvata određivanje uslova za prikladnost prostora i opreme za skladištenje dokumentarnog i arhivskog gradiva, kao i potrebne mjere za osiguranje ovog gradiva od krađe, provale, trošenja, prašine, vatre, vode, neprikladnih temperatura i vlage, svjetlosti i štetnih zračenja, kao i drugih štetnih bioloških, hemijskih i fizičkih uticaja*.[9] Cjelina arhivskih stručnih aktivnosti u oblasti materijalne zaštite arhivskog i dokumentarnog gradiva može se definirati kao sistem upravljanja rizicima u očuvanju i zaštiti ovog gradiva kroz vrijeme. Iz ovoga možemo izvesti zaključak: u slučaju da informacije zapisane u dokumentaciji imaju vrijednost za društvo, materijalnu zaštitu možemo definirati kao podskup arhivskih stručnih aktivnosti koje osiguravaju „informacijsku sigurnost" u arhivima i kod stvaraoca u oblasti fizičkog gradiva.

Za potrebe ovog rada, pojam „informacijska sigurnost" ćemo tretirati kao krovni izraz koji u oblasti arhivske djelatnosti obuhvata širok spektar politika, aktivnosti i mjera usmjerenih na osiguranje dugoročne sigurnosti i očuvanje arhivskog gradiva, uključujući njihove kontekste. Ako kao polazište za definiciju pojma „informacijska sigurnost u arhivu" uzmemo definiciju materijalne zaštite i nadogradimo je definicijom informacijske sigurnosti prema standardu ISO 27000, koja obuhvata sljedeće elemente: politike informacijske sigurnosti, organizaciju informacijske sigurnosti, zaštitu ljudskih resursa, upravljanje imovinom, kontrolu pristupa, kriptografiju, fizičku i okolišnu sigurnost, uspostavljanje, razvoj i održavanje informacijskih sistema, sigurnost operacija, komunikacijsku sigurnost, odnose s dobavljačima, upravljanje incidentima i druge sigurnosne aspekte, možemo oblikovati osnovu za sveobuhvatnu i savremenu sigurnosnu politiku u arhivskim institucijama.

Ako tome dodamo fokus na usluge u oblaku, osiguranje neprekidnog poslovanja IKT, obavještavanje o prijetnjama, nadzor fizičke sigurnosti, maskiranje podataka, brisanje informacija, sprečavanje curenja podataka, aktivnosti praćenja, web filtriranje i sigurno kodiranje[10], dobijamo okvir za kompleksnu i savremenu sigurnosnu politiku koja je potrebna u arhivskoj instituciji. Pri tome je potrebno ovu politiku razmatrati i u svjetlu OAIS[11] modela,

[9] UVDAG. *Uredba o varstvu dokumentarnega in arhivskega gradiva*. (2017). "Uradni list RS", št. 42/17. Pridobljeno 1. 7. 2024 s spletne strani: http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED6619.

[10] M. Edwards, (2024). The Ultimate Guide to ISO 27001. ISMS.online. Pridobljeno 17. 7. 2024 s spletne strani: https://www.isms.online/iso-27001/#iso-270012013-iso-270012022-whats-the-difference .

[11] OAIS (Open Archival Information System) je referentni model za arhivske informacijske sisteme koji definiše standardne principe i zahtjeve za dugoročno čuvanje informacija. Model

posebno zbog statusa osoba koje ulaze u interakciju s nadležnom arhivskom institucijom. Potrebno je razlikovati između stvaraoca ili predavatelja arhivskog gradiva, koji obično djeluju u skladu s određenim i provjerenim sigurnosnim politikama, i korisnika čije sigurnosne prakse nije uvijek moguće osigurati, posebno u slučaju anonimnih korisnika.

ISO standardi u oblasti informacijske sigurnosti

Područje informacione sigurnosti uređeno je nacionalnim i nadnacionalnim zakonodavstvom, kao i brojnim standardima koji obezbeđuju usklađene sigurnosne prakse. Među njima, standardi ISO[12] imaju ključnu ulogu, jer nude sveobuhvatan okvir za upravljanje rizicima i zaštitu informacionih sistema u arhivskom okruženju.[13] Njihova primjena omogućava arhivskim institucijama uspostavljanje sistematskih procedura koje obezbeđuju sigurnost, povjerljivost i cjelovitost njihovih informacionih izvora.

Pored zaštite informacionih sistema, ključno je i razumjevanje uske povezanosti između informacione sigurnosti i dugoročne pohrane zapisa u digitalnom obliku. Sigurnosni incidenti, kao što su gubici podataka ili neovlaštene izmjene, mogu ozbiljno ugroziti dostupnost i autentičnost arhivskog materijala. Stoga, odgovarajuće upravljanje sigurnošću i čuvanje digitalnih zapisa moraju biti pažljivo planirani i sprovodeni, jer je to od suštinskog značaja za dugoročno očuvanje digitalnih arhiva.[14]

U ovom radu ćemo se fokusirati samo na one ISO standarde koji se direktno odnose na obezbijeđivanje informacione sigurnosti u elektronskom okruženju. Zbog ograničenog obima ovog rada, nećemo se detaljno baviti standardima koji regulišu druge aspekte arhivske delatnosti, kao što su upravljanje elektronskim arhivskim materijalom, materijalna zaštita fizičkog arhivskog materijala ili upravljanje dokumentarnim gradivom.

OAIS pruža okvir za organizacije koje se bave arhiviranjem, omogućavajući im da osiguraju, upravljaju i pristupaju informacijama tokom vremena, uz naglasak na očuvanje integriteta i dostupnosti podataka.

[12] ISO standardi su međunarodno priznate smernice koje razvija Međunarodna organizacija za standardizaciju (ISO). Namijenjeni su obezbeđivanju kvaliteta, sigurnosti, efikasnosti i dosljednosti u različitim industrijama.

[13] T. Hajtnik, Ocena in obvladovanje tveganj pri dolgoročni e-hrambi s pomočjo programskega orodja = Assessment and risk management at long-term preservation with the help of software tool. V: Gostenčnik, Nina (ur). *Uporabnikom prijazni arhivi: knjiga povzetkov*: Mednarodna konferenca Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: 11-13. maj 2022, Slovenija, Pokrajinski arhiv Maribor, Radenci 2022, 54.

[14] T. Hajtnik, Kako sta povezani informacijska varnost in dolgoročna hramba zapisov v digitalni obliki. V: Gostenčnik, Nina (ur). *Arhivi v primežu narave in tehnologije: knjiga povzetkov*: Mednarodna konferenca Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: 15-17. maj 2024, Slovenija, Pokrajinski arhiv Maribor, Radenci 2024, 70-71.

Uvod u ISO standarde sa područja informacijske sigurnosti

ISO standardi su ključni za obezbjeđivanje usklađenosti s najboljim praksama u oblasti informacione sigurnosti. U arhivskom okruženju, gdje je potrebno zaštititi materijal kako u fizičkom, tako i u elektronskom obliku, ovi standardi omogućavaju uspostavljanje sistematskih pristupa za zaštitu podataka, obezbjeđivanje neprekidnog rada i smanjenje rizika. Cilj standarda je podržati organizacije u implementaciji robusnih sigurnosnih sistema koji omogućavaju dugoročno očuvanje i dostupnost njihove poslovne dokumentacije.

ISO 19011: Smjernice za procjenu sistema upravljanja

Standard pruža sveobuhvatne smjernice za izvođenje procjena sistema upravljanja, s naglaskom na osiguranje da se svi sigurnosni postupci provode u skladu sa utvrđenim standardima. Standard uključuje načela procjene, vođenje programa procjene te ocjenjivanje kompetencija osoba koje učestvuju u procjenama. Također je značajan za arhivske institucije jer omogućava redovno pregledanje sigurnosnih praksi i osigurava da sistemi rade u skladu s najnovijim standardima. Procjena sistema je ključna za identifikaciju nedostataka i uvođenje poboljšanja koja mogu spriječiti sigurnosne incidente, kao što su gubitak podataka ili neovlašteni pristup arhivskom materijalu.

Veza između definicije informacijske sigurnosti u arhivskim institucijama i ISO standarda je ključna za uspostavljanje sveobuhvatnog sigurnosnog okvira koji omogućava dugoročno očuvanje i sigurnost arhivskog gradiva. Standardi kao što su ISO 27000 i ISO 19011 predstavljaju temelj za oblikovanje savremene sigurnosne politike koja uključuje kako fizičku, tako i digitalnu zaštitu.

ISO 22301: Sistem upravljanja za zaštitu od smetnji

Standard postavlja zahtjeve za uspostavljanje sistema upravljanja koji osigurava zaštitu od smetnji i omogućava brzo oporavak nakon mogućih incidenata. Ovaj standard je posebno važan za arhivske institucije, jer osigurava okvir za reagiranje na nesreće, tehničke greške ili kibernetske napade koji bi mogli utjecati na dostupnost arhivskog gradiva. Osnovni cilj ovog standarda je smanjiti vjerojatnost smetnji i poboljšati spremnost organizacija na reakciju na takve događaje. Uključuje uspostavljanje planova za neprekidno poslovanje koji definiraju ključne procese za osiguranje neprekidnog pristupa podacima, čak i u slučaju vanrednih situacija.

ISO 22313: Smjernice za neprekidno poslovanje

Standard nadograđuje ISO 22301 i pruža detaljnije smjernice za uspostavljanje sistema neprekidnog poslovanja. Predstavlja okvir koji pomaže

organizacijama u implementaciji najboljih praksi za osiguranje neprekidnog rada njihovih sistema. U arhivima, gdje je stalna dostupnost arhivskog gradiva od ključne važnosti, ISO 22313 je neophodan za planiranje i implementaciju strategija koje osiguravaju kontinuitet operacija čak i u vremenima krize. Standard omogućava oblikovanje fleksibilnih planova koji uključuju procjenu rizika, prioritetno određivanje ključnih resursa i osiguranje rezervnih rješenja za backup podataka. Njegov cilj je osigurati da organizacije, uključujući arhivske institucije, mogu brzo i efikasno raditi, bez obzira na moguće smetnje, te da će u slučaju izvanrednih situacija brzo uspostaviti normalno poslovanje.

ISO 16363:2012 Procjena i certificiranje pouzdanih elektronskih repozitorija

Standard postavlja zahtjeve za procjenu i certificiranje elektronskih repozitorija kako bi se osigurala njihova dugoročna pouzdanost, integritet i dostupnost elektronskog gradiva. Definira kriterije koje je potrebno ispuniti za dugoročno čuvanje elektronskog gradiva i pruža okvir za ocjenjivanje elektronskih repozitorija u smislu njihove sposobnosti očuvanja autentičnosti, cjelovitosti, dostupnosti i upotrebljivosti elektronskog gradiva tokom vremena.

Ovaj standard je posebno značajan za arhivske institucije koje upravljaju dugoročnim čuvanjem elektronskog gradiva, jer omogućava provjeru da li elektronski repozitoriji ispunjavaju zahtjeve za dugoročno očuvanje osjetljivih podataka i kulturne baštine. Arhivskim institucijama pomaže da uspostave povjerenje u svoje elektronske arhive i osigurava da ti sistemi ispunjavaju najviše standarde u pogledu sigurnosti i pouzdanosti.

Ključni ISO standardi za informatičku i kibernetsku sigurnost u arhivskim sistemima

Povjerenje u dugoročna rješenja za pohranu elektronskog gradiva zahtijeva jasne sigurnosne protokole, jer već mala greška može uzrokovati nepovratne gubitke podataka. ISO standardi u ovoj oblasti nude pouzdan okvir za upravljanje rizicima i zaštitu elektronskih arhiva.[15]

Obitelj standarda ISO 27000 pokriva široku oblast informacijske sigurnosti i uključuje niz standarda koji organizacijama pomažu u zaštiti svojih informacija i sistema. Ovi standardi pružaju organizacijama smjernice za upravljanje rizicima i prijetnjama koje bi mogle ugroziti principe sigurne pohrane elektronskog arhivskog gradiva (dostupnost, upotrebljivost, cjelovitost, autentičnost, trajnost). Usklađenost s ovim standardima ne samo da povećava

[15] T. Hajtnik, *Elektronsko arhiviranje : ISO standardi kot odgovor na zakonska določila*: predavanje na 3. mednarodni konferenci e-ARH.si, Ljubljana, 7-8. november 2018.

sigurnosnu otpornost arhiva, već i jača povjerenje javnosti u dugoročnu pohranu digitalnih zapisa.[16]

U nastavku su istaknuti ključni standardi koji su posebno važni i za arhivske ustanove:

ISO/IEC 27001:2022 Zahtevi za sistem upravljanja sigurnošću informacija

ISO/IEC 27001 je osnovni standard za uspostavljanje, implementaciju, održavanje i poboljšanje sistema upravljanja sigurnošću informacija (u daljnjem tekstu: SUSI). Organizacijama omogućava da smanje sigurnosne rizike i zaštite podatke od povreda, uključujući sveobuhvatne sigurnosne mjere.

ISO/IEC 27002:2022 Smjernice za implementaciju sigurnosnih kontrola

Standardu ISO/IEC 27001 je komplementaran standard ISO 27002, koji nudi referentni popis općih kontrola u oblasti informacijske sigurnosti i detaljna uputstva za njihovu implementaciju. Namijenjen je organizacijama koje žele poboljšati sigurnosne mjere u skladu s ISO/IEC 27001 i obuhvata različita područja informacijske sigurnosti, od tehničkih do organizacijskih mjera.

ISO/IEC 27003:2017 Praktična pomoć pri implementaciji ISO 27001

Standard pruža smjernice za učinkovitu implementaciju SUSI. Nudi praktične savjete i alate za uspostavljanje sigurnosnih mjera, kako ih definira standard ISO/IEC 27001.

ISO/IEC 27004:2023 Mjerenje uspješnosti sigurnosnih sistema

Standard je fokusiran na mjerenje uspješnosti i efikasnosti SUSI prema standardu ISO/IEC 27001. Definira konkretne metode za praćenje, mjerenje, analiziranje i ocjenjivanje sigurnosnih kontrola, što organizacijama omogućava da tačno prate uspješnost svojih sigurnosnih mjera.

ISO/IEC 27005:2022 Upravljanje rizicima u oblasti informacijske sigurnosti

Standard pruža smjernice i uputstva za prepoznavanje, ocjenjivanje i upravljanje rizicima povezanim s informatičkom sigurnošću. Usko je povezan sa standardima ISO/IEC 27001 i ISO/IEC 27002 i pomaže organizacijama u sistematičnom upravljanju sigurnosnim rizicima.

[16] *Ibidem*.

ISO/IEC 27006-1:2024 Certificiranje sistema upravljanja informatičkom sigurnošću

Standard definiše zahtjeve za tijela koja certificiraju sisteme upravljanja sigurnošću informacija (SUSI). Fokus je na kompetencijama i pouzdanosti certifikacionih tijela koja ocjenjuju usklađenost organizacija sa standardom ISO/IEC 27001.

ISO/IEC TS 27006-2:2021 Akreditacija certifikacijskih organa za sisteme upravljanja privatnošću

Standard pruža smjernice za akreditaciju[17] certifikacijskih organa koji certifikuju[18] sisteme za upravljanje privatnošću informacija. Definiše zahtjeve i daje smjernice za procjenitelje koji ocjenjuju usklađenost organizacija sa standardima ISO/IEC 27701 i ISO/IEC 27001.

ISO/IEC 27007:2020 Smernice za procese sistema upravljanja sigurnošću informacija

Standard sadrži smjernice za izvođenje procesa sistema upravljanja sigurnošću informacija (SUVI) u skladu sa ISO/IEC 27001. Namijenjen je onima koji moraju razumjeti i provoditi unutrašnje ili vanjske procese sigurnosnih sistema. Uključuje metode za ocjenjivanje kompetentnosti revizora i upravljanje revizijskim programima.

ISO/IEC TS 27008:2019 Pregled i ocjenjivanje sigurnosnih kontrola

Standard određuje smjernice za pregled i tehničko ocjenjivanje implementacije i funkcionisanja sigurnosnih kontrola u okviru ISO/IEC 27001. Fokusira se na osiguranje tehničke usklađenosti kontrola informacijske sigurnosti.

[17] *Akreditacija* je postupak kojim neovisni i ovlašteni organ (akreditacijski organ) potvrđuje da certifikacijski organi ispunjavaju određene zahtjeve za obavljanje certifikacijskih usluga. Radi se o postupku ocjenjivanja i odobravanja koji osigurava da certifikacijski organ djeluje u skladu s određenim međunarodno priznatim standardima, kao što je ISO/IEC 17021 (za certifikaciju sistema upravljanja). Akreditacija potvrđuje kompetentnost, nepristrasnost i dosljednost certifikacijskih organa.

[18] *Certifikacija* je postupak kojim certifikacijski organ potvrđuje da određeni proizvod, proces, sistem ili organizacija ispunjavaju određene zahtjeve ili standarde (npr. ISO 27001 za informacijsko sigurnost). Certifikacija je dakle namijenjena potvrđivanju da su određeni procesi ili sistemi u skladu sa zahtjevima standarda.

ISO/IEC 27017:2015 Sigurnosne kontrole za usluge u oblaku

Standard se fokusira na specifične sigurnosne izazove u okruženjima oblaka i pruža smjernice za implementaciju kontrola informacijske sigurnosti u oblaku. U praksi se skup tih kontrola može razlikovati u zavisnosti od toga da li se radi o korisnicima ili pružateljima usluga u oblaku. Također, može se razlikovati prema procjenama rizika i drugim pravnim, ugovornim, regulatornim ili drugim zahtjevima u vezi sa informacijskom sigurnošću.

ISO/IEC 27018:2019 Zaštita ličnih podataka u oblaku

Standard definiše zahtjeve za zaštitu ličnih podataka prilikom korištenja oblaka. Na osnovu zahtjeva ovog standarda, pružatelji oblaka moraju provoditi zaštitu na načine koji omogućavaju njima i njihovim klijentima ispunjavanje zahtjeva važeće legislative i propisa o zaštiti ličnih podataka. Ovi zahtjevi se također mogu razlikovati u zavisnosti od pravne nadležnosti i uslova ugovora između pružatelja usluga u oblaku i klijenta.

ISO/IEC 27031:2011 Neprekidno poslovanje IKT sistema

Standard određuje smjernice za osiguranje neprekidnog poslovanja informacijske i komunikacijske tehnologije (IKT). Organizacijama pomaže u pripremi planova za neprekidno poslovanje u slučaju poremećaja ili vanrednih situacija.

ISO/IEC 27032:2023 Smernice za kibernetsku sigurnost

Standard ISO 27032 je međunarodno priznat standard, namijenjen upravljanju kibernetskim rizicima. Dizajniran je kao pomoć organizacijama u zaštiti od kibernetskih napada i upravljanju rizicima povezanima s korištenjem informacijske tehnologije. Pruža smjernice za prepoznavanje, ocjenjivanje i upravljanje kibernetskim rizicima, kao i smjernice za reagiranje na incidente i oporavak nakon njih.

ISO/IEC 27033-1:2015 Sigurnost računalnih mreža

Standard pruža pregled sigurnosti računalnih mreža i povezanih definicija. Definira i opisuje koncepte povezane s sigurnošću mreže te daje smjernice za planiranje, implementaciju i održavanje sigurnosnih mjera u mrežama.

ISO 27033-2:2012 Planiranje i dizajn sigurnosti mreža

Standard daje smjernice organizacijama za planiranje, dizajniranje i implementaciju sigurnosti mreža. Pruža praktične preporuke za dokumentiranje sigurnosnih kontrola u mrežnim strukturama.

ISO 27033-3:2010 Sigurnosne prijetnje i zaštitne mjere za mreže

Prijetnje, tehnike planiranja i nadzorne probleme povezane s referentnim mrežnim scenarijima definira standard ISO 27033-3. Za svaki scenarij nudi detaljna uputstva o sigurnosnim prijetnjama, tehnikama i kontrolama sigurnosnog planiranja potrebnim za ublažavanje povezanih rizika. Standard se u određenim dijelovima poziva na standarde ISO/IEC 27033-4, ISO/IEC 27033-5 i ISO/IEC 27033-6.

ISO 27033-4:2014 Sigurnost komunikacija između mreža (sigurnosni prolazi)

Standard sadrži smjernice za zaštitu komunikacija između mreža korištenjem sigurnosnih prolaza (vatrozid, sustav zaštite od upada itd). U skladu s politikom informacijske sigurnosti prolaza, definira: metode prepoznavanja i analize sigurnosnih prijetnji mreže, mrežne sigurnosne zahtjeve, korištenje tehnika za planiranje i upravljanje prijetnjama, te metode rješavanja pitanja vezanih uz implementaciju, rad, praćenje i reviziju postavljenih kontrola.

ISO 27033-5:2013 Sigurnost virtualnih privatnih mreža (VPN)

Standard daje smjernice za odabir, implementaciju i praćenje tehničkih kontrola potrebnih za osiguranje sigurnosti veza virtualnog privatnog mrežnog (VPN) povezivanja između mreža i za povezivanje udaljenih korisnika s mrežama.

ISO 27033-6:2016 Sigurnost bežičnih mreža

Sigurnosni zahtjevi i povezane prijetnje, sigurnosna kontrola te tehnike planiranja bežičnih mreža nalaze se u standardu ISO 27033-6. Zahtjevi su namijenjeni upotrebi prilikom pregleda ili odabira tehničke sigurnosne arhitekture/dizajnerskih opcija koje uključuju korištenje bežične mreže u skladu s ISO/IEC 27033-2. Standard je namijenjen korisnicima i izvođačima odgovornim za implementaciju i održavanje tehničkih kontrola potrebnih za osiguranje sigurnih bežičnih mreža.

ISO/IEC 27033-7:2023 Sigurnost virtualizacijske mrežne infrastrukture

Sigurnosni rizik u vezi s virtualizacijskom mrežnom infrastrukturom te smjernice za implementaciju sigurnosti virtualizacije mreže nalaze se u standardu ISO 27033-7. Namijenjen je korisnicima i izvođačima koji su odgovorni za implementaciju i održavanje tehničkih kontrola potrebnih za osiguranje sigurnih virtualizacijskih okruženja.

ISO/IEC 27034:2011 – Sigurnost aplikacija

Standard ISO/IEC 27034 pruža smjernice za zaštitu aplikacija i njihovog životnog ciklusa, što je važno i za arhive i organizacije koje koriste aplikacije za obradu i pohranu podataka.

ISO/IEC 27035-1:2023 Upravljanje incidentima u informacijskoj sigurnosti

Standard ISO/IEC 27035-1 je ključni dio serije standarda za upravljanje incidentima informacijske sigurnosti. Definira ključne koncepte, principe i procese za učinkovito upravljanje incidentima u informacijskoj sigurnosti. Pruža strukturirani pristup pripremi, otkrivanju, izvještavanju, ocjenjivanju i odgovoru na incidente. Također sadrži smjernice za prilagodbu ovih procesa prema vrsti, veličini i prirodi poslovanja organizacije. Organizacijama omogućava poboljšanje njihove spremnosti i odgovora na sigurnosne incidente.

ISO/IEC 27035-2:2023 – Planiranje odgovora na incidente

Standard nastavlja sa smjernicama za planiranje i pripremu odgovora na incidente te sticanje iskustava iz odgovora na incidente. Poziva se i na ISO/IEC 27035-1:2023, poglavlje 5.2 i 5.6. Organizacije mogu prilagoditi smjernice date u ovom standardu prema vrsti, veličini i prirodi poslovanja u vezi s rizicima u informacijskoj sigurnosti.

ISO/IEC 27035-3:2020 Operativni aspekti odgovora na incidente

Standard se bavi operativnim aspektima upravljanja incidentima, uključujući kibernetičke prijetnje, s aspekta ljudi, procesa i tehnologije. Fokusira se na sve ključne faze odgovora na incidente: od otkrivanja i izvještavanja, preko trijaže i analize, do odgovora, zadržavanja, uklanjanja i obnavljanja sistema. Standard pokriva i korištenje zaštitnih alata, poput vatrozida, IDS/IPS sistema, te jasne procedure za upravljanje incidentima i strukture izvještavanja unutar organizacije. Pruža temelje za učinkovito upravljanje incidentima i sprečavanje ponovnih napada.

ISO/IEC 27036-1:2021 Sigurnost u odnosima s dobavljačima

Standard ISO/IEC 27036-1 je uvodni dio porodice standarda ISO/IEC 27036. Ovaj standard pruža pregled zaštite informacijskih sistema u okviru poslovnih odnosa s dobavljačima. Definira principe za osiguranje sigurnosti informacija u lancu opskrbe te postavlja ključne sigurnosne zahtjeve koje treba uzeti u obzir pri poslovanju s dobavljačima. Naglašava potrebu za jasnom komunikacijom i nadzorom sigurnosnih mjera u svim fazama odnosa između organizacija i dobavljača, što je ključno za zaštitu osjetljivih podataka.

ISO/IEC 27036-2:2022 Zaštita informacija između naručitelja i dobavljača

Standard definira temeljne zahtjeve za osiguranje sigurnosti informacija u cijelom životnom ciklusu narudžbi i isporuka. Pruža smjernice za uspostavljanje, upravljanje i poboljšanje sigurnosnih praksi između naručitelja i dobavljača te obuhvaća različite scenarije, uključujući isporuku softvera i hardvera, održavanje poslovnih procesa i usluga računarstva u oblaku. Naglašava važnost transparentnosti i upravljanja sigurnosnim rizicima u svim fazama poslovnih odnosa.

ISO/IEC 27036-3:2023 Upravljanje rizicima u lancima opskrbe

Standard sadrži smjernice za naručitelje proizvoda i usluga te dobavljače hardvera i softvera o transparentnosti i upravljanju rizicima za sigurnost informacija, koji nastaju iz fizičke disperzije i višeslojnog lanca opskrbe hardverom, softverom i uslugama. Također sadrži smjernice za odgovor na rizike koji proizađu iz fizičke disperzije i višeslojnog lanca opskrbe, što može utjecati na informatičku sigurnost u organizacijama koje ga koriste. Dokument predviđa i uključivanje procesa i praksi zaštite informacija u procese životnog ciklusa sistema i softvera, kao što je opisano u standardima ISO/IEC/IEEE 15288, ISO/IEC/IEEE 12207 i ISO/IEC 27002.

ISO/IEC 27036-4:2016 Bezbednost prilikom korištenja usluga u oblaku

Za klijente i pružatelje usluga u oblaku, ovaj standard pruža upute za sticanje uvida u rizike za bezbjednost informacija povezane s korištenjem usluga u oblaku, efikasno upravljanje tim rizicima i odgovaranje na rizike karakteristične za sticanje ili pružanje usluga u oblaku, koji mogu uticati na bezbjednost informacija u organizacijama koje koriste te usluge.

ISO/IEC 27037:2012 Postupanje s digitalnim dokazima

Standard daje smjernice za postupanje s potencijalnim digitalnim dokazima, koji su ključni u istragama incidenata informacione bezbjednosti. Definiše procedure identifikacije, prikupljanja, sticanja i očuvanja potencijalnih digitalnih dokaza. Također postavlja opšte smjernice za postupanje s nedigitalnim dokazima, koji mogu biti značajni u analizi incidenata, te pomaže organizacijama u njihovim disciplinskim postupcima i razmjeni potencijalnih digitalnih dokaza među nadležnim organizacijama.

ISO/IEC 27039:2015 Detekcija i prevencija provale (IDS/IPS)

Standard pruža smjernice za planiranje, izbor i implementaciju sistema za detekciju i prevenciju provala (IDS/IPS). Naglasak je na osiguravanju da su ovi sistemi pravilno konfigurisani za detekciju, prevenciju i odgovaranje na kibernetičke napade. Uključuje smjernice za pravilnu instalaciju i funkcionisanje takvih sistema, kao i kontinuirano praćenje tih sistema kako bi se obezbijedila optimalna zaštita od provale.

ISO/IEC 27040:2024 Sigurno skladištenje podataka

Standard nudi detaljne smjernice za sigurno skladištenje podataka. Pruža tehničke i operativne zahtjeve za planiranje, upravljanje i zaštitu podataka u različitim scenarijima skladištenja, bilo na uređaju ili tokom prenosa putem komunikacijskih veza. Uključuje i sigurnosne zahtjeve za hardver i softver, te kontrolu pristupa, čime se osigurava sveobuhvatna sigurnosna strategija za zaštitu osjetljivih podataka tokom cijelog životnog ciklusa.

ISO/IEC 27701:2019 Upravljanje privatnošću informacija

Standard ISO 27701 proširuje porodicu standarda ISO/IEC 27000 i definiše zahtjeve za upravljanje ličnim podacima. Pruža smjernice za uspostavljanje sistema za zaštitu ličnih podataka i osiguranje usklađenosti sa zakonodavstvom o zaštiti podataka, kao što su Opća uredba EU o zaštiti podataka (GDPR) i Kalifornijski zakon o pravima na privatnost (CPRA). Uključuje kontrole specifične za privatnost i pomaže organizacijama u uvođenju politika za zaštitu privatnosti i poboljšanje njihove usklađenosti s propisima o zaštiti ličnih podataka.

ISO/IEC 27799:2016 Upravljanje sigurnošću informacija u zdravstvenoj informatici

Ovaj standard je posebno dizajniran za zdravstvene organizacije i fokusira se na sigurnost informacija u zdravstvenoj informatici. Temelji se na

smjernicama ISO/IEC 27002 i prilagođava ih potrebama zdravstvenih podataka, posebno u zaštiti ličnih zdravstvenih informacija. Osigurava minimalnu razinu sigurnosti koja mora biti održavana u zdravstvenim ustanovama, te podstiče zaštitu povjerljivosti, cjelovitosti i dostupnosti osjetljivih zdravstvenih podataka

Ključni komplementarni ISO standardi za informacijsku sigurnost

Pored grupe standarda ISO 27000, sve važniji u arhivskoj praksi postaju i standardi ISO 16363 i ISO 18128, jer pružaju okvir za uspostavljanje pouzdanih sistema za dugoročnu e-arhivu arhivskog gradiva.[19] (Hajtnik, 2020; Hajtnik, 2021). *ISO 16363*, koji definiše zahtjeve za održive digitalne arhive, ključan je za osiguranje vjerodostojnosti i cjelovitosti elektronskih zapisa, dok *ISO 18128*[20] nudi smjernice za učinkovito upravljanje rizicima prilikom obrade i čuvanja elektronskih zapisa. Zajedno omogućavaju bolje strateško planiranje i provođenje sigurnosnih mjera koje smanjuju rizike od gubitka podataka, neovlaštenih promjena i drugih sigurnosnih incidenata, što je od ključne važnosti za povjerenje u arhivske sisteme. Korištenje ovih standarda omogućava arhivskim institucijama da uspostave i održavaju visoku razinu informacijske sigurnosti, čime se osigurava dugoročna očuvanost i sigurnost elektronskog gradiva.

Dodatno, uz navedene standarde, ističemo još dva ISO standarda koja igraju važnu ulogu u uspostavljanju cjelovitih sistema upravljanja informacijskom sigurnošću i uslugama u arhivskim sistemima, a to su:

ISO 31073:2022 - Standard za terminologiju upravljanja rizicima

Ovaj standard predstavlja ključni okvir za razvoj zajedničkog razumijevanja koncepata i terminologije upravljanja rizicima. Definira jedinstven rječnik koji organizacije mogu koristiti za usklađeno upravljanje rizicima u različitim aplikacijama. Terminologija iz ovog dokumenta osigurava

[19] T. Hajtnik, Skladnost s standardom ISO 16363 - je to odgovor za našo digitalno prihodnost? = ISO 16363 compliance - is this the answer for our digital future?. V: Semlič Rajh, Zdenka (ur). *Arhivi v službi človeka - človek v službi arhivov: relevance v raziskavah arhivske znanosti = Archives in the Service of People - People in the Service of Archives: Relevance in the Research of Archival Science*: 8. znanstvena konferenca z mednarodno udeležbo Za človeka gre: relevanca znanosti in izobraževanja = 8th Scientific Conference with International Participaton All About People: Relevance of Science and Education : 5. znanstveno raziskovalni, študijski in izobraževalni simpozij = 5th Scientific Research, Study and Educational Symposium: zbornik recenziranih prispevkov = peer-rewieved proceedings book : Maribor, 14. 3. 2020, 72-81. Maribor: AMEU - ECM, Alma Mater Press. Pridobljeno 17. 10. 2024 s spletne strani: http://press.almamater.si/index.php/amp/catalog/book/22; T. Hajtnik, *Upravljanje s tveganji pri dolgoročni e-hrambi: rešitve za ustvarjalce*: spletno predavanje na 5. konferenci e-ARH.si, 17-18. 11. 2021.

[20] ISO 18128:2024 Informacija i dokumentacija — Rizici zapisa — Procjena rizika za upravljanje zapisima.

jasno i dosljedno razumijevanje pojmova povezanih s upravljanjem rizicima s kojima se organizacije suočavaju. Tako omogućava bolju komunikaciju među različitim sudionicima te učinkovitije upravljanje rizicima unutar organizacija.

ISO/IEC 20000-1:2018 - Zahtjevi za sistem upravljanja uslugama (SUS)

Standard ISO/IEC 20000-1 definira zahtjeve za uspostavljanje, implementaciju, održavanje i kontinuirano poboljšanje sistema upravljanja uslugama (SUS). Ovaj sistem omogućava upravljanje cijelim životnim ciklusom usluga, od planiranja i dizajniranja do prijelaza i poboljšanja usluga, koje ispunjavaju dogovorene zahtjeve i donose vrijednost za klijente, korisnike i organizaciju koja pruža usluge. Njegova svrha je osigurati da usluge odgovaraju dogovorenim zahtjevima i donose vrijednost za klijente, korisnike i organizaciju koja ih pruža. Implementacija SUS-a je strateška odluka koju diktiraju ciljevi organizacije, upravne zahtjeve te potrebe za učinkovitim i fleksibilnim uslugama. Standard osigurava kontinuiranu vidljivost, nadzor i poboljšanja, što dovodi do povećane učinkovitosti u upravljanju uslugama.

Implementacija ISO standarda informacijske sigurnosti u arhivskim institucijama

Zahtjevi, preporuke ili smjernice ISO standarda u oblasti informacijske sigurnosti mogu se implementirati u arhivskim institucijama na različite načine - direktno putem uvođenja standarda ili indirektno kroz važeću nacionalnu arhivsku legislativu. Primjer implementacije ovih zahtjeva u Sloveniji je prilagodba zakonodavstva u oblasti arhivske djelatnosti i informacijske sigurnosti.

Oblast arhivske djelatnosti u Sloveniji uređuje Zakon o zaštiti dokumentarnog i arhivskog gradiva te arhivima[21], (ZVDAGA), koji definiše brojne zakonske zahtjeve u vezi s čuvanjem i zaštitom arhivskog gradiva. Ovi zahtjevi su često povezani s implementacijom međunarodnih standarda, poput ISO standarda, koji pružaju smjernice za odgovarajuće postupanje s elektronskim arhivskim gradivom. ISO standardi su ključni za osiguranje usklađenosti arhivske prakse sa zakonskim odredbama, jer omogućavaju uspostavljanje adekvatnih sigurnosnih politika i protokola za dugoročno čuvanje elektronskog gradiva.[22]

Specifično se na informacijsku sigurnost u arhivima odnose i sljedeći podzakonski akti:

- *Uredba o zaštiti dokumentarnog i arhivskog gradiva* [23] (UVDAG);

[21] "Uradni list RS", št. 30/06 in 51/14.
[22] T. Hajtnik, *Elektronsko arhiviranje: ISO standardi kot odgovor na zakonska določila*: predavanje na 3. mednarodni konferenci e-ARH.si, Ljubljana, 7-8. november 2018.
[23] "Uradni list RS", št. 42/17.

- *Pravilnik o jedinstvenim tehnološkim zahtjevima za preuzimanje i čuvanje gradiva u digitalnom obliku*.[24] (PETZ) te
- *Pravilnik o stručnoj osposobljenosti za rad s dokumentarnim gradivom*[25] (PSUDDG).

Oblast informacijske sigurnosti u Sloveniji uređuju i:
- *Zakon o informacijskoj sigurnosti*[26] (ZInfV),
- *Zakon o kritičnoj infrastrukturi*[27] (ZKI),
- *Uredba o sigurnosnoj dokumentaciji i minimalnim sigurnosnim mjerama povezanih subjekata*[28] (UVDMVUPS),

Zakon o zaštiti dokumentarne i arhivske građe i arhivima (ZVDAGA)

U ZVDAGA se nalazi mnogo članova koji su posredno ili neposredno usmjereni na ograničavanje različitih rizika, uključujući informacijske rizike koji se javljaju u oblasti arhivske djelatnosti u Sloveniji. Posebna pažnja na informacijsku sigurnost posvećena je u člancima koji definišu periode nedostupnosti arhivske građe, kao i obaveze javnopravnih osoba u zaštiti osjetljivih podataka. Ključni aspekt informacijskog rizika razmatra i poglavlje o osiguravanju infrastrukture i usluga, gdje se zahtijeva uspostavljanje i održavanje sigurne infrastrukture za upravljanje arhivskom gradivom. Ovaj dio zakonodavstva se efikasno povezuje sa zahtjevima ISO standarda, posebno standarda iz porodice ISO/IEC 27000, koji pokrivaju uspostavljanje sigurnosnih politika, zaštitu podataka i kontrolu pristupa. Implementacija ovih standarda u arhivske procese pomaže u osiguravanju dugoročne očuvanosti arhivske građe, sigurnosti pristupa i usklađenosti s pravnim zahtjevima.

Uredba o zaštiti dokumentarne i arhivske građe (UVDAG)

UVDAG se, slično kao i ZVDAGA, posredno ili neposredno odnosi na upravljanje rizicima koji se javljaju pri dugoročnom čuvanju i upravljanju arhivskom građom. Veliki dio odredbi UVDAG fokusira se na informacijsko osiguranje, posebno članci koji se bave fazama prikupljanja, čuvanja i pratećih usluga, sadržajem unutrašnjih pravila, praćenjem i sprovođenjem tih pravila, kao i dodatnim zahtjevima za pružatelje usluga čuvanja.

[24] "Uradni list RS", št. 118/20.
[25] "Uradni list RS", št. 66/16.
[26] "Uradni list RS", št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23.
[27] "Uradni list RS", št. 75/17 in 189/21 – ZDU-1M.
[28] "Uradni list RS", št. 8/23.

Pravilnik o jedinstvenim tehnološkim zahtjevima za prikupljanje i čuvanje građe u digitalnom obliku (PETZ)

PETZ je u velikoj mjeri operativni dokument, u kojem se gotovo svi članci odnose na oblast informacijske sigurnosti. Praktično svi članci pravilnika povezuju se s sigurnosnim aspektima, pri čemu su posebno istaknuti elementi poput unutrašnjih pravila i njihovog sprovođenja, stručne osposobljenosti procjenjivača, neprekidnog rada, određivanja odgovorne osobe za informacijsku sigurnost, procjena rizika i plan upravljanja rizicima. Također, pravilnik pokriva fizičko i tehničko osiguranje prostorija i opreme, upravljanje sigurnosnim incidentima, kontrolu i sigurnosne preglede. Usko je usklađen s međunarodnim standardima, kao što su ISO/IEC 27001 i ISO/IEC 27005, koji definišu metode za identifikaciju i upravljanje informacijskim rizicima, te osiguravaju usklađenost s sigurnosnim zahtjevima, čime se arhivskim institucijama omogućava dugoročna zaštita elektronske arhivske građe.

Pravilnik o stručnoj osposobljenosti za rad s dokumentarnim gradivom (PSUDDG)

PSUDDG izričito navodi da je informacijska sigurnost ključni sastavni dio kurikuluma za obrazovanje osoba koje rade s dokumentarnim gradivom. Obrazovanje u oblasti sigurnosti se oslanja na zahtjeve ISO standarda, kao što su ISO/IEC 27001 (koji određuje uspostavljanje sigurnosne uprave) i ISO/IEC 27002 (koji pruža smjernice za implementaciju sigurnosnih kontrola). Tako PSUDDG doprinosi osposobljenosti arhivskih radnika u oblasti informacijske sigurnosti, što je od suštinskog značaja za održavanje visokih sigurnosnih standarda prilikom rada s dokumentarnim gradivom u fizičkom i elektronskom obliku.

Zakonodavstvo na polju informacijske sigurnosti

Zakonodavstvo u oblasti informacijske sigurnosti, uključujući ZInfV, ZKI i UVDMVUPS, izravno se odnosi na Arhiv Republike Slovenije (Arhiv RS), kao i na cijelu slovensku javnu arhivsku službu, posebno zbog zajedničkog upravljanja slovenskim elektronskim arhivom e-ARH.si. Na osnovu prvog stavka 9. člana ZInfV, Vlada Republike Slovenije je odredila da je Arhiv RS obveznik koji upravlja informacijskim sistemima i dijelovima mreže, te provodi informacijske usluge koje su ključne za nesmetano funkcioniranje države ili za osiguranje nacionalne sigurnosti.

Unutar Arhiva RS djeluje *Sektor za elektronske arhive i računarsku podršku*, koji je odgovoran za planiranje, razvoj, testiranje i implementaciju informacijskih rješenja namijenjenih podršci stručnom arhivskom radu. Osim toga, ovaj sektor se brine za održavanje visoke razine informacijske sigurnosti. Tako su slovenski arhivi obvezani poštovati sigurnosne politike utvrđene

zakonodavstvom, što uključuje korištenje sigurnih veza, odgovarajuća pravila za promjenu lozinki i druge sigurnosne mjere koje su u skladu s međunarodnim standardima, kao što je ISO/IEC 27001.

Implementacija ovih sigurnosnih politika u skladu sa zakonodavstvom i standardima osigurava zaštitu arhivske građe te sigurno i pouzdano funkcioniranje informacionih sistema, što je ključno za dugoročnu sigurnost i očuvanje arhivske građe. Tako se slovenski arhivi usklađuju s međunarodnim smjernicama i standardima, što omogućava uspješno suočavanje sa sigurnosnim izazovima u savremenom arhivskom okruženju..

Informacijska sigurnost pri arhivskom stručnom radu

Informacijska sigurnost je ključni aspekt arhivskog stručnog rada, jer nije ograničena samo na elektronsko okruženje, već su faktori rizika informacijske sigurnosti prisutni u različitim procesima arhivskog stručnog rada. Ovo se ne odnosi samo na pitanja adekvatne materijalne i pravne zaštite arhivskog gradiva, ili na zaštitu osjetljivih podataka u arhivima, već također uključuje vrlo jednostavne svakodnevne aktivnosti, gdje može doći do promjene redoslijeda arhivskog gradiva, pogrešnog odlaganja tehničkih jedinica, neodgovarajućeg povezivanja arhivskih opisa s njihovim digitalnim kopijama, a na kraju i zbog namjernog curenja podataka. Čak i manje greške mogu ugroziti vjerodostojnost gradiva, stoga je nužno uspostaviti robusne sisteme i protokole za sprječavanje ovih rizika.

Namjerne i nenamjerne promjene

Rizici se često javljaju nenamjerno, na primjer, prilikom neodgovarajućeg rukovanja gradivom, što može dovesti do privremenog ili trajnog onemogućavanja pristupa informacijama arhivske vrijednosti. Česti primjeri uključuju nenamjerno mijenjanje redoslijeda ili nepravilno označavanje arhivskog gradiva. S druge strane, postoje i slučajevi namjernog curenja podataka ili krađa, što naglašava potrebu za boljim sigurnosnim rješenjima.

Materijalna zaštita i ABC metoda

Na polju materijalne zaštite cjelokupnog spektra kulturne baštine, posebno se ističe ABC metoda ili metoda Michalski, koja se temelji na standardu ISO 31000 i predstavljena je u publikaciji pod naslovom “The ABC Method: a risk management approach to the preservation of cultural heritage”.[29] Primjena

[29] S. Michalski, J. L. Pedersoli, *The ABC Method: A risk management approach to the preservation of cultural heritage.* 163 strani. Canadian Conservation Institute Ottawa 2016. Pridobljeno 1. 7. 2024 s spletne strani: https://www.iccrom.org/sites/default/files/2017-12/risk_manual_2016-eng.pdf.

ove metode omogućava sveobuhvatan pristup upravljanju rizicima i posebno je pogodna za očuvanje arhivskih i drugih kulturnih dobara.

Sigurnosni protokoli i zakonodavstvo

U praksi arhivske djelatnosti pojavili su se i slučajevi krađa arhivskog gradiva, koji su ukazali na potrebu za boljim sigurnosnim protokolima i tehničkim rješenjima za sprječavanje takvih incidenata.

Kazenski zakonik Republike Slovenije[30] u 259. članu Kaznenog zakonika Republike Slovenije propisane su kazne za kaznena djela povezana s arhivskim gradivom. Član navodi: „Tko protupravno otuđuje, uništava, prikriva arhivsko gradivo ili ga čini neupotrebljivim, kaznit će se zatvorom od tri mjeseca do tri godine." Ova legislativa naglašava ključnu ulogu zaštite arhivskog gradiva, ne samo kao pravnu odgovornost, već i kao bitan dio stručnog upravljanja arhivima.

Upravljanje rizicima na nivou informacijske infrastrukture

U arhivima je ključno uspostaviti sistem za proaktivno i reaktivno upravljanje potencijalnim opasnostima vezanim za dugoročno čuvanje digitalnog gradiva. To uključuje prepoznavanje, ocjenu i upravljanje rizicima koji mogu utjecati na očuvanje i dostupnost podataka. Važna su programska sredstva koja podržavaju ocjenjivanje i upravljanje rizicima u kontekstu dugoročne e-hrambe.[31] Uz pomoć ovih alata, arhivi mogu identificirati ranjivosti u svojim sistemima i uspostaviti zaštitne mjere kako bi spriječili gubitak podataka ili neovlašten pristup arhivskom gradivu.

Na primjeru slovenskih javnih arhiva može se primijetiti da prilikom digitalizacije arhivskih i drugih stručnih postupaka koriste vlastitu informacijsko-komunikacijsku infrastrukturu[32] i da su međusobno povezani[33], istovremeno, u nekim segmentima se oslanjaju na širu državnu infrastrukturu, koja je ključna za nesmetano funkcionisanje šire zajednice. Također, u pojedinim

[30] "Uradni list RS", št. 50/12 – službeni pročišćeni tekst, 54/15, 6/16 – popr, 38/16, 27/17, 23/20, 91/20, 95/21, 186/21, 105/22 – ZZNŠPP in 16/23.

[31] T. Hajtnik, Ocena in obvladovanje tveganj pri dolgoročni e-hrambi s pomočjo programskega orodja = Assessment and risk management at long-term preservation with the help of software tool. V: Gostenčnik, Nina (ur). *Uporabnikom prijazni arhivi: knjiga povzetkov: Mednarodna konferenca Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: 11-13. maj 2022*, Radenci, Slovenija, Pokrajinski arhiv Maribor 2022, 54.

[32] Tu spadaju lokalni fizički i virtualni serveri, radne stanice, štampači, skeneri, višenamjenski uređaji, WIFI pristupne tačke, aktivna i pasivna mrežna oprema poput prekidača, vatrozida, sigurnosnih i nadzornih podsistema itd.

[33] Kao primjer možemo navesti informacijski sistem Slovenske javne arhivske službe, koji se temelji na uzajamnoj bazi podataka SJAS i posebnoj sigurnoj komunikacijskoj infrastrukturi, koja omogućava čuvanje digitalnih oblika arhivskog gradiva te prikupljanje metapodataka o arhivskom gradivu, njihovu obradu i internu i eksternu upotrebu.

segmentima koriste i infrastrukturu i informacijska okruženja koja su važna za širu zajednicu[34] ili čak za državu[35]. Važno je naglasiti da je stepen integracije arhivskog sistema s drugim sistemima direktno povezan s većim zahtjevima za informatičku sigurnost. To je posebno vidljivo u posljednjih pet godina, kada su se na polju informatičke sigurnosti dogodile značajne promjene.

Prije uspostave zajedničke informacijske infrastrukture slovenskih javnih arhiva 2020. godine, svaki arhiv je samostalno brinuo o svojoj informatičkoj sigurnosti, ovisno o svojim tehničkim i finansijskim mogućnostima. Prije pet godina, arhivi su koristili standardne vatrozidove i imali su pojedinačne unutrašnje mreže s antivirusnim rješenjima na barem jednom serveru. „Usluge u oblaku" bile su ograničene na sigurnu pohranu datoteka, poput SCSI diskova, dodijeljenih pojedinim arhivima putem Slovenske akademske mreže (ARNES), ili kao dodatni diskovi u općim rješenjima kao što su Dropbox, Google Drive ili OneDrive. Sigurne veze izvan lokalnih mreža uspostavljene su u regionalnim arhivima još 2009. godine za uzajamnu platformu SIRAnet. Ona je 2016. godine, pod posebnim sigurnosnim uvjetima, postala dio mreže slovenske javne uprave (HKOM), što je omogućilo pristup zajedničkoj sigurnoj elektronskoj pohrani (Fedora Commons), smještenoj na informatičkoj infrastrukturi Arhiva RS. Politike lozinki su bile na relativno niskom nivou; na mnogim mjestima lozinke uopšte nisu bile potrebne za prijavu na lokalne računare ili pojedine aplikacije.

Elektronska pošta u slovenskim arhivima bila je uspostavljena na različite načine. Zaposleni su koristili poštanske sandučiće koji su im bili direktno dodijeljeni u okviru ARNES-a ili putem poštanskog sistema slovenske javne uprave HKOM, kao i preko vlastitih poštanskih servera koji su se povezivali s ARNES-om ili HKOM-om. Značajka svih ovih poštanskih sistema bila je da su arhivski stručnjaci svakodnevno primali veliki broj "spam" i "phishing" elektronskih poruka. Njihova velika količina zahtijevala je određeno vrijeme za pregledavanje i brisanje neželjene pošte, a istovremeno je omogućila zaposlenima da se upoznaju i s virusom tipa "locker", koji srećom tada još nije prouzročio veću štetu.

Uspostavom zajedničke metapodatkovne baze slovenskih javnih arhiva na infrastrukturi Arhiva RS 2021. godine, sigurnost arhivskih sistema postigla je

[34] Kao primjer možemo navesti da je pet slovenskih javnih arhiva uključeno u bibliotečki informacijski sistem Cobiss, u koji je uključeno 932 biblioteka i koji ima ukupno 7.325.000 zapisa u bazi. COBISS – *Kooperativni online bibliografski sistem in servisi*, 2024. Institut informacijskih znanosti, Maribor. Pridobljeno 17. 7. 2024 s spletne strani: https://www.cobiss.si/cobiss.htm.

[35] Kao primjer možemo navesti da su svi slovenski javni arhivi sigurno povezani u informacijski sistem Krpan. Sistem je namijenjen upravljanju dokumentarnim gradivom, smješten je na centralnoj informatičkoj infrastrukturi i koriste ga svi organi državne uprave, uključujući vladu, ministarstva, organe u sastavu, vladine službe, upravne jedinice i druge državne organe. *Prenova informacijskega sistema za podporo upravljanju z dokumentarnim gradivom – KRPAN*, 2023. Republika Slovenija, Ministrstvo za digitalno preobrazbo. Pridobljeno 17. 7. 2024 s spletne strani: https://www.gov.si/zbirke/projekti-in-programi/prenova-informacijskega-sistema-za-podporo-upravljanju-z-dokumentarnim-gradivom/.

novu razinu. Nove vatrozidne zaštite omogućile su bržu komunikaciju unutar standardizirane računalne mreže. Ubrzo nakon uspostavljanja nove komunikacijske platforme 2020. godine, u okviru projekta e-ARH.si izvršen je i prvi sveobuhvatni sigurnosni pregled komunikacijsko-informatičke infrastrukture.

Rezultati prvog sigurnosnog pregleda pokazali su brojne nedostatke, ne samo u operativnim sistemima i politikama lozinki, već i u općem razumijevanju informatičke sigurnosti među zaposlenima. Test s "phishing" porukom pokazao je da je veliki dio zaposlenih otvorio zlonamjernu poruku, što je ukazalo na potrebu za dodatnim obukama i podizanjem svijesti o sigurnosnim prijetnjama.

Na temelju tog pregleda, izvršena su brojna poboljšanja i otklonjene sigurnosne ranjivosti. Uvedene su sistematske nadogradnje operativnih sistema, uspostavljene su složenije politike lozinki koje se redovno mijenjaju, te su uvedene strože sigurnosne procedure za prijavu na radne stanice i aplikacije.

Krajem 2023. godine, Slovenska javna arhivska služba izvršila je drugi, složeniji sigurnosni pregled cjelokupne infrastrukture SJAS-a. Rezultati pregleda bili su lošiji nego što su odgovorni očekivali, jer su nakon prvog pregleda smatrali da neće biti većih iznenađenja na polju sigurnosti. Ispostavilo se da je zbog općeg razvoja informacijske tehnologije i lakše dostupnih sigurnosnih ranjivosti, stepen rizika u slovenskom uzajamnom arhivskom informacijskom sistemu znatno porastao. To povećava mogućnost provale te neželjenih ili čak zlonamjernih manipulacija podacima.

Ključni naglasci pregleda ukazali su na potrebu za:

- uvođenje dvostepene autentifikacije korisnika u arhivima,
- izvođenje segmentacije postojećih lokalnih računarskih mreža
- sveobuhvatnim ažuriranjima virtualizacionih platformi, lokalnih servera i radnih stanica,
- premještanje svih lokalnih web i poštanskih servera u sigurnija okruženja
- sveobuhvatnim ažuriranjima virtualizacionih platformi, lokalnih servera i radnih stanica,
- premještanje svih lokalnih web i poštanskih servera u sigurnija okruženja,
- vrlo opreznom rukovanju sa osjetljivim sigurnosnim podacima u elektronskom okruženju, jer postoji visok rizik od nenamjernog curenja podataka (tzv. "data leak").
- uspostavi sistema uzajamnog upravljanja utvrđenim rizicima, koji obuhvata hardversku, sistemsku, komunikacijsku i aplikativnu opremu..

Izvještaj drugog pregleda ipak je pokazao određeni napredak – broj zaposlenih koji su se upecali na 'phishing' poruke bio je znatno manji nego tokom prvog sigurnosnog pregleda.

S upravljačkog aspekta, pokazalo se da će biti potrebno svake godine planirati ulaganja značajnih finansijskih sredstava i ljudske resurse za osiguranje informacione sigurnosti. Namjenska finansijska sredstva prvenstveno će biti

usmjerena na ažuriranja hardverske i softverske opreme za zaštitu od novih sigurnosnih prijetnji, koje utiču kako na vlastiti sistem, tako i na sisteme sa kojima sarađuju. Ulaganje u ljudske resurse uključuje obrazovanje o informacijskoj sigurnosti i obuku zaposlenih za pravilno postupanje i reagovanje na sigurnosne prijetnje, što će smanjiti poznate i još nepoznate rizike.

Informacijski rizik: curenje i zloupotreba podataka

Arhivsko gradivo kao dio kulturne baštine načelno je dostupno javnosti bez većih ograničenja, Međutim, arhivski stručnjaci često se suočavaju s podacima koji su zbog zakonskih propisa privremeno zaštićeni i do kojih se može doći samo putem posebnog postupka. Ovi podaci, posebno lični podaci i zdravstvene informacije, zahtijevaju posebnu obradu i zaštitu, jer njihovo nepropisno rukovanje ili nenadzirano otkrivanje može imati ozbiljne posljedice.

I pored pažljivog rukovanja podacima, posebno u digitalnom obliku, u arhivima mogu se javiti tri glavne forme kršenja sigurnosti podataka: uništenje podataka, curenje podataka i kršenje povjerljivosti podataka.

Uništenje podataka

Uništenje podataka može se dogoditi zbog tehnoloških, sistemskih ili ljudskih grešaka; bilo namjerno ili nenamjerno. Bez obzira na uzrok, posljedica je gubitak podataka, što može dovesti do gubitka povjerenja u organizaciju i njen profesionalni integritet.

Curenje podataka

Iako je uništenje podataka često povezano s tehničkim kvarovima ili ljudskim greškama, curenje podataka obično se događa zbog nepažnje zaposlenih, koji često ne trebaju posebna tehnička znanja za iskorištavanje ranjivosti sistema. Curenje podataka definišemo kao neovlašteni prenos podataka iz organizacije ka neovlaštenim osobama ili spoljnim primaocima.[36] Do curenja podataka obično dolazi zbog nesretnih okolnosti, bilo tokom njihovog prenosa[37],

[36] *What is Data Leakage*?, 2024. Forcepoint. Pridobljeno 17. 7. 2024 s spletne strani: https://www.forcepoint.com/cyber-edu/data-leakage.

[37] Npr. kada su poslani putem e-pošte, API poziva, chatova i drugih komunikacija.

mirovanjem[38] ili upotrebom[39] i to bez obzira na to da li su u fizičkom, elektronskom ili hibridnom obliku.[40]

Kršenje povjerljivosti podataka

U praksi je kršenje povjerljivosti podataka često rezultat pokušaja spoljnih upada, koji koriste ranjivosti hardverske, softverske ili sigurnosne infrastrukture, kao i nepredviđenih rizika. Napadači identifikuju te ranjivosti i koriste ih za izmjenu, brisanje ili krađu podataka.

Curenje podataka i kršenje povjerljivosti podataka su, iako različiti pojmovi, usko povezani. Curenje podataka omogućava njihovu zloupotrebu, što može dovesti do kršenja njihove povjerljivosti.

Informacijski rizici: IOT (Internet stvari)

Internet stvari (IoT) predstavlja mrežu povezanih uređaja koji omogućavaju međusobnu komunikaciju i razmjenu podataka putem interneta. Iako IoT donosi brojne prednosti, kao što su automatizacija procesa, efikasno prikupljanje podataka i optimizacija radnih tokova, s njim su također povezani značajni sigurnosni rizici, uključujući i u kontekstu arhivske djelatnosti. Zbog slabe sigurnosne infrastrukture, IoT uređaji često su izloženi kibernetskim napadima, što može dovesti do curenja osjetljivih podataka, neovlaštenog pristupa arhivskim sistemima, pa čak i do manipulacije podacima.

U arhivima se IoT uređaji često koriste za praćenje okolišnih uslova, kao što su temperatura, vlažnost i osvjetljenje, koji utiču na dugoročno očuvanje fizičkog arhivskog materijala. Ako napadači dobiju pristup tim uređajima, to može dovesti do nepravilnog upravljanja okolišnim parametrima, što može ozbiljno ugroziti sigurnost i cjelovitost arhivskog materijala. Osim toga, napadači mogu dobiti pristup osjetljivim informacijama putem IoT uređaja, što dodatno povećava rizik od gubitka ili krađe podataka.

Kako bi smanjili rizike povezane s IoT-om, arhivi moraju uspostaviti sveobuhvatne sigurnosne mjere, koje uključuju enkripciju komunikacijskih puteva između uređaja, redovne nadogradnje softvera i hardvera IoT uređaja, kao i korištenje sigurnosnih rješenja, poput vatrozida i segmentacije mreže za zaštitu

[38] Podaci mogu biti izloženi u mirovanju zbog pogrešne konfiguracije cloud usluga, neispravnog rada baza podataka, nepravilnih postavki ili nenadgledanih promjena statusa zapisa, kao i zbog izgubljenih ili neadekvatno zaštićenih uređaja koji sadrže te podatke.

[39] Podaci mogu biti izloženi tokom korištenja, npr. prilikom štampanja na zajedničkim štampačima, pravljenja i objavljivanja snimaka ekrana koji sadrže osjetljive informacije, ili zbog nenadgledanog čuvanja na javno dostupnim skladištima ili prenosnim USB uređajima.

[40] *Data Leakage: Common Causes, Examples & Tips for Prevention*, 2024. BlueVayant. Pridobljeno 17. 7. 2024 s spletne strani: https://www.bluevoyant.com/knowledge-center/data-leakage-common-causes-examples-tips-for-prevention.

IoT sistema. Također, ključno je uspostaviti redovno nadgledanje i praćenje rada uređaja, čime se osigurava brzo otkrivanje mogućih anomalija ili kibernetskih prijetnji. Obuka zaposlenih o potencijalnim rizicima koje IoT donosi također je bitna za uspostavljanje efikasne sigurnosne kulture.

U kontekstu arhivske djelatnosti, pouzdana upotreba IoT tehnologija ključna je za zaštitu arhivskog materijala, kako fizičkog, tako i elektronskog. Implementacija robusnih sigurnosnih mjera i kontinuirano nadgledanje IoT uređaja omogućit će arhivima da iskoriste prednosti ovih tehnologija, dok istovremeno smanjuju informacijske rizike.

Informacijski rizici: Zaključavanje datoteka (Ransomware)

Zaključavanje datoteka, bolje poznato kao napad sa zlonamjernim softverom (ransomware), predstavlja jedan od najserioznijih sigurnosnih izazova s kojima se suočavaju organizacije, a arhivi nisu izuzetak. U ovom tipu napada, zlonamjerni softver šifrira datoteke i podatke u sistemu, a napadači traže otkupninu u zamjenu za ključ za dešifriranje podataka. Iako su takvi napadi često motivisani željom za finansijskom dobiti, u arhivskom okruženju mogu izazvati još ozbiljnije posljedice, poput nepovratnog gubitka ili onemogućenog pristupa dragocjenom arhivskom materijalu.

Kako bi smanjili rizik od ovakvih napada, arhivi moraju uspostaviti sveobuhvatan sistem zaštite koji uključuje najmanje:

- *Redovno pravljenje sigurnosnih kopija podataka:* Sigurnosne kopije podataka moraju biti pohranjene na više odvojenih, sigurnih lokacija[41], koje nisu direktno povezane s mrežom, čime se smanjuje mogućnost infekcije zlonamjernim softverom.
- *Korištenje napredne antivirusne zaštite:* Osnovno sredstvo odbrane predstavljaju redovno ažurirani antivirusni programi koji u realnom vremenu otkrivaju i štite od ransomware napada.
- *Redovne nadogradnje sistema i softvera:* Rednim instaliranjem sigurnosnih ažuriranja za operativne sisteme i aplikacije smanjuju se sigurnosne ranjivosti koje napadači mogu iskoristiti.
- *Obuka zaposlenih:* Zaposleni su prva linija odbrane protiv kibernetskih napada, stoga je važno da budu obučeni za prepoznavanje sumnjivih poruka, phishing napada i opasnih priloga.
- *Razvoj plana za odgovor na incidente:* Ključan za smanjenje uticaja potencijalnog napada je plan za upravljanje incidentima, koji uključuje

[41] S PETZ (51. član) je određeno da moraju javnopravne osobe, uključujući arhive i pružatelje usluga e-hranjenja koji čuvaju javno arhivsko gradivo u digitalnom obliku, osigurati pohranu sigurnosnih kopija potrebnih za obnovu sistema e-hranjenja na najmanje dva geografski udaljena mesta. Ta mesta ne smeju biti u istom području pogođenom poplavama ili zemljotresima, kao ni u istom području kao glavno mesto čuvanja.

mjere za brzu obnovu podataka, smanjenje štete i upravljanje posljedicama.

Arhivi moraju, zbog osjetljivosti svog gradiva, razviti proaktivne strategije za upravljanje rizicima povezanim s ransomware napadima, jer se u ovim slučajevima radi o više od samo finansijskog gubitka – radi se o zaštiti historijskih i kulturnih resursa koji su ključni za društveno pamćenje.

Informacijski rizici: Korištenje rješenja iz oblasti umjetne inteligencije (UI)

Umjetna inteligencija (UI) postaje ključni dio arhivske stručne djelatnosti, jer omogućava automatizaciju brojnih procesa, poput razvrstavanja dokumenata, digitalizacije, prepoznavanja teksta i analize velikih količina podataka. U vrednovanju i odabiru elektronskog gradiva, tehnologija može značajno povećati efikasnost ovih procesa. Neke tehnološke solucije već su u upotrebi za selekciju i vrednovanje arhivskog gradiva, što omogućava preciznije i brže donošenje odluka o tome koje gradivo zadržati, a koje izbaciti. Ove solucije se temelje na algoritmima i UI, koji poboljšavaju tačnost odluka i smanjuju rizike povezane sa ručnom obradom velikih količina podataka.[42]

Iako UI donosi brojne prednosti, kao što su veća efikasnost i tačnost, takođe sa sobom nosi određene informacione rizike koje arhivi ne smiju zanemariti. To potvrđuje i pregled upotrebe UI u e-arhivskom gradivu, predstavljen na 3. međunarodnoj konferenciji e-ARH.si, gdje su istaknute mogućnosti koje tehnologija UI donosi za unapređenje upravljanja arhivskim gradivom.[43] Upotrebom UI poboljšava se efikasnost obrade elektronskog arhivskog gradiva, što otvara pitanja o rizicima nepravilne obrade i interpretacije podataka.

Prvi izazov pri korištenju UI-a je rizik od nepravilne obrade ili interpretacije podataka. Greške u algoritmima ili nepotpuni ulazni podaci mogu dovesti do pogrešnih rezultata, kao što su greške u arhivskoj bazi podataka, gubitak važnih informacija ili čak trajne promjene u arhivskom materijalu, što može negativno utjecati na njegovu cjelovitost i dostupnost

Drugi izazov predstavlja ranjivost UI sistema na kibernetičke napade. Napadači mogu manipulirati algoritmima, unositi pristrasne podatke (tzv. "zagađenje podataka") ili izvoditi napade čiji je cilj iskriviti rezultate UI rješenja,

[42] T. Hajtnik, A. Škoro Babić, Ali nam lahko pri vrednotenju in odbiranju elektronskega gradiva pomaga tehnologija?. *Moderna arhivistika: časopis arhivske teorije in prakse*. [Spletna izd]. 2018, letn. 1, št. 1, 169-196. Pridobljeno 17. 10. 2024 s spletne strani: http://www.pokarh-mb.si/uploaded/datoteke/radenci_20181/1_2018_169-196_%C5%A0koro.pdf.

[43] A. Bole, T. Hajtnik, A. Škoro Babić, *Splošni pregled uporabe umetne inteligence pri obravnavanju e-arhivskega gradiva: predstavitev kompetenčnega centra 2*: predavanje na 3. mednarodni konferenci e-ARH.si, Ljubljana, 7-8. november 2018. [COBISS.SI-ID 2079093].

što može dovesti do pogrešnih zaključaka i odluka.[44] Ovo može biti opasno i u arhivima, gdje su podaci često osjetljivi i nenadoknadivi.

Važan izazov pri korištenju umjetne inteligencije (UI) u arhivima predstavlja rizik od falsifikovanja arhivskog materijala već u fazi njegovog nastanka kod stvaralaca, tzv. "lažni" dokumenti. Napredak digitalnih tehnologija omogućio je lakše stvaranje falsifikovanih dokumenata. Ovi dokumenti mogu sadržavati lažne ili manipulirane podatke koji izgledaju autentično, ali su stvoreni s ciljem obmanjivanja. Takvi dokumenti mogu zamijeniti autentične zapise, što ima ozbiljne posljedice za historijski integritet, pravne procese i čak političke odluke. Rizik je posebno izražen kod digitalizovanog materijala, gdje su mogućnosti za falsifikovanje veće zbog dostupnosti i fleksibilnosti digitalnih alata.

Historijski primjer koji dobro ilustrira ovo rizik su falsifikovani Hitlerovi dnevnici, koje je 1983. godine objavila njemačka revija Stern. Iako su prvobitno smatrani vjerodostojnim, kasnije analize su otkrile da se radi o falsifikovanom materijalu, što je izazvalo jedan od najvećih skandala u istoriji medija.[45] Ovaj događaj upozorava na važnost precizne provjere autentičnosti materijala prije nego što postane javno dostupan.

Trenutno nije poznato da su zapisi stvoreni umjetnom inteligencijom (UI) službeno uključeni u arhivske sisteme. Ipak, postoje zabrinutosti oko sintetičkih medija, kao što su tekstovi koje generira UI i deepfake videozapisi. Sve veća upotreba UI za stvaranje uvjerljivo falsifikovanog sadržaja predstavljaće ogroman izazov za arhiviste u očuvanju vjerodostojnosti digitalnih zapisa. Ovaj trend postavlja važna pitanja o integritetu digitalnih zapisa, posebno s obzirom na to da su alati UI sposobni stvoriti veoma realistične, ali lažne medije, koji bi mogli biti pogrešno prepoznati kao autentični. O tome se diskutovalo i na skupu Arhivskog društva Slovenije, gdje je naglašena važnost zaštite materijala, posebno u vezi sa upotrebom UI za provjeru autentičnosti arhivskih zapisa i digitalnih dokumenata.[46]

Ovi primjeri naglašavaju potrebu da arhivi uspostave robusne metode provjere kako bi osigurali da se sadržaj generiran umjetnom inteligencijom pravilno identifikuje prije nego što ga preuzmu od stvaralaca, čime se ne ugrožava vjerodostojnost arhivskih zapisa.

---

[44] F. Marulli, S. Marrone, L. Verde, Sensitivity of Machine Learning Approaches to Fake and Untrusted Data in Healthcare Domain. *Journal of Actuator Networks*, 2022. Pridobljeno 15. 10. 2024 s spletne strani: https://www.mdpi.com/2224-2708/11/2/21.

[45] ABC News, 2023. Fake Hitler diaries published by Stern in 1983: *The media scandal that rocked Europe*. ABC News. https://www.abc.net.au/news/2023-05-26/fake-hitler-diaries-published-by-stern-in-1983-media-scandal/102367442.

[46] M. Grobelnik, T. Hajtnik, M. Novak, Š. Robnik, Z. Semlič Rajh, *Umetna inteligenca in možnosti vpeljave novih digitalnih procesov v arhive, prenos dobrih praks iz sorodnih institucij, strokovna terminologija s področja digitalizacije in druga odprta vprašanja*: okrogla miza in delavnica na 31. zborovanju Arhivskega društva Slovenije: Bohinjska Bistrica, 5-6. 10. 2023.

U tom smislu, mogu se poslužiti različitim pristupima, kao što su:

- Uspostavljanje preciznih i strogih postupaka provjere izvora arhivskog materijala; provjera autentičnosti izvora će i dalje zahtijevati blisku saradnju sa stvaraocima materijala.
- Postavljanje jasnih zahtjeva za stvaraoce arhivskog materijala u vezi s metapodacima koji prate arhivski materijal prilikom predaje, uključujući zahtjev za određenim podacima kao što su datum nastanka, autorstvo, kontekst stvaranja i zapisi o mogućim promjenama ili prijenosima.
- Uspostavljanje saradnje s vanjskim institucijama i stručnjacima, kao što su digitalni forenzički stručnjaci ili organizacije za provjeru autentičnosti. Ove institucije mogu pregledati i analizirati digitalni materijal, provjeravajući njegovu integritet i potvrđujući vjerodostojnost prije preuzimanja u arhiv. Forenzička analiza može uključivati provjeru metapodataka, datotečnih sistema i drugih tehničkih aspekata koji mogu otkriti eventualne manipulacije ili falsifikate materijala.
- Ključna će postati i implementacija tehnoloških rješenja, odnosno specijalizovanih algoritama za otkrivanje falsifikata, koji omogućavaju provjeru vjerodostojnosti digitalnih zapisa. Na primjer, alat Microsoft Video Authenticator dizajniran je za otkrivanje manipulacija u slikama i videozapisima, uključujući falsifikovane materijale stvorene pomoću UI. Također, DeepFake Detection Challenge (DFDC), koji razvija Facebook u saradnji s više istraživačkih institucija, nudi napredna rješenja za otkrivanje lažnih videozapisa. Alati poput Forensic Image Analyzer za analizu slika, Deepware Scanner za otkrivanje deepfake videozapisa, te GPT-2 Output Detector za identifikaciju lažnih tekstova koje generiraju modeli UI, postali su ključni za otkrivanje manipulacija u slikama, videozapisima, tekstovima ili zvučnim snimcima. Korištenje takvih i sličnih alata omogućit će arhivima da smanje rizik od preuzimanja falsifikovanih dokumenata i osiguraju viši nivo vjerodostojnosti digitalnih zapisa.
- I pored tehnoloških rješenja, i dalje će biti korisno i važno da arhivisti provode i „ručne" preglede materijala. Na primjer, ako prepoznaju nesuglasja u stilovima, formatu, kontekstu ili drugim karakteristikama materijala, to bi moglo značiti da materijal možda nije autentičan i vjerodostojan. Stoga će stručna procjena arhivista, koji su obučeni za prepoznavanje potencijalno falsifikovanog materijala, i dalje biti ključna.
- Arhivi će morati u programe obuke koje organizuju za stvaraoce arhivskog materijala uključiti i rizike povezane s upotrebom UI.

Sprovodeći ove mjere i pristupe, arhivi će moći smanjiti rizik od preuzimanja falsifikovanog materijala, čak i ako nemaju neposrednu kontrolu nad njegovim stvaranjem.

Zaključak

Članak ističe ključne izazove s kojima se arhivi suočavaju u dobi digitalizacije, koji će ostati aktuelni i u budućnosti. Informacijska sigurnost naglašena je kao temeljni stub zaštite arhivskog gradiva, posebno zbog ranjivosti koje donose nove tehnologije, poput veštačke inteligencije, interneta stvari i oblaka. Arhivi moraju uspostaviti višeslojne sigurnosne mere za zaštitu gradiva od različitih prijetnji, kao što su napadi zlonamjernim softverom (ransomware), curenje podataka i falsifikovanje dokumenata.

Hajtnik[47] upozorava na usku povezanost između informacijske sigurnosti i dugoročne pohrane elektronskih zapisa, što naglašava nužnost sveobuhvatnih sigurnosnih mera za zaštitu arhivskog gradiva. Članak takođe ističe važnost bliske saradnje između arhiva i stvaralaca gradiva, s obzirom na to da arhivi često nemaju potpunu kontrolu nad izvorom gradiva, što stvara rizik od pojave „lažnog" arhivskog gradiva. Uvođenje strogih sigurnosnih politika, usklađenih sa međunarodnim standardima (npr. porodica standarda ISO 27000), redovno provjeravanje sigurnosnih sistema i korišćenje specijalizovanih tehnologija za otkrivanje falsifikata ključni su koraci za obezbeđivanje sigurnosti.

Hajtnik[48] ističe da će uspostavljanje pouzdane e-repozitorije biti ključno za dugoročno čuvanje i dostupnost arhivskih zapisa, što dodatno potvrđuje značaj sveobuhvatnih sigurnosnih politika u digitalnom okruženju. Usklađenost sa standardom ISO 16363 omogućava uspostavljanje povjerljivih sistema za dugoročnu elektronsku pohranu, što je suštinski važno za budućnost arhivske prakse u digitalnom svijetu.[49] I pored tehnoloških rješenja, ljudska procjena arhivista ostaje od izuzetne važnosti za obezbjeđivanje cjelovitosti i vjerodostojnosti arhivskog gradiva.

---

[47] T. Hajtnik, Kako sta povezani informacijska varnost in dolgoročna hramba zapisov v digitalni obliki. V: Gostenčnik, Nina (ur). *Arhivi v primežu narave in tehnologije: knjiga povzetkov: Mednarodna konferenca Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja*: 15.-17. maj 2024, Radenci, Slovenija, 70-71. Maribor: Pokrajinski arhiv.

[48] T. Hajtnik, E-repozitorij: kdaj bo zaupanja vreden sistem dolgoročne e-hrambe = Digital repository: when will be a trustworthy [system] for long term digital preservation: predavanje na 7. znanstveni konferenci z mednarodno udeležbo "Za človeka gre: prihodnost zdaj!", Alma Mater Europae, Maribor, 16. 3. 2019.

[49] T. Hajtnik, Skladnost s standardom ISO 16363 - je to odgovor za našo digitalno prihodnost? = ISO 16363 compliance - is this the answer for our digital future?. V: Semlič Rajh, Zdenka (ur). *Arhivi v službi človeka - človek v službi arhivov: relevance v raziskavah arhivske znanosti = Archives in the Service of People - People in the Service of Archives: Relevance in the Research of Archival Science:* 8. znanstvena konferenca z mednarodno udeležbo Za človeka gre: relevanca znanosti in izobraževanja = 8th Scientific Conference with International Participaton All About People: Relevance of Science and Education: 5. znanstveno raziskovalni, študijski in izobraževalni simpozij = 5th Scientific Research, Study and Educational Symposium: zbornik recenziranih prispevkov = peer-rewieved proceedings book: Maribor, 14. 3. 2020, 72-81. Maribor: AMEU - ECM, Alma Mater Press. Pridobljeno 17. 10. 2024 s spletne strani: http://press.almamater.si/index.php/amp/catalog/book/22 .

Digitalna transformacija arhivske djelatnosti uz pomoć riješenja poput sistema e-ARH.si omogućava efikasnije povezivanje stvaralaca, arhiva i korisnika, čime se poboljšava arhiviranje i dostupnost gradiva.[50] Sve to dodatno naglašava potrebu za uspostavljanjem robusnih sistema za dugoročnu zaštitu digitalnog arhivskog gradiva.

Analiza primjera iz slovenske arhivske prakse u članku takođe ukazuje na potrebu za stalnim obrazovanjem arhivista i bliskom saradnjom sa spoljnim stručnjacima i institucijama, što će biti ključno za dugoročnu sigurnost i trajnost arhivskog gradiva.

Summary

The article highlights the key challenges faced by archives in the age of digitization, which will remain relevant in the future. Information security is emphasized as a fundamental pillar of archival material protection, especially due to the vulnerabilities brought about by new technologies such as artificial intelligence, the Internet of Things, and cloud computing. Archives must establish multilayered security measures to protect materials from various threats, such as malware attacks (ransomware), data breaches, and document forgery.

Heitnik warns about the close relationship between information security and the long-term preservation of electronic records, underlining the necessity for comprehensive security measures to protect archival materials. The article also highlights the importance of close collaboration between archives and record creators, as archives often lack complete control over the source of materials, creating a risk of "fake" archival records. The introduction of strict security policies, aligned with international standards (e.g, the ISO 27000 family of standards), regular security system checks, and the use of specialized technologies to detect forgeries are key steps in ensuring security.

Heitnik emphasizes that establishing reliable e-repositories will be crucial for the long-term preservation and accessibility of archival records, further reinforcing the importance of comprehensive security policies in the digital environment. Compliance with the ISO 16363 standard enables the establishment of trusted systems for long-term electronic storage, which is essential for the future of archival practice in the digital world. Despite technological solutions, human assessment by archivists remains of paramount importance in ensuring the integrity and authenticity of archival materials.

The digital transformation of archival activities, with solutions such as the e-ARH.si system, enables more efficient connection between record creators, archives, and users, thereby improving the archiving process and material

[50] T. Hajtnik, *Upravljanje s tveganji pri dolgoročni e-hrambi: rešitve za ustvarjalce*: spletno predavanje na 5. konferenci e-ARH.si, 17-18. 11. 2021.

accessibility. All of this further emphasizes the need for establishing robust systems for the long-term protection of digital archival materials.

The analysis of examples from Slovenian archival practice in the article also points to the need for continuous education of archivists and close cooperation with external experts and institutions, which will be crucial for the long-term security and sustainability of archival materials.

BIBLIOGRAFIJA/BIBLIOGRAPHY

1. ABC News. (2023). *Fake Hitler diaries published by Stern in 1983: The media scandal that rocked Europe*. ABC News. https://www.abc.net.au/news/2023-05-26/fake-hitler-diaries-published-by-stern-in-1983-media-scandal/102367442.
2. Bole A, Hajtnik T, Škoro Babić A, *Splošni pregled uporabe umetne inteligence pri obravnavanju e-arhivskega gradiva: predstavitev kompetenčnega centra 2*: predavanje na 3. mednarodni konferenci e-ARH.si, Ljubljana, 7-8. november 2018. [COBISS.SI-ID 2079093].
3. COBISS – *Kooperativni online bibliografski sistem in servisi*, 2024. Institut informacijskih znanosti, Maribor. Pridobljeno 17. 7. 2024 s spletne strani: https://www.cobiss.si/cobiss.htm.
4. *Data Leakage: Common Causes, Examples & Tips for Prevention*, 2024. BlueVayant. Pridobljeno 17. 7. 2024 s spletne strani: https://www.bluevoyant.com/knowledge-center/data-leakage-common-causes-examples-tips-for-prevention.
5. Edwards M, The Ultimate Guide to ISO 27001. ISMS.online. Pridobljeno 17. 7. 2024 s spletne strani: https://www.isms.online/iso-27001/#iso-270012013-iso-270012022-whats-the-difference.
6. Gartner Glossary (n.d). Gartner. Pridobljeno 1. 7. 2024 s spletne strani: https://www.gartner.com/en/glossary .
7. Grobelnik M, Hajtnik T, Novak M, Robnik Š, Semlič Rajh Z, *Umetna inteligenca in možnosti vpeljave novih digitalnih procesov v arhive, prenos dobrih praks iz sorodnih institucij, strokovna terminologija s področja digitalizacije in druga odprta vprašanja*: okrogla miza in delavnica na 31. zborovanju Arhivskega društva Slovenije: Bohinjska Bistrica, 5-6. 10. 2023.
8. Hajtnik T, *Elektronsko arhiviranje: ISO standardi kot odgovor na zakonska določila*: predavanje na 3. mednarodni konferenci e-ARH.si, Ljubljana, 7.-8. november 2018.
9. Hajtnik T, Skladnost s standardom ISO 16363 - je to odgovor za našo digitalno prihodnost? = ISO 16363 compliance - is this the answer for our digital future?. V: Semlič Rajh, Zdenka (ur). *Arhivi v službi človeka - človek v službi arhivov: relevance v raziskavah arhivske znanosti = Archives in the Service of People - People in the Service of Archives: Relevance in the Research of Archival Science*: 8. znanstvena konferenca z mednarodno udeležbo Za človeka gre: relevanca znanosti in izobraževanja = 8th Scientific Conference with International Participaton All About People: Relevance of Science and Education: 5. znanstveno raziskovalni, študijski in izobraževalni simpozij = 5th Scientific Research, Study and Educational Symposium: zbornik recenziranih prispevkov = peer-rewieved proceedings book : Maribor, 14. 3. 2020, 72-81. Maribor: AMEU - ECM, Alma Mater Press. Pridobljeno 17. 10. 2024 s spletne strani: http://press.almamater.si/index.php/amp/catalog/book/22 .
10. Hajtnik T, *Ocena in obvladovanje tveganj pri dolgoročni e-hrambi s pomočjo programskega orodja = Assessment and risk management at long-term preservation with the help of software tool*. V: Gostenčnik, Nina (ur). Uporabnikom prijazni arhivi: knjiga povzetkov: Mednarodna konferenca Tehnični in vsebinski problemi klasičnega in

elektronskega arhiviranja: 11-13. maj 2022, Radenci, Slovenija, 54. Maribor: Pokrajinski arhiv.
11. Hajtnik T, *Usmeritve in zahteve za varno hrambo elektronskih dokumentov skladno s predpisi:* predavanje na posvetovanju 2. Ravnateljev zajtrk na temo Kako pravilno voditi in hraniti dokumente: Ljubljana, 15. november 2023.
12. Hajtnik T, *Kako sta povezani informacijska varnost in dolgoročna hramba zapisov v digitalni obliki*. V: Gostenčnik, Nina (ur). Arhivi v primežu narave in tehnologije: knjiga povzetkov: Mednarodna konferenca Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: 15-17. maj 2024, Radenci, Slovenija, 70-71. Maribor: Pokrajinski arhiv.
13. Hajtnik T, *E-repozitorij : kdaj bo zaupanja vreden sistem dolgoročne e-hrambe = Digital repository: when will be a trustworthy [system] for long term digital preservation:* predavanje na 7. znanstveni konferenci z mednarodno udeležbo "Za človeka gre: prihodnost zdaj!", Alma Mater Europae, Maribor, 16. 3. 2019.
14. Hajtnik T, *Upravljanje s tveganji pri dolgoročni e-hrambi: rešitve za ustvarjalce*: spletno predavanje na 5. konferenci e-ARH.si, 17-18. 11. 2021.
15. Hajtnik T, Škoro Babić A, Ali nam lahko pri vrednotenju in odbiranju elektronskega gradiva pomaga tehnologija?. *Moderna arhivistika: časopis arhivske teorije in prakse*. [Spletna izd]. 2018, letn. 1, št. 1, 169-196. Pridobljeno 17. 10. 2024 s spletne strani: http://www.pokarh-mb.si/uploaded/datoteke/radenci_20181/1_2018_169-196_%C5%A0koro.pdf.
16. *Informacijska varnost*, 2024. Pridobljeno 1. 7. 2024 s spletne strani: https://www.gov.si/teme/informacijska-varnost/.
17. *Information Security* (InfoSec) defined. (N.d). Microsoft. Pridobljeno 14. 7. 2024 s spletne strani: https://www.microsoft.com/en-au/security/business/security-101/what-is-information-security-infosec.
18. *Information security*. (n.d) Dictionary of Military and Associated Terms. (2005). Pridobljeno 17. 7. 2024 s spletne strani: https://www.thefreedictionary.com/information+security.
19. ISO 19011:2018(en) - Guidelines for auditing management systems. Pridobljeno 22. 7. 2024 s spletne strani: https://www.iso.org/standard/70017.html.
20. ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements. Pridobljeno 22. 7. 2024 s spletne strani: https://www.iso.org/standard/75106.html.
21. ISO 22313:2020 - Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301. Pridobljeno 22. 7. 2024 s spletne strani: https://www.iso.org/standard/75107.html .
22. ISO 27799:2016. Health informatics — Information security management in health using ISO/IEC 27002. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/62777.html.
23. ISO 31000:2018 - Risk management. Guidelines. Pridobljeno 1. 7. 2024 s spletne strani: https://www.iso.org/standard/65694.html.
24. ISO 31073:2022. Risk management — Vocabulary. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/79637.html.
25. ISO/IEC 20000-1:2018. Information technology — Service management. Part 1: Service management system requirements. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/70636.html.
26. ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Pridobljeno 22. 7. 2024 s spletne strani: https://www.iso.org/standard/27001.
27. ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection Information security controls. Pridobljeno 1. 7. 2024 s spletne strani: https://www.iso.org/standard/75652.html.

28. ISO/IEC 27003:2017 - Information technology — Security techniques — Information security management systems — Guidance. Pridobljeno 17. 7. 2024 s spletne strani: https://www.iso.org/standard/63417.html.
29. ISO/IEC 27004:2016 - Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation. Pridobljeno 22. 7. 2024 s spletne strani: https://www.iso.org/standard/64120.html.
30. ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Pridobljeno 22. 7. 2024 s spletne strani: https://www.iso.org/standard/80585.html.
31. ISO/IEC 27006-1:2024 - Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems. Part 1: General. Pridobljeno 22. 7. 2024 s spletne strani: https://www.iso.org/standard/82908.html.
32. ISO/IEC 27007:2020 - Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing. Pridobljeno 22. 7. 2024 s spletne strani: https://www.iso.org/standard/77802.html.
33. ISO/IEC 27017:2015. Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/43757.html.
34. ISO/IEC 27018:2019. Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/76559.html.
35. ISO/IEC 27031:2011. Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/44374.html.
36. ISO/IEC 27032:2023. Cybersecurity — Guidelines for Internet security. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/76070.html.
37. ISO/IEC 27033-1:2015 Information technology — Security techniques — Network security. Part 1: Overview and concepts. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/63461.html.
38. ISO/IEC 27033-2:2012. Information technology — Security techniques — Network security. Part 2: Guidelines for the design and implementation of network security. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/51581.html.
39. ISO/IEC 27033-3:2010. Information technology — Security techniques — Network security. Part 3: Reference networking scenarios — Threats, design techniques and control issues. Pridobljeno 25. 7. 2024 s spletne strani: https://www.iso.org/standard/51582.html.
40. ISO/IEC 27033-3:2010. Information technology — Security techniques — Network security. Part 3: Reference networking scenarios — Threats, design techniques and control issues. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/51582.html.
41. ISO/IEC 27033-4:2014. Information technology — Security techniques — Network security. Part 4: Securing communications between networks using security gateways. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/51583.html.
42. ISO/IEC 27033-5:2013. Information technology — Security techniques — Network security. Part 5: Securing communications across networks using Virtual Private Networks (VPNs). Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/51584.html.
43. ISO/IEC 27033-6:2016. Information technology — Security techniques — Network security. Part 6: Securing wireless IP network access. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/51585.html.

44. ISO/IEC 27033-7:2023. Information technology – Network security. Part 7: Guidelines for network virtualization security. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/80972.html.
45. ISO/IEC 27035-1:2023. Information technology — Information security incident management. Part 1: Principles and process. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/78973.html.
46. ISO/IEC 27035-2:2023. Information technology — Information security incident management. Part 2: Guidelines to plan and prepare for incident response. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/78974.html.
47. ISO/IEC 27035-3:2020. Information technology — Information security incident management. Part 3: Guidelines for ICT incident response operations. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/74033.html.
48. ISO/IEC 27036-1:2021. Cybersecurity — Supplier relationships. Part 1: Overview and concepts. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/82905.html.
49. ISO/IEC 27036-2:2022. Cybersecurity — Supplier relationships. Part 2: Requirements. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/82060.html.
50. ISO/IEC 27036-3:2023. Cybersecurity — Supplier relationships. Part 3: Guidelines for hardware, software, and services supply chain security. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/82890.html.
51. ISO/IEC 27036-4:2016. Information technology — Security techniques — Information security for supplier relationships Part 4: Guidelines for security of cloud services. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/59689.html.
52. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/44381.html.
53. ISO/IEC 27039:2015 - Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems. Pridobljeno 22. 7. 2024 s spletne strani: https://www.iso.org/standard/56889.html.
54. ISO/IEC 27040:2024. Information technology — Security techniques — Storage security. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/80194.html.
55. ISO/IEC 27701:2019. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Pridobljeno 24. 7. 2024 s spletne strani: https://www.iso.org/standard/71670.html.
56. ISO/IEC TS 27006-2:2021 - Requirements for bodies providing audit and certification of information security management systems. Part 2: Privacy information management systems. Pridobljeno 22. 7. 2024 s spletne strani: https://www.iso.org/standard/71676.html.
57. ISO/IEC TS 27008:2019 - Information technology — Security techniques — Guidelines for the assessment of information security controls. Pridobljeno 22. 7. 2024 s spletne strani: https://www.iso.org/standard/67397.html.
58. KZ-1. *Kazenski zakonik*. (2023). "Uradni list RS", št. 50/12 – uradno prečiščeno besedilo, 54/15, 6/16 – popr., 38/16, 27/17, 23/20, 91/20, 95/21, 186/21, 105/22 – ZZNŠPP in 16/23. Pridobljeno 1. 7. 2024 s spletne strani: https://pisrs.si/pregledPredpisa?id=ZAKO5050.
59. Marulli F, Marrone S, Verde L, Sensitivity of Machine Learning Approaches to Fake and Untrusted Data in Healthcare Domain. *Journal of Actuator Networks*, 2022. Pridobljeno 15. 10. 2024 s spletne strani: https://www.mdpi.com/2224-2708/11/2/21.
60. Michalski S, Pedersoli J. L, *The ABC Method: A risk management approach to the preservation of cultural heritage*. 163 strani. Canadian Conservation Institute. Ottawa 2016. Pridobljeno 1. 7. 2024 s spletne strani: https://www.iccrom.org/sites/default/files/2017-12/risk_manual_2016-eng.pdf.

61. M. Novak, Stanje in perspektive vzajemnega metapodatkovnega korpusa slovenske javne arhivske službe. *Moderna arhivistika* 2023, 6 (2), 308–333. Maribor: Pokrajinski arhiv Maribor. Pridobljeno 1. 7. 2024 s spletne strani: https://doi.org/10.54356/MA/2023/MJUO4040.
62. PETZ. *Pravilnik o enotnih tehnoloških zahtevah za zajem in hrambo gradiva v digitalni obliki*, 2020, "Uradni list RS", št. 118/20. Pridobljeno 1. 7. 2024 s spletne strani: https://pisrs.si/pregledPredpisa?id=PRAV12755.
63. *Prenova informacijskega sistema za podporo upravljanju z dokumentarnim gradivom – KRPAN*, 2023. Republika Slovenija, Ministrstvo za digitalno preobrazbo. Pridobljeno 17. 7. 2024 s spletne strani: https://www.gov.si/zbirke/projekti-in-programi/prenova-informacijskega-sistema-za-podporo-upravljanju-z-dokumentarnim-gradivom/.
64. PSUDDG. *Pravilnik o strokovni usposobljenosti za delo z dokumentarnim gradivom, 2025*. "Uradni list RS", št. 66/16. Pridobljeno 1. 7. 2024 s spletne strani: https://pisrs.si/pregledPredpisa?id=PRAV12754.
65. UVDAG. *Uredba o varstvu dokumentarnega in arhivskega gradiva*, 2017, "Uradni list RS", št. 42/17. Pridobljeno 1. 7. 2024 s spletne strani: http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED6619.
66. UVDMVUPS. *Uredba o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov*, 2023, "Uradni list RS", št. 8/23. Pridobljeno 1. 7. 2024 s spletne strani: https://pisrs.si/pregledPredpisa?id=URED8592.
67. *What is Data Leakage*?, 2024. Forcepoint. Pridobljeno 17. 7. 2024 s spletne strani: https://www.forcepoint.com/cyber-edu/data-leakage.
68. *What Is Information Security*?, 2024. Fortinet. Pridobljeno 14. 7. 2024 s spletne strani: https://www.fortinet.com/resources/cyberglossary/information-security.
69. What is information security? (N.d.). IBM. Pridobljeno 14. 7. 2024 s spletne strani https://www.ibm.com/topics/information-security.
70. ZInfV. *Zakon o informacijski varnosti*, 2023, "Uradni list RS", št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23. Pridobljeno 1. 7. 2024 s spletne strani: https://pisrs.si/pregledPredpisa?id=ZAKO7707.
71. ZKI. *Zakon o kritični infrastrukturi*, 2021, "Uradni list RS", št. 75/17 in 189/21 – ZDU-1M. Pridobljeno 1. 7. 2024 s spletne strani: https://pisrs.si/pregledPredpisa?id=ZAKO7106.
72. ZVDAGA. *Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih*, 2014, "Uradni list RS", št. 30/06 in 51/14. Pridobljeno 1. 7. 2024 s spletne strani: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4284.