A Proposed Framework for Technical Requirements of Copyright Protection for Information Resources in NLAI Information Systems Using Fuzzy Delphi Technique

Zeinab Papi
PhD Knowledge and Information Science; Assistant Professor; Information Management and Knowledge Organization Department; National Library and Archives of Iran; Tehran, Iran;
Email: z-papi@nlai.ir

Iranian Journal of Information Processing and Management

Received: 25, Jun. 2023 **Accepted: 18, Jul. 2023**

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Vol. 39 | No. 2 | pp. 503-534
Winter 2024
https://doi.org/10.22034/jipm.2023.706814

Abstract: The purpose of the current research is to identify technical requirements for protection of information resources in the information systems (ISs) of National Library and Archives of Iran (NLAI) and evaluate them. The present study is an applied research in terms of purpose. In present study a qualitative approach is used to examine and analyze the status of the ISs of the NLAI. Documentary analysis, Tem analysis, and Fuzzy Delphi techniques were used to collect data. The research community includes the ISs of the NLAI and experts in the field of information technology. The ISs consisted of Digital Library system, Iranian Newspaper System (SANA), National Libraries Network, National Document Center Network, Iran Publications database, Manuscript database, Iranian Scientific Publications System. Also, 21 people (10 people to interview and 11 people to participate in Delphi techniques) were selected experts in the fields of Iss, digital libraries, copyright and technology. For data analysis, coding and categorization of concepts were used of open coding for documentary analysis and Tem analysis. Qualitative data analysis was done manually using MAXQDA 2020 software. Also, descriptive survey was used to analyze the indicators in fuzzy Delphi method and calculations were done using Excel. Tableau 2018 software was used to display and draw indicators better.

Therefore, using Tem analysis method, 70 indicators of preventive technical requirements were identified, and then these indicators were given to 11 experts, and after two rounds of fuzzy Delphi panel, 69 indicators identified. These indicators including 12 components were carried out. Finally, indicators “Adobe Reader and other tools” was removed from the checklist. The use of different methods to collect technical indicators and the use of triangulation method gives credibility to the research. Network

Security, standards and frameworks, Authentication, digital reading tools, digital preservation, payment systems; rights metadata, access control, copy control, License, Digital repository and transfer have formed 12 components of preventive technical requirements. Also, the findings of the research showed that digital and bibliographic systems were at a weak level in terms of taking advantage of preventive technical requirements for copyright. This study offered technical framework. The use of technical requirements such as lookInside, the copyright of policy, rights metadata, development and updating of systems and communication and interaction with the software support company, METS standard and use of digital repository offered in the studied ISs.

Keywords: Technical Requirements, Copyright, Information Resources (ISs), Digital Information Resources, National Library and Archives of Iran (NLAI), Information Systems

ارائه چارچوب پیشنهادی الزامات فنی حمایت از کپی‌رایت منابع اطلاعاتی در سامانه‌های اطلاعاتی سازمان اسناد و کتابخانه ملی ایران (تکنیک دلفی فازی)

زینب پاپی

دکتری علم اطلاعات و دانش‌شناسی؛ استادیار؛
گروه پژوهشی مدیریت اطلاعات و سازماندهی دانش؛
سازمان اسناد و کتابخانه ملی ایران؛ تهران، ایران؛
z-papi@nlai.ir

پژوهش‌نامهٔ پردازش و مدیریت اطلاعات

دریافت: ۱۴۰۲/۰۴/۰۴ | **پذیرش:** ۱۴۰۲/۰۴/۲۷ | مقاله برای اصلاح به مدت ۱ روز نزد پدیدآور بوده است.

نشریهٔ علمی | رتبهٔ بین‌المللی
پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)
شاپا (چاپی) ۸۲۲۳-۲۲۵۱
شاپا (الکترونیکی) ۸۲۳۱-۲۲۵۱
نمایه در LISTA، ISC، و SCOPUS
jipm.irandoc.ac.ir
دورهٔ ۳۹ | شمارهٔ ۲ | ص‌ص ۵۰۳-۵۳۴
زمستان ۱۴۰۲
https://doi.org/10.22034/jipm.2023.706814

چکیده: پژوهش حاضر با هدف شناسایی الزامات فنی حفاظت از کپی‌رایت منابع اطلاعاتی در سامانه‌های اطلاعاتی «سازمان اسناد و کتابخانه ملی ایران» و سپس ارزیابی آن‌ها انجام شده است. این پژوهش از نظر هدف کاربردی است به این دلیل که شناسایی الزامات فنی می‌تواند به بهبود حفاظت از حقوق پدیدآورندگان در سامانه‌ها کمک کند. برای گردآوری داده‌ها از رویکرد کیفی استفاده شده و روش تحلیل اسنادی، تحلیل مضمون و فن دلفی فازی به‌کار رفته است. جامعه پژوهش شامل سامانه‌های «سازمان اسناد و کتابخانه ملی ایران» و ۲۱ نفر (۱۰ نفر در مصاحبه و ۱۱ نفر در پنل دلفی) از متخصصان حوزه کتابخانه‌های دیجیتال، فناوری اطلاعات و سامانه‌های اطلاعاتی برای شرکت در مصاحبه و پنل دلفی است. سامانه‌های مورد مطالعه عبارت‌اند از: سامانه منابع دیجیتال، شبکه کتابخانه‌های کشور، شبکه مراکز اسناد کشور، بانک نشریات ایران، فهرستگان نسخ خطی، سنا (سامانه نشریات ایران)، و سامانه نشریات علمی ایران. برای تحلیل داده‌ها از کدگذاری و مقوله‌بندی مفاهیم در قالب کدگذاری باز برای تحلیل اسنادی و تحلیل مضمون استفاده شد. تحلیل کیفی داده‌ها با روش تحلیل مضمون به‌صورت دستی و با استفاده از نسخه ۲۰۲۰ نرم‌افزار «مکس کیودی‌ای» انجام شد. همچنین برای تحلیل شاخص‌ها در روش دلفی فازی، از پیمایش توصیفی استفاده شد و محاسبات با استفاده از «اکسل» صورت گرفت. برای نمایش و ترسیم بهتر شاخص‌ها، نرم‌افزار Tableau نسخه ۲۰۱۸ به‌کار رفته است. یافته‌ها با استفاده از

روش تحلیل مضمون بیانگر شناسایی ۷۰ شاخص الزامات فنی پیشگیرانه است. این شاخص‌ها در اختیار ۱۱ نفر خبره قرار گرفت و پس از دو دور انجام پنل دلفی فازی، توافق بر روی ۶۹ شاخص که دربردارنده ۱۲ مؤلفه بودند، صورت گرفت. سرانجام، شاخص «استفاده از آدوب ریدر و سایر ابزارها» از سیاهه وارسی حذف شد. استفاده از رویکرد مثلث‌سازی روش‌شناختی تأییدی بر اعتبار پژوهش است. یافته‌ها نشان می‌دهد که در سامانه‌های مورد بررسی، اغلب شاخص‌های فنی مربوط به الزامات فنی پیشگیرانه استفاده نمی‌شود. امنیت شبکه، استانداردها و چارچوب‌ها، احراز هویت، ابزارهای خوانش دیجیتال، حفاظت دیجیتال، سیستم‌های پرداخت، فراداده حقوقی، کنترل دسترسی، کنترل کپی، مجوز، مخزن دیجیتال، و نقل و انتقال ۱۲ مؤلفه الزامات فنی پیشگیرانه را شکل داده‌اند. همچنین یافته‌های پژوهش حاکی از آن است که سامانه‌های دیجیتال و کتابشناختی از نظر بهره‌گیری از الزامات فنی پیشگیرانه برای رعایت کپی‌رایت نیز در سطح ضعیفی قرار دارند. نتایج این پژوهش استفاده از الزامات فنی از جمله ریزدانگی، تدوین سیاست کپی‌رایت و استفاده از فراداده حقوقی، توسعه و روزآمد نگه‌داشتن سامانه‌ها و ارتباط و تعامل با شرکت پشتیبان نرم‌افزار، استاندارد «متس» و بهره‌گیری از مخزن دیجیتال را در سامانه‌های مورد مطالعه به‌منظور حفاظت از حقوق پدیدآورندگان و بهره‌داران آثار پیشنهاد می‌دهد.

کلیدواژه‌ها: کپی‌رایت، منابع اطلاعاتی، منابع اطلاعات دیجیتال، منابع کتابخانه‌ای، سامانه‌های سازمان اسناد و کتابخانه ملی ایران، الزامات فنی، حق مؤلف

۱. مقدمه

گسترش استفاده از منابع اطلاعاتی چه به‌صورت فیزیکی و یا دیجیتال، موانع و مشکلات زیادی در دسترسی به این منابع در فضای دیجیتال به‌وجود آورده است. یکی از این مسائل که می‌توان آن را به‌عنوان یک چالش برشمرد، موضوع حقوق مؤلفان و بهره‌داران آن منابع است. کتابخانه‌ها به‌طور معمول با توجه به نوع نگاه خود به نظریه دسترسی در برابر مالکیت تمایل بسیاری به در دسترس قراردادن منابع اطلاعاتی دارند. البته، این امر با توجه به وظیفه ذاتی کتابخانه‌ها صورت می‌گیرد که اشاعه اطلاعات از آن جمله است.

بنابراین، برای جلوگیری از نادیده‌انگاشتن حقوق مادی و معنوی پدیدآورنده، باید به‌دنبال راهکارهایی بود که بدون ایجاد اختلال در این مجرای جدید، حقوق پدیدآورنده هم حفظ شود (نوروزی ۱۳۸۱). الزامات فنی مانند کنترل دسترسی، و کنترل کپی (پاپی ۱۳۹۴؛ Technological Protection Measures and the Copyright Amendment Act 2006)،

واترمارک (آب‌نقش) دیجیتال، رمزنگاری، استگانوگرافی[1]، امضای دیجیتال، گواهینامه امنیتی (Digital Rights Management and Technical Protection Measures 2006؛ Jean-Mary 2020؛ Wazirali et al. 2021) و مانند آن از این دست محسوب می‌شوند. استفاده از این الزامات در سامانه‌های اطلاعاتی کتابخانه‌ها به حفظ توازن بین دو نظریه مالکیت و دسترسی و حفاظت از حقوق پدیدآور و کاربر کمک می‌کند.

«سازمان اسناد و کتابخانه ملی ایران» چند سالی است که به ایجاد و توسعه سامانه‌های مختلف در حوزه منابع کتابخانه‌ای و اسنادی، از جمله سامانه منابع دیجیتال، شبکه کتابخانه‌های کشور، شبکه مراکز اسناد کشور، بانک نشریات ایران، فهرستگان نسخ خطی، سنا (سامانه نشریات ایران) و سامانه نشریات علمی ایران پرداخته است. بنابراین، حفظ مالکیت و جلوگیری از استفاده غیرقانونی از منابع اطلاعاتی موجود در سامانه‌ها و همچنین ایجاد دسترسی قانونمند برای کاربران، نیازمند الزامات فناورانه‌ای است که بتواند در راستای این دو هدف گام بردارد؛ چرا که پیاده‌سازی سامانه‌های کاربرمحور بدون توجه به کپی‌رایت منابع اطلاعاتی می‌تواند به اعتماد و باور بهره‌داران منابع اطلاعاتی در سامانه‌ها خدشه وارد سازد. سامانه‌های یادشده با توجه به نوع عملکردشان در دو دسته دیجیتال و کتابشناختی قرار می‌گیرند: سامانه‌هایی که در زمان انجام پژوهش تنها دسترسی به اطلاعات کتابشناختی منابع را فراهم کرده‌اند، و سامانه‌هایی که در حال حاضر افزون بر اطلاعات کتابشناختی، دسترسی به متن کامل و مشاهده برخی از منابع را نیز امکان‌پذیر نموده‌اند. استفاده از هر دو دسته سامانه برای کاربران حقیقی و حقوقی می‌تواند منافع زیادی به ارمغان آورد، اما نباید از حقوق پدیدآور منابع موجود در سامانه‌های یادشده غافل ماند. در این پژوهش در خصوص سامانه‌ها دو نکته حائز اهمیت است: نکته اول، برای سامانه‌هایی که در زمان انجام پژوهش تنها دسترسی به اطلاعات کتابشناختی منابع را فراهم کرده‌اند، الزامات حفاظتی فنی ارائه‌شده برای آینده سامانه‌ها مناسب است. نکته دیگر اینکه سامانه‌هایی که در حال حاضر افزون بر اطلاعات کتابشناختی، دسترسی به متن کامل و مشاهده برخی از منابع را نیز امکان‌پذیر نموده‌اند. ضمن بررسی الزامات حفاظتی فنی این‌گونه سامانه‌ها، برای دسترسی به تمام‌متن منابع در آینده نیز اقدامات حفاظتی مورد نیاز برای رعایت کپی‌رایت ارائه می‌شود. بر همین اساس، پژوهش حاضر

1. steganography

در نظر دارد وضعیت موجود سامانه‌های اطلاعاتی «سازمان اسناد و کتابخانه ملی ایران» را از نظر میزان رعایت کپی‌رایت منابع اطلاعاتی با توجه به الزامات فناورانه بررسی و تحلیل کند. حاصل این تحلیل‌ها ارائه راهکارهایی فنی برای بهبود و توسعه سامانه‌های مذکور برای حفاظت از کپی‌رایت است. با این اوصاف، پژوهش کنونی به‌دنبال پاسخ به پرسش‌های زیر است:

۱. وضعیت سامانه‌های مورد بررسی از نظر امکانات و تجهیزات فنی برای حفاظت از کپی‌رایت منابع اطلاعاتی چگونه است؟
۲. چارچوب پیشنهادی الزامات فنی به‌منظور حفاظت از کپی‌رایت منابع اطلاعاتی در سامانه‌های اطلاعاتی «سازمان اسناد و کتابخانه ملی ایران» کدام است؟

۲. پیشینه پژوهش

بررسی پژوهش‌ها و مطالعات در داخل و خارج از کشور بیانگر آن است که در راستای پژوهش حاضر تاکنون چند رویکرد وجود دارد: ۱. پژوهش‌ها و مطالعاتی که به اقدامات حفاظتی فناورانه پرداخته‌اند؛ ۲. مطالعاتی که بررسی سامانه‌های اطلاعاتی را از منظر امنیت اطلاعات مورد توجه قرار داده‌اند؛ ۳. حفاظت دیجیتال در قوانین کپی‌رایت کشورها از جمله موضوعات دیگری است که توسط پژوهشگران کنکاش شده است؛ و ۴. یکی از مؤلفه‌های امنیت و حفاظت از اطلاعات، استفاده از سیستم «دی‌آرام»[1] است که در برخی از پژوهش‌ها این موضوع به‌صورت مجزا مد نظر قرار گرفته است. بنابراین با توجه به رویکردهای گفته‌شده، پژوهش‌ها و مطالعاتی از این رویکردها مورد بهره‌برداری قرار گرفت که ارتباط نزدیک‌تری با موضوع پژوهش داشته‌اند. پژوهش‌های داخل و خارج از کشور با توجه به موضوع، روش و یافته‌ها مطالعه و تحلیل شدند (جدول ۱).

جدول ۱. تصویری توصیفی از پژوهش‌های انجام‌شده

موضوع	نویسنده/ سال	هدف	روش	یافته‌ها
اقدامات حفاظتی فنی	Keplinger (2001)	شناسایی اقدامات حفاظتی فناورانه در وب	کیفی/ تحلیلی	استفاده از اقدامات سخت‌افزاری و نرم‌افزاری مانند رمزنگاری، امضای دیجیتال، استگانوگرافی و کنترل استفاده از آثار تحت حمایت کپی‌رایت

1. digital rigths managemnent (DRM)

موضوع	نویسنده/ سال	هدف	روش	یافته‌ها
	Conroy (2006)	تعیین اقدامات حفاظتی فناورانه در قانون کپی‌رایت آفریقای جنوبی	کیفی/ مطالعه تطبیقی	استفاده از رمز عبور به‌عنوان یکی از اقدامات فنی کنترل دسترسی
	Hassanein& Ghinea (2013)	ارائه نمونه پیشنهادی برای استفاده از انگشت‌نگاری در محتوای دیجیتال	تجربی/ تحلیلی	استفاده از فناوری بارکد در الگوریتم انگشت‌نگاری متن برای حفاظت از کپی‌رایت محتوای دیجیتال
	Stabingis, Sarlauskiene and Cepaitiene, (2014)	شناسایی اقدامات برای جلوگیری از سرقت علمی	کیفی/ تحلیلی	استفاده از نرم‌افزارهای کشف سرقت علمی
	پاپی (۱۳۹۴)	شناسایی الزامات فنی برای حفاظت از کپی‌رایت رساله‌ها و پایان‌نامه‌ها در سامانه گنج ایرانداک	ترکیبی/ پیمایش توصیفی و گراندد تئوری	استفاده از الزامات فنی مانند کنترل دسترسی، کنترل کپی، پروتکل‌های امن انتقال فرامتن، احراز هویت، شناسگرهای دیجیتال، سیستم‌های کشف کپی، سیستم مدیریت حقوق دیجیتال و سیستم‌های الکترونیکی مدیریت کپی‌رایت برای سامانه اطلاعاتی گنج
	Abu Sirhan et al. (2019)	بررسی سیستم مدیریت حقوق دیجیتال در کتابخانه‌های دانشگاه‌های دولتی اردن	کیفی	استفاده از روش‌های حفاظتی مختلفی مانند کدگذاری، احراز هویت، اعتبارسنجی و واترمارک دیجیتال در کتابخانه‌های دانشگاه‌های دولتی اردن و استفاده نکردن از روش‌هایی مانند امضای دیجیتال، اثرانگشت دیجیتال، سیستم‌های تشخیص کپی و سیستم پرداخت
	آموزگار، نوروزی و صراف‌زاده (۱۴۰۱)	شناسایی چالش‌های حق مؤلف منابع دیجیتال متنی		یکی از چالش‌های حق مؤلف منابع دیجیتالی را چالش‌های فناوری حفاظتی، سیستمی و شبکه‌ای بیان می‌کنند. پژوهشگران با روش پیمایشی- تحلیلی به‌دنبال شناسایی چالش‌های حق مؤلف منابع دیجیتال متنی از طریق مدیران کتابخانه‌های دیجیتال دانشگاه‌های شهر تهران بودند.

موضوع	نویسنده/ سال	هدف	روش	یافته‌ها
امنیت اطلاعات در سامانه‌های اطلاعاتی	تقوا و ایزدی (۱۳۹۲)	شناسایی شیوه‌های احراز هویت در سامانه‌های اطلاعاتی	توصیفی	دسترس‌پذیری و احراز هویت (دربردارنده رمزنگاری و استفاده از شناسه کاربری) به‌عنوان مؤلفه‌های امنیتی
	حریری و نظری (۱۳۹۱)	ارزیابی امنیت اطلاعات در کتابخانه‌های دیجیتال ایرانی	کمی/ پیمایش ارزیابانه	بررسی امنیت اطلاعات در ۴۵ کتابخانه دیجیتال؛ برآورد میانگین امنیت کتابخانه دیجیتال کتابخانه ملی ایران در حدود ۰/۸۰ (از ۱۰۰)؛ شاخص کنترل دسترسی کتابخانه‌های دیجیتال تحت بررسی، ۰/۷۹ است.
	European Commission (2011)	ارائه استانداردی برای امنیت اطلاعات سامانه‌های اطلاعاتی	نوعی استاندارد/ روش آن براساس شیوه‌های تدوین استانداردهای بین‌المللی	اشاره به مکانیزم‌های کنترل دسترسی دربردارنده ویژگی‌های سخت‌افزاری، نرم‌افزاری، رویه‌های عملیاتی و مدیریتی؛ توجه به انواع مختلف احراز هویت مانند احراز هویت زیستی، توکن، رمز عبور، پین و نظیر آن
	نوروزی (۱۳۹۰)	بررسی محورهای توسعه در کتابخانه‌های دیجیتال	کیفی/ تحلیل اسنادی	استفاده از دیواره آتش، سیستم تشخیص نفوذ، نرم‌افزارهای ضدویروس را برای امنیت نرم‌افزار کتابخانه دیجیتال مهم قلمداد می‌کنند. این اقدامات فنی برای تحکیم و افزایش امنیت مؤثر هستند.
	کوکبی و کوهی رستمی (۱۳۹۴)	ارزیابی امنیت اطلاعات در سامانه‌های نهاد کتابخانه‌های عمومی کشور	کمی/ پیمایش ارزیابانه	بررسی چهار «سامانه شبکه کتابخوانان حرفه‌ای»، «سامانه طرح کتاب من»، «سامانه پیام مشرق» و «سامانه آماری فرزین» نهاد کتابخانه‌های عمومی کشور از امنیت اطلاعات؛ شاخص وضعیت کنترل دسترسی در این سامانه‌ها در سطح متوسط است.
بررسی استثنائات کتابخانه‌ای و حفاظت دیجیتال در قوانین	Crews (2008)	بررسی استثنائات و معافیت‌های کتابخانه‌ای در قانون کپی‌رایت ۱۸۴ کشور جهان	کیفی/ مطالعه تطبیقی	توجه به کنترل دسترسی و یا کنترل حقوق مالک اثر در قوانین کشورها برای جلوگیری یا محدودیت در تکثیر اثر

موضوع	نویسنده/ سال	هدف	روش	یافته‌ها
	Huiming (2021)	مقایسه و تحلیل قوانین کپی‌رایت ایالات متحده، اتحادیه اروپا با چین در زمینه اقدامات حفاظتی فناورانه	کیفی/ مقایسه تطبیقی، تحلیل نظری	مقایسه اقدامات فنی در حمایت از کپی‌رایت را در قوانین ایالات متحده، اتحادیه اروپا با چین (WCT, WPPT)؛ ناسازگاری بین حفاظت از اقدامات فنی و حفظ کتابخانه‌های دیجیتالی در قانون کپی‌رایت چین؛ پیشنهاد اعمال محدودیت‌ها و استثناهایی در خصوص اقدامات فنی برای کتابخانه‌ها در قانون‌گذاری جدید در چین
	رحمانی (۱۳۹۰)	تحلیل قانون کپی‌رایت ایران با اقتضائات سیستم مدیریت حقوق دیجیتال	کیفی/ تحلیلی	منافع کاربران را در نظر نگرفته، و موضوع استثنائات که در قوانین مورد تأکید است، در این سیستم به آن کم‌توجهی شده است. از مصادیق مهم این منافع، استفاده منصفانه بدون نیاز به اجازه یا پرداخت است.
	آقاسیدجوادی و علیپور حافظی (۱۳۹۵)	بررسی سیستم مدیریت حقوق دیجیتال در سامانه گنج ایرانداک	کاربردی/ مطالعه موردی	بررسی فناوری «دی‌آرام» در سامانه گنج ایرانداک؛ نامطلوب بودن سامانه از نظر زیرساخت‌های امنیتی؛ مواجه‌شدن با تهدیدهایی نظیر دسترسی غیرمجاز، اشکال مدیریتی، عدم امکان پیگرد؛ نیاز به استفاده از فناوری «دی‌آرام»؛ پیشنهاد استفاده از رمزنگاری نامتقارن، گواهینامه دیجیتال، واترمارکینگ پیشرفته و امضای دیجیتال در سامانه

جمع‌بندی مطالعات پیشین

همان‌طور که از مطالعه پژوهش‌های مختلف برمی‌آید، پژوهش‌هایی به اقدامات حفاظتی فناورانه برای حمایت از کپی‌رایت اختصاص یافته است. پژوهش‌های (Keplinger 2001; Conroy 2006; Hassanein and Ghinea 2013; Stabingis, Sarlauskiene and Cepaitiene 2014; Abu Sirhan and et al. 2019 و پاپی ۱۳۹۴) در این دسته قرار می‌گیرند. این پژوهش‌ها به اقدامات کنترل دسترسی و کنترل کپی مانند رمزنگاری، امضای دیجیتال، استگانوگرافی و کنترل استفاده از آثار، فناوری بارکد در الگوریتم انگشت‌نگاری متن، نرم‌افزارهای کشف سرقت علمی، پروتکل‌های امن انتقال فرامتن، احراز هویت، شناسگرهای دیجیتال، سیستم مدیریت حقوق دیجیتال، سیستم‌های الکترونیک مدیریت کپی‌رایت، اعتبارسنجی و آب‌نقش دیجیتال، سیستم‌های تشخیص کپی و سیستم پرداخت اشاره شده است. همچنین پژوهش «آموزگار، نوروزی و صراف‌زاده» (۱۴۰۱) یکی از چالش‌های حق مؤلف منابع دیجیتال را چالش‌های فناوری حفاظتی، سیستمی و شبکه‌ای برمی‌شمارند. دسته دیگری از پژوهش‌ها مؤلفه‌های امنیتی در سامانه‌های اطلاعاتی را مورد تحلیل قرار داده بودند؛

از جمله، پژوهش‌هایی مانند «تقوا و ایزدی» (۱۳۹۲)، «حریری و نظری» (۱۳۹۱)، «نوروزی» (۱۳۹۰)، «کوکبی و کوهی رستمی» (۱۳۹۴) و European Commission (2011). با توجه به بررسی‌ها روشن می‌شود که شیوه‌های مختلفی برای احراز هویت اجرا می‌شود. در استاندارد اتحادیه اروپا و پژوهش «تقوا و ایزدی» (۱۳۹۲)، به شیوه‌هایی مانند احراز هویت زیستی، توکن، رمز عبور، پین، شناسه کاربری و نظیر آن اشاره شده است. در دو پژوهش دیگر در این دسته، شاخص‌های کنترل دسترسی در سامانه‌های نهاد کتابخانه‌های عمومی کشور و سامانه دیجیتال کتابخانه‌های مورد بررسی قرار دارند. در پژوهش «کوکبی و کوهی رستمی» (۱۳۹۴)، شاخص‌های امنیتی در سطح متوسط و در پژوهش «حریری و نظری» (۱۳۹۱)، سامانه دیجیتال کتابخانه ملی در سطح خوبی قرار گرفته است. پژوهش «نوروزی» (۱۳۹۰) نیز مؤلفه‌هایی در امنیت اطلاعات مانند استفاده از دیواره آتش، سیستم تشخیص نفوذ و نرم‌افزارهای ضدویروس را در نرم‌افزارهای کتابخانه دیجیتال ضروری می‌داند. با توجه به مطالعات موجود، برخی از پژوهش‌ها صرفاً قوانین کپی‌رایت کشورها را در راستای حفاظت دیجیتال بررسی کرده بودند. پژوهش‌های Crews (2008) و Huiming (2021) در این دسته قرار می‌گیرند. تکثیر آثار در قوانین کپی‌رایت کشورها، استثنائات کتابخانه‌ای و معاهدات بین‌المللی مانند WCT و WPPT در این پژوهش‌ها مطالعه و تحلیل شده بودند. پژوهش‌هایی از این دست می‌توانند به دولت‌ها برای اصلاح قوانین‌شان کمک کنند. یکی از اقدامات حفاظتی فنی برای بهبود فضای مجازی و تعامل کاربر و پدیدآورندگان، استفاده از نرم‌افزار «دی‌آرام» است. کاربرد فناوری «دی‌آرام» برای جلوگیری از تکثیر غیرمجاز در پژوهش‌های «رحمانی» (۱۳۹۰) و «آقاسیدجوادی و علیپور حافظی» (۱۳۹۵) مورد توجه و تأکید قرار گرفته است.

بنابراین، با توجه به بررسی و تحلیل مطالعات صورت‌گرفته می‌توان گفت که تاکنون پژوهشی همچون پژوهش حاضر در کشور انجام نشده است. چند ویژگی برای پژوهش حاضر قابل ارائه است: در پژوهش حاضر استفاده از فناوری «دی‌آرام» تنها به‌عنوان یکی از الزامات فنی برای حمایت از کپی‌رایت مورد بررسی قرار می‌گیرد. همچنین در این پژوهش به ارزیابی سامانه‌های مختلف پرداخته می‌شود. در پژوهش حاضر از سامانه منابع دیجیتال که حاوی منابع اطلاعاتی مختلف (کتاب، رساله و پایان‌نامه، نسخ خطی، منابع غیرکتابی، و مانند آن) با ویژگی‌های متفاوت و با دسترس‌پذیری‌های مختلف هستند تا سامانه‌های دیگری مانند سامانه نشریات ایران تحلیل می‌شوند. این در حالی است که

در دیگر پژوهش‌ها مانند پژوهش «آقاسیدجوادی و علیپور حافظی» (۱۳۹۵) هدف، بررسی فناوری «دی‌آرام» در «سامانه گنج ایرانداک» است که صرفاً رساله‌ها و پایان‌نامه‌ها را پوشش می‌دهد. در پژوهش «پاپی» (۱۳۹۴) نیز الزامات فنی برای رعایت کپی‌رایت در «سامانه گنج ایرانداک» مورد بررسی قرار گرفته است. در پژوهش‌های مورد بررسی دیگر تنها به برخی از اقدامات فنی در سامانه‌ها اشاره شده است. ضمن اینکه در روش‌شناسی پژوهش حاضر تفاوت‌هایی با سایر پژوهش‌ها وجود دارد. در این پژوهش با توجه به اهداف و پرسش‌های پژوهش از روش‌هایی مانند رویکرد کیفی و روش ارزیابانه، تحلیل اسنادی، تحلیل مضمون، روش دلفی فازی و پیمایش توصیفی استفاده می‌شود.

۳. روش پژوهش

پژوهش حاضر از نظر هدف کاربردی است؛ به این دلیل که شناسایی الزامات فنی می‌تواند به بهبود حفاظت از حقوق پدیدآورندگان در سامانه‌ها کمک کند، و از نوع ارزیابانه است و در آن برای گردآوری داده‌ها از رویکرد کیفی استفاده شده است. به همین منظور، برای شناسایی شاخص‌های فنی از روش تحلیل اسنادی (مطالعه منابع و پژوهش‌ها) در تهیه سیاهه وارسی استفاده شد. در ادامه، برای تحلیل بخشی از داده‌ها از روش تحلیل مضمون و برای اعتبارسنجی شاخص‌ها، رویکرد دلفی فازی به‌کار برده شد. برابر آنچه بیان شد، در چند گام به ساختار روش پژوهش می‌پردازیم. **گام نخست:** با توجه به اهداف پژوهش، برای استخراج شاخص‌های مربوط به الزامات فنی، مطالعات و منابع مختلف پژوهشی بررسی و تحلیل شد. جست‌وجو در پایگاه‌های اطلاعاتی داخلی مانند اپک «سازمان اسناد و کتابخانه ملی ایران»، «گنج ایرانداک»، پرتال جامع علوم انسانی، پرتال علمی «جهاد دانشگاهی» با کلیدواژه‌های الزامات فنی، امنیت اطلاعات، کپی‌رایت در کتابخانه‌ها، سامانه‌های اطلاعاتی و کپی‌رایت و کتابخانه‌های دیجیتال انجام شد. همچنین در پایگاه‌های اطلاعاتی خارجی مانند «گوگل اسکالر»[1]، «ساینس دایرکت»[2]، «امرالد»[3]، «کتابخانه دیجیتال دانشگاه ایندیانا»[4]، Oalib، Sagepub، Jstor، و با کلیدواژه‌های Technical measures or requirements in digital libraries, copyright and libraries information systems جست‌وجو انجام شد. **گام دوم:** پس از استخراج مفاهیم مربوط به الزامات فنی

1. Google Scholar 2. ScienceDirect 3. Emerald
4. Digital Library of Indiana University

مربوط به موضوع پژوهش، برای تکمیل و کشف مفاهیم بیشتر و رفع برخی ابهامات، با ۱۰ نفر از متخصصان داخل و خارج از کشور مصاحبه نیمه‌ساختاریافته انجام شد. در انتخاب افراد برای مصاحبه از نمونه‌گیری هدفمند و سپس به‌صورت گلوله‌برفی استفاده شد و مصاحبه تا زمان اشباع داده‌ها ادامه یافت. نحوه شناسایی متخصصان با توجه به دانش، تجربه، تمایل و زمان کافی برای شرکت در پژوهش بوده است. تعداد ۱۰ نفر از متخصصان برای مصاحبه اعلام آمادگی کردند (جدول ۳). با اعلام آمادگی افراد، مصاحبه به‌صورت نیمه‌ساختاریافته با افراد داخل کشور به‌صورت حضوری، مجازی و افراد خارج از کشور از طریق پست الکترونیک انجام شد. متخصصان عضو پنل دلفی نیز با توجه به ویژگی‌هایی که بیان شد، انتخاب شدند. تعداد ۱۱ نفر در دور اول و دوم پنل دلفی حضور داشتند (جدول ۴). با توجه به شرایط مصاحبه‌شوندگان و نظر آن‌ها، مصاحبه‌ها به‌صورت حضوری، شبکه اجتماعی و پست الکترونیک انجام گرفت. برای رفع ابهام در مصاحبه و کسب اطلاعات بیشتر و عمیق‌تر، مصاحبه‌ها در سه یا چهار دور ادامه یافت. پیش از انجام مصاحبه، اطلاعات مختصری از موضوع و پرسش‌های کلی برای مصاحبه‌شونده به زبان فارسی و انگلیسی (برای متخصصان خارج از کشور) ارسال شد. برای گمنامی نام مصاحبه‌شوندگان به‌جای نام فرد مصاحبه‌شونده از کد (مصاحبه‌شونده کد ۱، ۲، ۳ و ...) استفاده شد. انجام مصاحبه‌ها تا زمانی که داده جدیدی به‌دست نیامد و تا زمان اشباع داده‌ها ادامه یافت. مصاحبه‌ها از ابتدای اسفندماه ۱۴۰۱ تا اول اردیبهشت‌ماه ۱۴۰۲ به طول انجامید.

پس از انجام و پیاده‌سازی مصاحبه‌ها برای تحلیل داده‌های به‌دست آمده، از روش تحلیل مضمون به‌صورت دستی در دو سطح مفهوم و مقوله استفاده شد (جدول ۵). تحلیل مضمون یک راهبرد تقلیل و تحلیل داده‌هاست که توسط آن داده‌های کیفی تقسیم‌بندی، طبقه‌بندی، تلخیص و بازسازی می‌شوند. تحلیل مضمون به‌عبارتی، راهبردی توصیفی است که یافتن الگوها و مفاهیم مهم را از دورن مجموعه داده‌های کیفی تسهیل می‌کند. در تحلیل مضمون مقایسه‌ای داده‌های مختلف به‌دست‌آمده از منابع مختلف، با یکدیگر مقایسه و تطبیق داده می‌شود تا شباهت‌ها و تفاوت‌ها شناخته شود (Given 2008 نقل در کمالی ۱۳۹۷).

مقوله‌های جدید استخراج‌شده از مصاحبه‌ها، که به الزامات فنی سامانه‌ها اختصاص داشتند، به سیاهه وارسی اضافه شدند. برای سنجش اعتبار درونی سیاهه وارسی از اعتبار

محتوا استفاده شد. سیاهه در اختیار دو نفر از متخصصان حوزه‌های یادشده قرار گرفت و نظرات آن‌ها دریافت و در سیاهه وارسی اعمال شد. همچنین آلفای کرونباخ برای سنجش پایایی سیاهه وارسی به‌کار رفت. پایایی ابزار اندازه‌گیری با استفاده از نرم‌افزار SPSS نسخه ۲۴ محاسبه شد. مقدار آلفای به‌دست آمده عددی برابر ۰/۹۸ است که اعتبار بسیار بالایی را نشان می‌دهد. **گام سوم**: برای اعتبارسنجی شاخص‌ها و الزامات فنی حفاظتی فناورانه در سامانه‌های اطلاعاتی «سازمان اسناد و کتابخانه ملی ایران»، از روش دلفی فازی استفاده شد. مقیاس انتخابی برای پرسش‌های سیاهه وارسی نیز طیف لیکرت (۱ الی ۵) بود. عدد ۱ به معنای بسیار کم و عدد ۵ به معنای بسیار زیاد مد نظر قرار گرفتند.

ارسال و دریافت سیاهه میان متخصصان در دو دور انجام شد. تعداد ۱۲۶ شاخص به‌عنوان الزامات فنی در مرحله اول و هنگام مطالعه متون و منابع و در مصاحبه با متخصصان استخراج شد. پس از بررسی و حذف موارد تکراری و انجام بازبینی، با استفاده از روش تحلیل مضمون تعداد ۷۰ شاخص الزامات فنی پیشگیرانه شناسایی شد. به‌منظور بسط بدنه دانشی موجود، پالایش و تأیید نهایی الزامات فنی از روش دلفی فازی استفاده شد. سیاهه وارسی در اختیار ۱۱ خبره قرار گرفت و از آن‌ها درخواست شد نظرشان را دربارهٔ هر شاخص در قالب متغیرهای کلامی مندرج در پرسشنامه بیان کنند (جدول ۲). با استفاده از روش دلفی فازی نظرات خبرگان مورد بررسی قرار گرفت. برای فازی‌سازی اعداد، ابتدا بر اساس طیف اعداد فازی مثلثی معادل طیف لیکرت ۵ درجه، به عدد فازی تبدیل می‌شوند.

جدول ۲. اعداد فازی مثلثی معادل طیف لیکرت ۵ درجه

عبارات زبانی	اعداد فازی مثلثی
بسیار کم	۰۰۰/۲۵
کم	(۰۰/۲۵، ۰/۵)
متوسط	(۰/۲۵، ۰/۵، ۰/۷۵)
زیاد	(۰/۵، ۰/۷۵، ۱)
بسیار زیاد	(۰/۷۵، ۱، ۱)

بر اساس رابطه $F_{AVE} = \frac{\sum l}{n} . \frac{\sum m}{n} . \frac{\sum u}{n}$ میانگین فازی از امتیازات اخذ می‌شود و توسط روابط $F_{AVE} = (L . M . U)$ و $X = \frac{L+M+U}{3}$ میانگین فازی به عدد قطعی تبدیل

می‌شود (حبیبی و آفریدی ۱۴۰۱). نتایج کلیه محاسبات فازی‌سازی، در جدول ۲، آورده شده است. در این پژوهش عدد آستانه ۰/۵ در نظر گرفته می‌شود.

در این مرحله میانگین فازی تنها شاخص «استفاده از آدوب ریدر و سایر ابزارها» کمتر از ۰/۵ بود و حذف شد. تحلیل دلفی فازی برای تمام شاخص‌های پذیرفته‌شده، در دور دوم ادامه پیدا کرد. در این دور ۶۹ شاخص بر اساس دیدگاه ۱۱ خبره مورد ارزیابی مجدد قرار گرفت. در این دور ۶۹ شاخص تأیید شدند. با توجه به اینکه اختلاف میانگین امتیازات سؤالات دور اول و دور دوم از عدد ۰/۲ کوچک‌تر بود، فرایند نظرسنجی متوقف شد (همان). در واقع، هرچه میانگین فازی‌زدایی‌شده بالا باشد، توافق بیشتری بر روی شاخص‌ها از دیدگاه خبرگان وجود دارد. شاخص‌های فوق در ۱۲ مؤلفه جای گرفتند.

گام چهارم: طیف استفاده‌شده در سیاهه وارسی برای ارزیابی سامانه‌ها دو گزینه «بلی» و «خیر» بود. سپس سامانه‌ها با استفاده از سیاهه وارسی توسط پژوهشگر و با کمک مدیران سامانه‌ها ارزیابی شدند. پس از ارزیابی با توجه به تعداد شاخص‌های الزامات فنی پیشگیرانه، سطح‌بندیِ اسامانه‌ها نیز صورت گرفت. سطوح ضعیف (۰-۲۳)، متوسط (۲۴-۴۶) و قوی (۴۷-۶۹) برای سامانه‌ها در نظر گرفته شد. جامعه پژوهش سامانه‌های مورد مطالعه دربردارنده سامانه‌های «سازمان اسناد و کتابخانه ملی ایران» بودند که عبارت‌اند از: سامانه منابع دیجیتال، شبکه کتابخانه‌های کشور، شبکه مراکز اسناد کشور، بانک نشریات ایران، فهرستگان نسخ خطی، سنا (سامانه نشریات ایران)، سامانه نشریات علمی ایران. «سازمان اسناد و کتابخانه ملی ایران» به‌عنوان تنها مرکزی است که برخی از سامانه‌ها مانند شبکه کتابخانه‌های کشور، شبکه مراکز اسناد کشور، فهرستگان نسخ خطی و سنا (سامانه نشریات ایران) در آنجا نگهداری و منابع اطلاعاتی آن برای کاربران قابل دسترس است. همچنین محتوای متنوع سامانه‌ها نیز از جمله دلایلی بود که سامانه‌های «سازمان اسناد و کتابخانه ملی ایران» به‌عنوان جامعه پژوهش برای مطالعه انتخاب شده‌اند.

جدول ۳. مشخصات مصاحبه‌شوندگان

ردیف	سطح تحصیلات	زمینه تخصصی	میزان تجربه کاری (به سال)	نام کشور
۱	کارشناس ارشد/ مهندسی تکنولوژی نرم‌افزار کامپیوتر	توسعه سامانه‌های اطلاعاتی، رمزنگاری	۱۵	ایران (تهران)
۲	دکتری تخصصی مهندسی فناوری اطلاعات	سامانه‌های اطلاعاتی	۲۰	ایران (تهران)
۳	دکتری علم اطلاعات و دانش‌شناسی	فناوری اطلاعات	۲۰	ایران (تهران)
۴	کارشناس ارشد فناوری اطلاعات	کتابخانه‌های دیجیتال	۱۷	ایران (تهران)
۵	دکتری فناوری اطلاعات و دکتری علم اطلاعات و دانش‌شناسی	فناوری اطلاعات، سامانه‌های اطلاعاتی	۲۱	ایران (تهران)
۶	Dr at Law, Assistant Professor	Copyright and Technology	۱۰	India (Delhi)
۷	Bachelor of Laws	Copyright, information creation, dissemination and management	۱۵	Nigeria (Ogwa Edo State)
۸	Professor, Intellectual Property Management	Intellectual Property Rights (IPRs), digital technology	۳۰	India (Delhi)
۹	Masters of Library Science	library technology, Digital libraries, Intellectual Property	۴۰	United States (California)
۱۰	PhD in computer science	Digital Library Strategist & Metadata Architect	۲۵	United States (Pennsylvania)
مجموع				۱۰ نفر

جدول ٤. مشخصات متخصصان و خبرگان عضو پنل دلفی

ردیف	سطح تحصیلات	زمینه تخصصی	میزان تجربه کاری (به سال)	دور اول پنل	دور دوم پنل
۱	دکتری ارتباطات	کتابخانه‌های دیجیتال	۲۵	ü	ü
۲	دکتری فناوری اطلاعات	سامانه‌های اطلاعاتی	۲۱	ü	ü
۳	دکتری علم اطلاعات و دانش‌شناسی	کتابخانه‌های دیجیتال	۲۰	ü	ü
۴	دکتری علم اطلاعات و دانش‌شناسی	کتابخانه‌های دیجیتال	۲۰	ü	ü

ردیف	سطح تحصیلات	زمینه تخصصی	میزان تجربه کاری (به سال)	دور اول پنل	دور دوم پنل
۵	کارشناسی مهندسی سخت‌افزار	سامانه‌های اطلاعاتی	۳۰	ü	ü
۶	کارشناس ارشد علم اطلاعات و دانش‌شناسی	سامانه‌های اطلاعاتی	۱۰	ü	ü
۷	دکتری علم اطلاعات و دانش‌شناسی	کتابخانه‌های دیجیتال	۱۵	ü	ü
۸	دکتری علم اطلاعات و دانش‌شناسی	کتابخانه‌های دیجیتال	۱۰	ü	ü
۹	کارشناس ارشد فناوری اطلاعات	کتابخانه‌های دیجیتال	۱۷	ü	ü
۱۰	کارشناس ارشد کامپیوتر- شبکه‌های کامپیوتری	سامانه‌های اطلاعاتی	۱۷	ü	ü
۱۱	کارشناس ارشد علم اطلاعات و دانش‌شناسی	سامانه‌های اطلاعاتی	۱۷	ü	ü
مجموع				۱۱ نفر	۱۱ نفر

برای ترسیم و تجسم داده‌ها پس از پایان پنل دلفی از نسخه ۲۰۲۰ نرم‌افزار «مکس کیودی‌ای» استفاده شد. همچنین برای تحلیل شاخص‌ها در روش دلفی فازی، پیمایش توصیفی به‌کار رفت و محاسبات با استفاده از «اکسل» صورت گرفت. برای نمایش و ترسیم بهتر شاخص‌ها در قالب نمودار، از نرم‌افزار Tableau نسخه ۲۰۱۸ استفاده شد.

Tableau نرم‌افزار رایگان تجسم داده‌های همه‌منظوره است که به‌طور گسترده در تجزیه‌وتحلیل داده‌ها استفاده می‌شود (Batt, Grealis, Harmon and Tomolonis 2020). به‌منظور اعتبارسنجی یافته‌های کیفی از روش سه‌سوسازی (مثلث‌سازی) روش‌شناختی استفاده شد. استفاده از روش‌های مختلف برای گردآوری اطلاعات مانند تحلیل اسنادی، تحلیل مضمون و دلفی فازی در این پژوهش می‌تواند اعتبار یافته‌های پژوهش را تأیید نماید. استفاده از راهبرد سه‌سوسازی نه‌تنها به نتایج معتبرتر و منطقی‌تر منجر می‌شود، بلکه به اعتقاد بسیاری از نظریه‌پردازان به کاهش سوگیری نیز کمک می‌کند (مدنی بروجنی و نصر ۱۳۸۸).

جدول ۵. نمونه‌ای از کدگذاری مصاحبه‌ها در تحلیل مضمون

مصاحبه‌شونده	نقل قول مرتبط	مفهوم	مقوله
Code 2	◇ The digital library systems I work with support metadata for expressing information on copyright and access control …. ◇	◇ استفاده از فراداده برای کپی‌رایت ◇ استفاده از فراداده برای کنترل دسترسی	◇ فراداده حقوقی و کپی‌رایت
Code 3	◇ modern research indicates that the emergence of blockchain technology may be useful to protect digital information content. Although research in this area is still scanty, however, the technology may be useful.	◇ استفاده از فناوری بلاک‌چین در محافظت از محتوای اطلاعات دیجیتال و کنترل دسترسی	◇ فناوری بلاک‌چین
کد ۱۰	◇ راجع به محتوای ویدیوئی هم امکان‌پذیر است که با ریزدانگی انجام میشه و میگیم از ثانیه فلان تا ثانیه فلان دربردارنده محدودیت دسترسی بشه. و این را به‌خصوص در مورد سامانه‌های محتوای ویدیوئی با ریپازیتوری میشه انجام داد و اگر مجهز به ریپازیتوری باشه خیلی راحت میشه انجام داد. ببینید ریپازیتوری منظور اینه که سامانه‌ای که در واقع عملیات اصلی ورودی و خروجی محتوا را بتونه به شکل یک اپریشن operation مشخص در نظر بگیره و این اپریشن operationمشخص را به شکلی انجام بده که هم خیلی ساده باشه و هم خیلی کارآمد باشه. حالا این عملیات خیلی ساده و خیلی مشخص در سیستم‌های مدیریت محتوای دیجیتال با استفاده از استاندارد OAIS تعریفش کردن	◇ استفاده از ریزدانگی در محتوای ویدیوئی ◇ امکان استفاده بهتر از ریزدانگی محتواهای ویدیوئی در ریپازیتوری ◇ استفاده از استاندارد OAIS در ریپازیتوری	◇ استفاده از ریزدانگی به‌کارگیری مخزن دیجیتال مدل مرجع آرشیوی OAIS

٤. یافته‌ها

٤-١. وضعیت سامانه‌های مورد بررسی از نظر امکانات و تجهیزات فنی برای حفاظت از کپی‌رایت منابع اطلاعاتی

پس از ارزیابی سامانه‌ها در خردادماه ۱۴۰۲، سامانه‌های مورد بررسی با توجه به نوع فعالیت، ساختار و عملکرد آن‌ها در دو گروه دیجیتال و کتابشناختی قرار داده شدند. سامانه‌های دیجیتال ملی، سامانه‌های نشریات ایران (سنا) و نشریات علمی ایران در دسته دیجیتال قرار گرفتند. ارائه منابع اطلاعاتی دیجیتال چه به‌صورت دیجیتال‌زاد و دیجیتال

در سامانه‌های مذکور از جمله دلیل این انتخاب است. سایر سامانه‌ها یعنی سامانه‌های بانک نشریات ایران، شبکه مراکز اسناد کشور، فهرستگان نسخ خطی و شبکه کتابخانه‌های کشور در دسته کتابشناختی جای می‌گیرند. سامانه‌های کتابشناختی صرفاً به ارائه اطلاعات کتابشناختی پرداخته و از نوع بانک اطلاعاتی محسوب می‌شوند.

٤-١-١. سامانه‌های دیجیتال: سامانه‌های دیجیتال مورد مطالعه از سیستم‌عامل ویندوز و پایگاه داده‌ای رابطه‌ای استفاده می‌کنند. زبان کوئری[1] مورد استفاده، SQL بوده و از «جاوا»[2] و Microsoft.NET به‌عنوان زبان برنامه‌نویسی بهره‌مند می‌شوند. در سنا و کتابخانه دیجیتال از نرم‌افزار «پاپیروس» استفاده می‌شود.

- **الزامات فنی پیشگیرانه:** همان‌طور که در جدول ۵، نشان داده شد، از ۶۹ شاخص الزامات فنی پیشگیرانه، ۲۱ (۳۰/۴۴ درصد) شاخص رعایت شده و ۴۸ شاخص (۶۹/۵۶ درصد) در سامانه‌های مورد مطالعه استفاده نشده است. یافته‌ها نشان داد که جداسازی[3] سرور پایگاه داده، رمزنگاری داده‌های حساس و پردازش استثنائات، استفاده از فایروال‌ها و اکسس ریموت‌های مختلف برای حفاظت از سرور، استفاده از تست نفوذ برای شناسایی شکاف‌های امنیتی، استفاده از ظرف عسل[4] برای حفاظت از سرور اصلی و دفع حملات و دریافت کانکشن‌های مفید، مسدودکردن آی‌پی بر اساس موقعیت مکانی، قطع دسترسی خروج دیتا از سرور برای کارکنان سامانه‌ها، استفاده از پروتکل ربات تی‌اکس‌تی[5] برای مدیریت دسترسی به محتواها برای خزشگرهای مجاز و غیرمجاز، محدودیت دسترسی برای کارکنان پردازش دیجیتال با تقسیم وظایف، تبدیل سامانه‌های بانک اطلاعاتی به سامانه‌های تحت وب و اعتبارسنجی[6] از جمله الزامات فنی هستند که در سامانه‌های دیجیتال مورد بررسی رعایت می‌شوند. اما از سرویس‌های وب[7] و پروکسی‌سرور برای دریافت منابع و اعمال محدودیت‌های دسترسی استفاده نمی‌شود. شاخص‌های فوق را می‌توان به‌عنوان شاخص‌های مهم در امنیت شبکه سامانه‌ها قلمداد کرد.

شاخص‌های احراز هویت مانند، Single Sign-On (SSO)، استفاده از OpenAthens برای SSO، فراهم‌آوری مدیریت دسترسی و هویت با InCommon، احراز هویت چندعاملی[8]،

1. query
2. JAVA
3. isolation
4. honeypot
5. txt
6. authorization
7. WebServices
8. multi-factor authentication (MFA)

احراز هویت زیستی، استاندارد هش[1] امن و الگوریتم‌های رمزگذاری استاندارد و محرمانه مانند «کلیپر»[2]، استفاده از امضای دیجیتال، انگشت‌نگاری، و گواهی دیجیتال هیچ‌یک در سامانه‌های دیجیتال به‌عمل نمی‌آید و تنها شماره‌های شناسایی شخصی یا پین[3]ها برای اصالت‌سنجی کاربر در سامانه‌های مورد بررسی به‌کار می‌رود. تحلیل و ارزیابی سایر شاخص‌ها با سامانه‌های دیجیتال مورد مطالعه حاکی از آن است که برای کنترل دسترسی کاربر، شاخص دسترسی مدیریت‌شده کاربر[4] کاربرد دارد. همچنین شاخص‌های استفاده از کپچا[5] برای محتواهای متنی و تصویری و استفاده از کپچای صوتی برای محتواهای شنیداری استفاده نمی‌شوند. افزون بر این، شاخص‌های استفاده از بلاک‌چین[6] و توکن غیرقابل تعویض[7] در اعمال دسترسی‌های مجاز، نرم‌افزار مدیریت حقوق دیجیتال (دی‌آرام)، امانت دیجیتال کنترل‌شده[8]، قفل نرم‌افزاری، استفاده از آب نقش پنهان، اقدامات کنترل کپی برای خوانش کتاب‌های الکترونیک، استفاده از رمزگذاری p2p2، سیستم درهم‌سازی محتوا[9]، دسترسی تصادفی و محدود به فراداده در سامانه‌ها، استفاده از ریزدانگی برای قالب‌های متنی، صوتی و ویدیوئی، استفاده از ذره‌بین مجازی، مهر زمانی (استامپ زمانی)، استگانوگرافی، استفاده از پردازش زبان طبیعی در پردازش فایل‌های صوتی و ویدیوئی، استفاده از دیتا استریمینگ[10] برای فایل‌های ویدیوئی و سیستم کشف کپی برای کنترل کپی در سامانه‌های دیجیتال فوق استفاده نشده‌اند، بلکه استفاده از کنترل‌های دسترسی زمانی، حذف فراداده منابع ممنوعه از نمایه پایگاه داده، امکان استفاده از نمایش در لحظه و کد کردن یوآرال برای کنترل کپی در سامانه‌های مذکور به‌کار رفته است. همین‌طور، بررسی استفاده از مجوزها برای دسترسی به محتواهای دیجیتال در سامانه‌های مورد مطالعه بیانگر آن است که از مجوز کریتیو کامنز[11] و سایر مجوزها برای دسترسی به محتواهای دیجیتال، پروتکل OAuth و قراردادهای هوشمند در جامعه مورد بررسی استفاده نشده است؛ ضمن اینکه پروتکل‌های انتقال امن SSL یا TLS در HTTPs و گواهینامه امنیتی در سامانه‌های دیجیتال یادشده برای انتقال امن اطلاعات به‌کار می‌رود.

از جمله شاخص‌های دیگری که در سامانه‌های یادشده بررسی شد، شاخص‌های مربوط به حفاظت

1. hash function
2. Clipper
3. pin
4. user-managed access (UMA)
5. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)
6. blockchain
7. non-fungible token (NFT)
8. controlled digital lending (CDL)
9. content scramble system (CSS)
10. Data Streaming
11. Creative Commons

دیجیتال بود. از شناساگر شیء دیجیتال[1] در حفظ اصالت محتواهای دیجیتال، که برای دستیابی دائمی به محتواهای دیجیتال استفاده می‌شود، در سامانه‌های یادشده استفاده نشده است. همچنین از مدل مرجع سیستم اطلاعاتی آرشیوی باز (اُای‌آی‌اس)[2] تا حدودی استفاده شده است. همچنین فناوری «اچ‌دی‌سی‌پی»[3] برای حفاظت از محتواهای دیداری-شنیداری در سامانه‌های مورد مطالعه به‌کار نرفته است. برخ سامانه‌ها برای اعمال اقدامات فناورانه، از چارچوب‌های خاص و فریم‌ورک[4]ها استفاده می‌کنند. یافته‌ها نشان داد که از فریم‌ورک‌ها (مانند مایکروسافت، لاراول) برای اعمال اقدامات امنیتی در سامانه‌های دیجیتال تحت بررسی استفاده نمی‌شود. به همین ترتیب، استاندارد «اُدبلیواِی‌اس‌تی» برای پیاده‌سازی الزامات فنی، استاندارد «اس‌اِی‌ام‌ال»[5] برای ایمن‌سازی سرویس‌دهنده‌ها و SSO، استانداردهایی مانند ISO- IEC 27001, BS 7799, PCIDSS, ITIL, COBIT، معاهدات اینترنتی کپی‌رایت WPPT[6] و WCT[7] و تدوین سیاست‌های مدیریت امنیت اطلاعات برای حفاظت از منابع دیجیتال به‌عنوان چارچوب‌های فنی به‌منظور منع دسترسی‌های غیرمجاز به‌کار نمی‌رود. همچنین بخشی از سیاست‌گذاری داده[8] تهیه شده و به‌صورت کامل هنوز سیاست‌ها و خط‌مشی‌هایی برای سیاست‌گذاری داده در سامانه‌های مورد مطالعه تدوین نشده است. ضمن اینکه از استانداردهای فراداده‌ای دوبلین کور در سامانه‌های دیجیتال استفاده می‌شود، اما با توجه به کاربردهای گسترده استاندارد متس[9] در تهیه فراداده حقوقی، طبق اذعان مدیر سامانه، تا حدودی از آن استفاده شده است. البته با بررسی صورت‌گرفته هنوز بخش استفاده‌شده متس در سامانه دیجیتال اجرا نشده است.

استفاده از راه‌حل‌های اینترنت اشیا برای کتاب‌های دیجیتال یکی دیگر از الزامات فنی است که برای خوانش دیجیتال به‌کار می‌رود و در حفظ حقوق پدیدآور نقش دارد. این شاخص نیز در سامانه‌های دیجیتالِ مورد بررسی استفاده نشده است. استفاده از مخزن دیجیتال (ریپازیتوری[10] دیجیتال) به‌عنوان یکی از شاخص‌های مهم در مدیریت و حفظ مجموعه‌های دیجیتال نام برده شده است. همچنین مدل مرجع سیستم اطلاعاتی آرشیوی باز (اُای‌آی‌اس) که برای حفاظت بلندمدت از مجموعه‌های دیجیتال نقش مؤثری دارد، در سامانه‌ها استفاده نشده است. تحلیل یافته‌ها نشان داد که استفاده از خط‌مشی کپی‌رایت در قالب فراداده کپی‌رایت نیز در سامانه‌های مورد گفت‌وگو تاکنون اجرایی نشده است.

1. digital object identifier (DOI)
2. Open Archival Information System (OAIS)
3. high-bandwidth digital content protection (HDCP)
4. framework
5. security assertion markup language (SAML)
6. WIPO Performances and Phonograms Treaty (WPPT)
7. WIPO Copyright Treaty (WCT)
8. data policy
9. metadata encoding and transmission standard (METS)
10. repository

ضمن اینکه به اذعان مدیر سامانه‌های یادشده از سیستم‌های پرداخت در سامانه‌های دیجیتال استفاده شده است. سیستم‌های پرداخت نوع خاصی از اقدامات حفاظتی بوده که به‌عنوان میانجی میان ارائه‌دهنده محتوا و کاربر عمل می‌کنند. البته در عمل و با بررسی سامانه دیجیتال، این الزام نیز هنوز اجرایی نشده است.

به‌طور کلی، با توجه به تعداد شاخص‌های هم‌وزن در الزامات فنی (۶۹ شاخص)، مقیاس سطح سنجش سامانه‌ها در سه دسته ضعیف، متوسط و قوی تعریف شد. سامانه‌های مورد مطالعه از نظر سطح به‌کارگیری شاخص‌های فنی برای حفاظت از کپی‌رایت منابع اطلاعاتی در سطح ضعیفی قرار دارند. همان‌طور که در جدول ۶، مشخص است، بعد الزامات فنی پیشگیرانه با امتیاز ۲۱ در سطح ضعیف قرار گرفته‌اند.

جدول ٦. سطح‌بندی سامانه‌های دیجیتال مورد مطالعه از نظر رعایت شاخص‌های فنی برای حمایت از کپی‌رایت

ابعاد	شاخص‌ها	فراوانی		سطح‌بندی سامانه‌ها		
		بلی	خیر	ضعیف (۲۳-۰)	متوسط (٤٦-٢٤)	قوی (٦٩-٤٧)
الزامات فنی پیشگیرانه	۶۹	۲۱ (۳۰/۴۴ درصد)	۴۸ (۶۹/۵۶ درصد)	✓	–	–

٤-١-٢. سامانه‌های کتابشناختی

سامانه‌های کتابشناختی که از نوع بانک اطلاعاتی محسوب می‌شوند، در این پژوهش دربردارنده سامانه‌های بانک نشریات ایران، شبکه مراکز اسناد کشور، فهرستگان نسخ خطی و شبکه کتابخانه‌های کشور هستند که در «سازمان اسناد و کتابخانه ملی ایران» ایجاد و راه‌اندازی شده‌اند. سامانه‌های یادشده به‌ترتیب به ارائه اطلاعات کتابشناختی از نشریات، اسناد، نسخ خطی و کتاب می‌پردازند. اطلاعات این سامانه‌ها از مراکز مختلف گردآوری شده است.

در سامانه‌های کتابشناختی برعکس دیجیتال، از لینوکس[1] استفاده می‌شود. زبان کوئری آن SQL بوده و پایگاه داده‌ای رابطه‌ای به‌کار می‌برد. همچنین «جاوا» زبان برنامه‌نویسی مورد استفاده در سامانه‌های یادشده است.

نتیجه ارزیابی کیفی بعد الزامات فنی پیشگیرانه به همراه شاخص‌های فنی آن‌ها در

1. Linux

سامانه‌های مورد مطالعه به‌شرح زیر تشریح شده است:

- **الزامات فنی پیشگیرانه:** ارزیابی سامانه‌های کتابشناختی برای به‌کارگیری شاخص‌های فنی به‌منظور رعایت کپی‌رایت نشان داد که شاخص‌های جداسازی سرور پایگاه داده، رمزنگاری داده‌های حساس و پردازش استثنائات، استفاده از فایروال‌ها و اکسس‌ریموت[1]های مختلف برای حفاظت از سرور، استفاده از ظرف عسل برای حفاظت از سرور اصلی و دفع حملات و دریافت کانکشن‌های مفید، اعتبارسنجی، سرویس‌های وب و محدودیت دسترسی برای کارکنان پردازش دیجیتال با تقسیم وظایف انجام شده است. ضمن اینکه شاخص‌های فنی دیگر که در امنیت شبکه نیز مهم هستند، مانند استفاده از تست نفوذ برای شناسایی شکاف‌های امنیتی، مسدودکردن آی‌پی بر اساس موقعیت مکانی، قطع دسترسی خروج دیتا از سرور برای کارکنان سامانه‌ها، استفاده از پروتکل ربات تی‌اکس‌تی برای مدیریت دسترسی به محتواها برای خزشگرهای مجاز و غیرمجاز، تبدیل سامانه‌های بانک اطلاعاتی به سامانه‌های تحت وب و پروکسی‌سرور برای دریافت منابع و اِعمال محدودیت‌های دسترسی در سامانه‌های یادشده استفاده نشده است.

در ارزیابی شاخص‌های احراز هویت، یافته‌ها نشان داد که از (SSO) و شماره‌های شناسایی شخصی، یا پین‌ها در سامانه‌های مورد بررسی استفاده می‌شود. اما شاخص‌های فنی دیگر یعنی استفاده از OpenAthens برای SSO، فراهم‌آوری مدیریت دسترسی و هویت با InCommon، احراز هویت چندعاملی، احراز هویت زیستی، استاندارد هش امن و الگوریتم‌های رمزگذاری استاندارد و محرمانه مانند «کلیپر»، امضای دیجیتال، انگشت‌نگاری و گواهی دیجیتال، هیچ‌یک در سامانه‌های دیجیتال استفاده نمی‌شوند.

یافته‌های حاصل از ارزیابی سایر شاخص‌ها با سامانه‌های کتابشناختی نشان داد که شاخص دسترسی مدیریت‌شده کاربر (یوام‌ای) در کنترل دسترسی کاربر استفاده می‌شود. همچنین شاخص‌های استفاده از کپچا برای محتواهای متنی و تصویری و استفاده از کپچای صوتی برای محتواهای شنیداری به‌کار نرفته است.

افزون بر این، در خصوص سایر شاخص‌ها که به کنترل کپی اختصاص دارد، شاخص‌های استفاده از بلاک‌چین و توکن غیرقابل تعویض در اعمال دسترسی‌های مجاز،

1. remote access

نرم‌افزار مدیریت حقوق دیجیتال، امانت دیجیتال کنترل‌شده، قفل نرم‌افزاری، آب‌نقش پنهان، اقدامات کنترل کپی برای خوانش کتاب‌های الکترونیک، رمزگذاری p2p2، سیستم درهم‌سازی محتوا (سی‌اس‌اس)، دسترسی تصادفی و محدود به فراداده در سامانه‌ها، ریزدانگی برای قالب‌های متنی و صوتی و ویدیوئی، ذره‌بین مجازی، مهر زمانی (استامپ زمانی)، استگانوگرافی، پردازش زبان طبیعی در پردازش فایل‌های صوتی و ویدیوئی، دیتا استریمینگ برای فایل‌های ویدیوئی، سیستم کشف کپی، کنترل‌های دسترسی زمانی، حذف فراداده منابع ممنوعه از نمایه پایگاه داده، امکان استفاده از نمایش در لحظه و کد کردن یوآرال، برای کنترل کپی در سامانه‌های مذکور در حال حاضر استفاده نمی‌شود.

همچنین ارزیابی سایر شاخص‌ها نشان داد که از مجوز کریتیو کامنز بدون محدودیت برای دسترسی به اطلاعات کتابشناختی استفاده می‌شود؛ ضمن اینکه پروتکل OAuth و قراردادهای هوشمند در جامعه مورد بررسی به‌کار نرفته است. شاخص پروتکل‌های انتقال امن SSL یا TLS در HTTPs و گواهینامه امنیتی که در انتقال امن اطلاعات نقش دارد، در سامانه‌های یادشده به‌کار نرفته است. تنها از HTTPs در سامانه‌های فوق استفاده شده است. همین‌طور در ارزیابی سایر شاخص‌ها که به حفاظت دیجیتال مربوط می‌شد نیز شاخص شناساگر شیء دیجیتال و مدل مرجع سیستم اطلاعاتی آرشیوی باز استفاده نشده است. همچنین فناوری HDCP برای حفاظت از محتواهای دیداری-شنیداری در سامانه‌های مورد مطالعه به‌کار نرفته است.

برخی دیگر از شاخص‌ها بیشتر به بهره‌گیری از چارچوب‌ها و استانداردها در سامانه‌های فوق اختصاص داشت. یافته‌ها نشان داد که از فریم‌ورک‌ها (مانند مایکروسافت، لاراول) برای اعمال اقدامات امنیتی در سامانه‌های مورد مطالعه، از استاندارد «اُدبلیوایِ‌اس‌تی» برای پیاده‌سازی الزامات فنی، از استاندارد «اس‌ایِ‌ام‌ال» برای ایمن‌سازی سرویس‌دهنده‌ها و SSO، از استانداردهایی مانند ISO- IEC 27001, BS 7799, PCIDSS, ITIL, COBIT، معاهدات اینترنتی کپی‌رایت WPPT و WCT، تدوین سیاست‌های مدیریت امنیت اطلاعات برای حفاظت از منابع دیجیتال و سیاست‌گذاری داده و از استاندارد «متس» استفاده نمی‌شود. ضمن اینکه همانند سامانه‌های دیجیتال از استانداردهای فراداده‌ای دوبلین‌کور در سامانه‌های کتابشناختی استفاده می‌شود.

تحلیل و ارزیابی سامانه‌های مورد مطالعه با سایر شاخص‌ها نیز نشان داد که در حال حاضر از راه‌حل‌های اینترنت اشیا، مدل مرجع سیستم اطلاعاتی آرشیوی باز (اُایِ‌آی‌اس)

در مخزن دیجیتال، بهره‌گیری از مخزن دیجیتال برای مدیریت بهتر مجموعه‌های دیجیتال، فراداده حقوقی و کپی‌رایت، و سیستم‌های پرداخت استفاده نمی‌شود.

با توصیف بیان‌شده، از ۶۹ شاخص الزامات فنی پیشگیرانه که نام برده شد، ۱۴ شاخص (۲/ ۲۰ درصد) رعایت شده و ۵۵ شاخص (۷۹/۷ درصد) در سامانه‌های مورد مطالعه استفاده نشده است (جدول ۷).

جدول ۷. فراوانی شاخص‌های فنی رعایت کپی‌رایت در سامانه‌های کتابشناختی تحت بررسی

ابعاد	شاخص‌ها	فراوانی		سطح‌بندی سامانه‌ها		
		بلی	خیر	ضعیف (۰-۲۳)	متوسط (۲۴-۴۶)	قوی (۴۷-۶۹)
الزامات فنی پیشگیرانه	۶۹	۱۴ (۲۰/۲ درصد)	۵۵ (۷۹/۷ درصد)	✓	-	-

پس از بررسی و ارزیابی سامانه‌های مورد مطالعه با شاخص‌های فنی که پیش‌تر بیان شد، سطح‌بندی سامانه‌ها نیز با توجه به وضعیت سامانه‌ها انجام شد. بدین ترتیب، بعد الزامات فنی پیشگیرانه با امتیاز ۱۴ در سطح ضعیف قرار گرفت.

۴-۲. چارچوب پیشنهادی الزامات فنی به‌منظور حفاظت از کپی‌رایت منابع اطلاعاتی در سامانه‌های مورد مطالعه

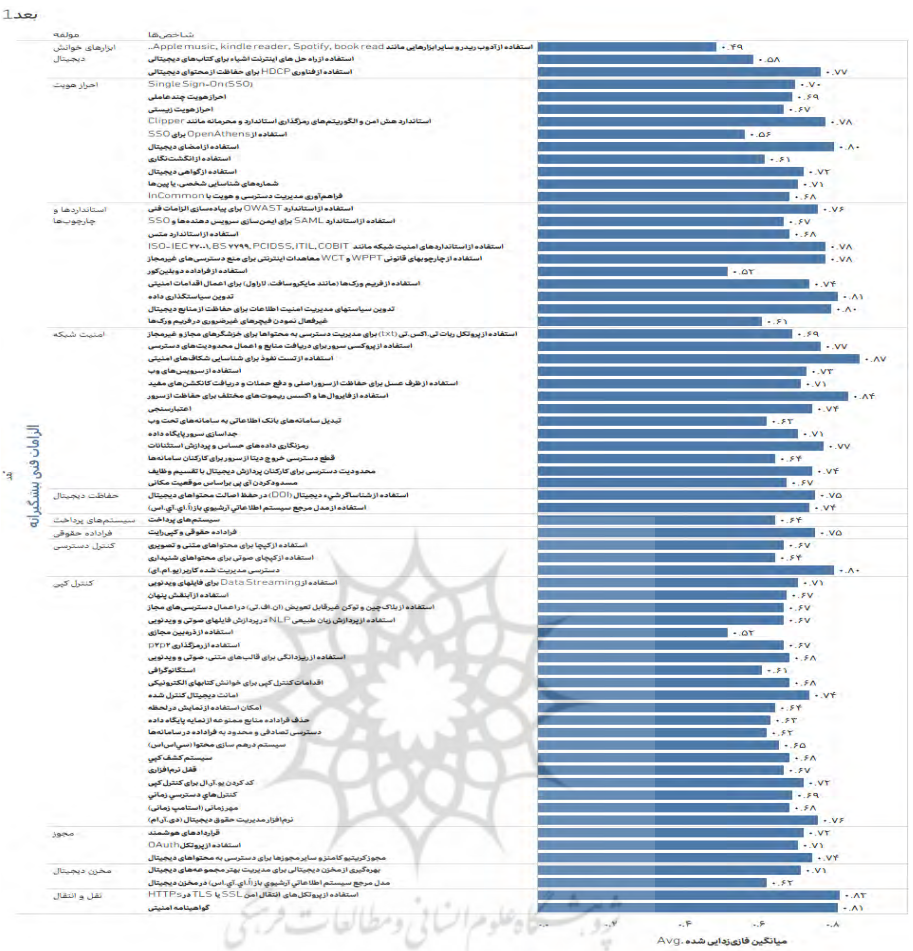
یافته‌های حاصل از روش دلفی فازی

در روش دلفی فازی که حالت غربالگری دارد، متغیرهایی تأیید می‌شوند که حداقل توافق روی آن‌ها ۵۰ درصد باشد. در دور اول، میانگین فازی تنها یک شاخص کمتر از ۰/۵ بود و شاخص «استفاده از آدوب ریدر و سایر ابزارها ...» حذف شد. در مرحلهٔ دوم نظرسنجی، نظرهای قبلی هر خبره و میزان اختلاف آن‌ها با دیدگاه سایر خبرگان، همراه با یک پرسشنامه بار دیگر برای اعضای گروه خبره ارسال شد. تحلیل دلفی فازی برای تمام شاخص‌های پذیرفته‌شده، در دور دوم ادامه پیدا کرد. در این دور ۶۹ شاخص بر اساس دیدگاه ۱۱ خبره مورد ارزیابی مجدد قرار گرفت.

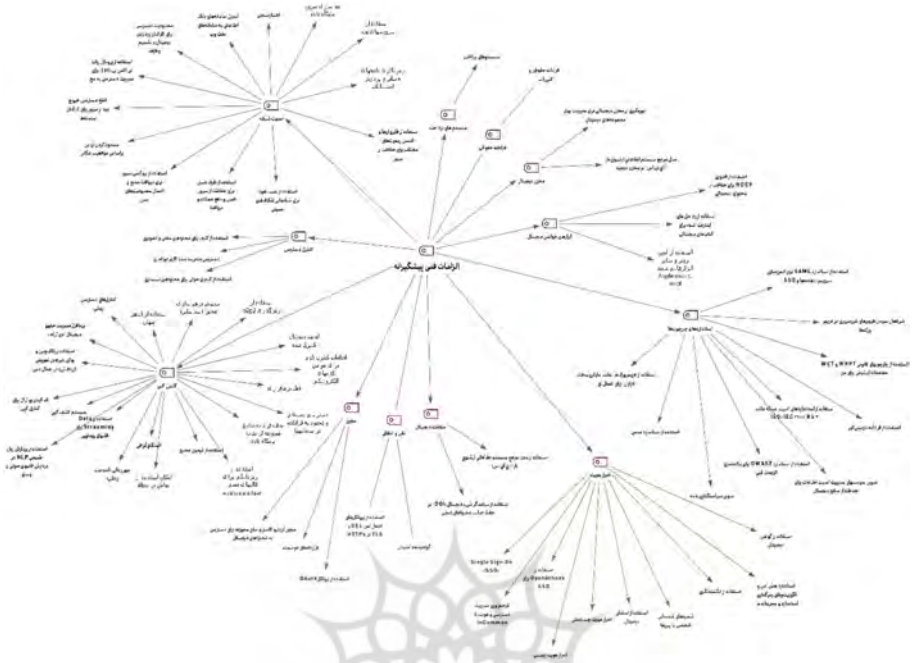
بر اساس نتایج به‌دست‌آمده مشخص شد که در تمامی موارد اختلاف کوچک‌تر از ۰/۲ است. بنابراین می‌توان دورهای دلفی را به پایان برد و نتیجه گرفت که از ۷۰ شاخص مورد بررسی ۶۹ شاخص از نظر ۱۱ نفر خبره از اعتبار لازم برخوردار است. همان‌طور

کـه در نمـودار ۱، قابـل مشـاهده اسـت، بـر اسـاس نظـر خبـرگان و میانگیـن فازی‌زدایی‌شـده (بیشـتر از ۰/۵) ۱۲ مؤلفـه و ۶۹ شـاخص به‌عنـوان الزامـات فنـی پیشـگیرانه شناسـایی شـدند. ۱۲ مؤلفـه امنیـت شـبکه، اسـتانداردها و چارچوب‌هـا، احـراز هویـت، ابزارهـای خوانـش دیجیتـال، حفاظـت دیجیتـال، سیسـتم‌های پرداخـت، فـراداده حقوقـی، کنتـرل دسترسـی، کنتـرل کپـی، مجـوز، مخـزن دیجیتـال، و نقل‌وانتقـال چارچـوب فنـی پیشـنهادی را شـکل می‌دهنـد. از میـان مؤلفه‌هـای ذکرشـده، اسـتفاده از شـاخص HTTPs کـه در مؤلفـه نقل‌وانتقـال تعریـف شـده، بـا میانگیـن فازی‌زدایی‌شـده ۰/۸۱ بیشـترین امتیـاز را دارا هسـتند. در مؤلفـه نقل‌وانتقـال اسـتفاده از ssl و گواهینامـه امنیتـی نیـز تعریـف شـده اسـت. طبـق نظـر مدیـر سـامانه‌های دیجیتـال از گواهینامـه امنیتـی و ssl در سـامانه‌های فـوق اسـتفاده می‌شـود، امـا بـا بررسـی انجام‌شـده[1] توسـط پژوهشـگر، گواهینامـه امنیتـی بـرای هیچ‌یـک از سـامانه‌های دیجیتـال و کتابشـناختی بـه‌کار نرفتـه اسـت. بـا توجـه بـه ارتبـاط مؤلفه‌هـا و شـاخص‌های الزامـات فنـی در کنـار هـم، در شـکل ۱، چارچـوب فنـی بـرای حفاظـت از کپی‌رایـت در سـامانه‌های در دسـت بررسـی ترسـیم و پیشـنهاد شـده اسـت.

۱. ضمن بررسی یوآرال، در پورتال زیر تمامی یوآرال‌های سامانه‌ها نیز چک شد:
https://www.sslshopper.com/ssl-checker.html#hostname=https://dl.nlai.ir/ui/forms/index.aspx



نمودار ۱. مؤلفه‌ها و شاخص‌های فنی مربوط به الزامات فنی پیشگیرانه (مستخرج از نظر خبرگان)



شکل ۱. چارچوب پیشنهادی الزامات فنی برای رعایت کپی‌رایت در سامانه‌های اطلاعاتی «سازمان اسناد و کتابخانه ملی ایران»

۵. بحث و نتیجه‌گیری

در پژوهش حاضر برای شناسایی الزامات فنی حفاظت از کپی‌رایت در سامانه‌های اطلاعاتی «سازمان اسناد و کتابخانه ملی ایران» و سپس ارزیابی سامانه‌ها، از روش‌های تحلیل اسنادی، تحلیل مضمون و دلفی فازی بهره گرفته شد. اعتبارسنجی شاخص‌های فنی با تکنیک دلفی فازی انجام شد. سپس سامانه‌های دیجیتال و کتابشناختی مورد مطالعه با استفاده از سیاهه وارسی تحلیل و ارزیابی شدند. نتایج بیانگر آن است که زبان مشترک برنامه‌نویسی هر دو دسته سامانه، «جاوا»ست. «جاوا» از جمله زبان‌های برنامه‌نویسی همه‌منظوره‌ای است که از امنیت برخوردار است (Skalka 2005). از دو سیستم‌عامل «لینوکس» و «ویندوز» در سامانه‌های اطلاعاتی کتابشناختی و دیجیتال استفاده می‌شود. انتخاب نوع سیستم‌عامل با توجه به کاربرد، نیازها و شرایط استفاده متفاوت است و نمی‌توان به‌طور دقیق پیشنهاد داد که در سامانه‌های یادشده، از «لینوکس» استفاده شود یا از «ویندوز».

اما در هر جهت تفاوت‌هایی بین دو سیستم‌عامل از نظر حفاظت از سامانه‌ها در برابر تهدیدات وجود دارد. می‌توان گفت «لینوکس» برای استقرار سرور مناسب است. همچنین در «ویندوز» دسترسی پیش‌فرض مدیر سیستم خطر امنیت را افزایش می‌دهد، در حالی که ماهیت منبع باز بودن «لینوکس»، امکان رفع خطر را زودتر فراهم می‌کند. گفتنی است در حالی که از نظر ویژگی‌های امنیتی تفاوت‌های زیادی بین دو سیستم‌عامل وجود دارد، اما هر دو برای بهبود خود به تکامل و توسعه ادامه می‌دهند (Albatli et al. 2023). همان‌طور که یافته‌ها نشان داد، سامانه‌های مورد گفت‌وگو از نظر بهره‌گیری از الزامات فنی پیشگیرانه برای رعایت کپی‌رایت در سطح ضعیفی قرار دارند. شاید به سامانه‌های کتابشناختی مورد بررسی به‌دلیل ارائه اطلاعات صرفاً کتابشناختی در حال حاضر نتوان ایرادی گرفت، اما از سامانه‌های دیجیتال که دربردارنده کتابخانه دیجیتال و نشریات ایران است، انتظار بیشتری در استفاده از الزامات فنی پیشگیرانه برای حفاظت از کپی‌رایت وجود دارد. نتایج این پژوهش با پژوهش «حریری و نظری» (۱۳۹۱) مبنی بر قابل قبول بودن مؤلفه‌های امنیت در سامانه دیجیتال ملی همسو نیست. ذکر این نکته ضروری است که در خصوص توسعه سامانه‌های کتابشناختی نیز می‌بایست الزامات فنی مورد نیاز برای رعایت کپی‌رایت مد نظر قرار گیرد.

به‌طور کلی، سامانه‌های مورد بررسی نتوانستند در ارزیابی شاخص‌های فنی امتیاز لازم را کسب کنند. شاید به همین دلیل در پژوهش «آموزگار، نوروزی و صراف‌زاده» (۱۴۰۱) چالش‌های فناوری حفاظتی برای حق مؤلف منابع دیجیتال مهم قلمداد می‌شود. بر اساس نتایج پژوهش از نظر خبرگان، ۱۲ مؤلفه و ۶۹ شاخص به‌عنوان الزامات فنی پیشگیرانه شناسایی شد. امنیت شبکه، استانداردها و چارچوب‌ها، احراز هویت، ابزارهای خوانش دیجیتال، حفاظت دیجیتال، سیستم‌های پرداخت، فراداده حقوقی، کنترل دسترسی، کنترل کپی، مجوز، مخزن دیجیتال، و نقل‌وانتقال، ۱۲ مؤلفه الزامات فنی پیشگیرانه هستند که برای حفاظت از کپی‌رایت در سامانه‌های اطلاعاتی اعتبارسنجی و تأیید شدند و چارچوب فنی پیشنهادی را شکل دادند (شکل ۱). می‌توان اذعان داشت که الزامات فنی پیشگیرانه‌ای که در پژوهش کنونی از نظر خبرگان مورد توافق و تأیید قرار گرفته با پژوهش‌ها و نظرات ارائه‌شده، مانند: Keplinger (2001)؛ Conroy (2006)؛ Crews (2008)؛ European Commission (2011)؛ Hassanein& Ghinea (2013)؛ Stabingis, Sarlauskiene and Cepaitiene (2014)؛ Abu Sirhan and et al. (2019)؛ Huiming (2021)؛ «تقوا و ایزدی» (۱۳۹۲)؛

«پاپی» (۱۳۹۴)؛ «کوکبی و کوهی رستمی» (۱۳۹۴)؛ «رحمانی» (۱۳۹۰)؛ «آقاسیدجوادی و علیپور حافظی» (۱۳۹۵) همخوانی داشته و تأیید می‌شود. از جمله شاخص‌های فنی مهم و البته قابل توجه که کتابخانه‌ها در ارتباط با ناشران و کاربران باید به آن توجه بیشتری کنند، استفاده از سرور «پروکسی» است که در سامانه‌های مورد بررسی استفاده نمی‌شود، اما در مصاحبه با یکی از متخصصان خارج از کشور بر آن تأکید شد.

"If we are cataloging a resource that is provided by an external publisher, a cataloger might link to the resource through our proxy server (which requires university authentication) and optionally note the access restriction in the catalog description" (Code 2).

سرور «پروکسی» خدماتی است که کتابخانه‌ها برای احراز هویت کاربران خود برای دسترسی به بسیاری از پایگاه‌های داده‌ای برخط و پورتال‌های ناشران از آن استفاده می‌کنند. کتابخانه‌ها با IP ناشر و کاربر، وی را احراز هویت می‌کند (Day 2017). نمونه‌ای از به‌کارگیری پروکسی‌سرور در« اُسی‌ال‌سی»[1] با استفاده از EZproxy انجام می‌شود. این سرویس به کتابخانه‌ها اجازه می‌دهد که منابع الکترونیکی را بدون توجه به مکان و زمان جست‌وجو به‌سادگی و به‌گونه‌ای ایمن به کاربران ارائه دهند. هزاران کتابخانه در بیش از ۱۰۰ کشور از EZproxy برای تسهیل دسترسی ایمن و قابل اعتماد به منابع الکترونیکی استفاده می‌کنند. ضمن اینکه همین سرویس، دسترسی مداوم به منابع الکترونیک را بدون اینکه نیاز به به‌خاطرسپاری رمزهای عبور و نام‌های کاربری متعدد باشد، به کاربران ارائه می‌دهد (OCLC 2023). همچنین از میان مؤلفه‌های ذکرشده در نقل‌وانتقال، از شاخص HTTPs در سامانه‌ها استفاده شده است. در مؤلفه نقل‌وانتقال استفاده از ssl و گواهینامه امنیتی نیز تعریف شده است. طبق نظر مدیر سامانه‌های دیجیتال از گواهینامه امنیتی و ssl در سامانه‌های فوق استفاده می‌شود، اما با بررسی انجام‌شده توسط پژوهشگر، گواهینامه امنیتی برای هیچ‌یک از سامانه‌های دیجیتال و کتابشناختی به‌کار نرفته است. به این موضوع به‌دلیل اهمیت آن، در مصاحبه با یکی از متخصصان خارج از کشور در حوزه کتابخانه‌های دیجیتال و سامانه‌های اطلاعاتی اشاره می‌شود:

*"Authentication is done over secure channels (such as SSL), so credentials do not get stolen. We also, like many other organizations on the Internet, have shifted towards making *all* online communications, not just authentication, go over secure channels when possible (such as https rather than http) to prevent eavesdropping; content alteration, or other attacks" (code 2).*

1. Online Computer Library Center (OCLC)

یکی دیگر از شاخص‌های فنی که در سامانه‌های دیجیتال و در توسعه سامانه‌های کتابشناختی می‌تواند به حفاظت از کپی‌رایت و حقوق پدیدآورندگان آثار کمک کند، ریزدانگی است. استفاده از قطعه‌بندی (سگمنت کردن)[1] فایل‌ها می‌تواند تا حدود زیادی خطر نقض حقوق پدیدآورندگان را تقلیل دهد. این امر با توسعه و روزآمد نگه‌داشتن سامانه‌ها به‌ویژه برای محتواهای صوتی و ویدیوئی امکان‌پذیر است؛ هرچند پیاده‌سازی برخی از الزامات فنی مانند ریزدانگی در مخزن دیجیتال به حفظ دارایی‌های دیجیتال در زمینه مدیریت امنیت، فراداده، حقوق کاربر، پدیدآور و مدیریت دسترسی کمک خواهد نمود (Rathje et al. 2005).

با تمام توصیفاتی که بیان شد، شاخص‌های پیش‌گفته می‌توانند در آینده برای توسعه سامانه‌های دیجیتال (از جمله کتابخانه دیجیتال ملی، نشریات ایران (سنا) و نشریات علمی ایران) مفید باشند. همچنین شاخص‌های پیشنهادشده می‌توانند جایگاه فعلی سامانه‌های کتابشناختی (از جمله بانک نشریات ایران، شبکه مراکز اسناد کشور، فهرستگان نسخ خطی و شبکه کتابخانه‌های کشور) را ارتقا داده و همراستا با اقدامات قانونی، الزامات فنی را به‌منظور رعایت کپی‌رایت در سامانه‌ها در پیش گیرند؛ ضمن اینکه چارچوب فنی پیشنهادی می‌تواند به همراه امتیازهای هر شاخص در سنجش سایر سامانه‌های مرتبط کمک کند. همچنین «سازمان اسناد و کتابخانه ملی ایران» و سایر کتابخانه‌های دارای سامانه‌های مشابه می‌توانند نسبت به اولویت‌بندی شاخص‌ها به‌منظور پیاده‌سازی آن‌ها در راستای حفاظت از کپی‌رایت و حقوق پدیدآورندگان اقدام کنند. در ادامه، بر اساس یافته‌های پژوهش برخی پیشنهادها به‌شرح زیر ارائه می‌شود:

۱. به‌کارگیری ریزدانگی برای منابع دیجیتال، صوتی و ویدیوئی؛
۲. تدوین سیاست کپی‌رایت برای تمامی منابع دیجیتال و یا استفاده از فراداده حقوقی برای منابع دیجیتال؛
۳. توسعه و روزآمد نگه‌داشتن سامانه‌ها و ارتباط و تعامل با شرکت پشتیبان نرم‌افزار؛
۴. قطع دسترسی خروج دیتا از سرور برای کارکنان سامانه‌ها؛
۵. استفاده از استاندارد «متس»؛
۶. بهره‌گیری از مخزن دیجیتال برای مدیریت بهتر مجموعه‌های دیجیتال؛

1. segmentation

۷. استفاده از «پروکسی‌سرور» برای دریافت منابع و اعمال محدودیت‌های دسترسی؛
۸. استفاده از فناوری بلاک‌چین به‌منظور حفاظت از محتوای اطلاعات دیجیتال و مدیریت کنترل دسترسی؛
۹. برنامه‌ریزی برای تبدیل سامانه‌های بانک اطلاعاتی به دیجیتال و توسعه سامانه‌های کتابشناختی در زمینه ارائه متن کامل کتاب‌های فارسی با مجوز از ناشران و رعایت حقوق پدیدآورندگان محتواها.

قدردانی

مقاله حاضر مستخرج از طرح پژوهشی مصوب شورای پژوهشی «سازمان اسناد و کتابخانه ملی ایران» است که با عنوان «بررسی و تحلیل الزامات فنی حمایت از کپی‌رایت منابع اطلاعاتی در سامانه‌های اطلاعاتی سازمان اسناد و کتابخانه ملی ایران: ارائه راهکارها» در خرداد ۱۴۰۲ به اتمام رسیده است. لازم است از اعضای محترم پنل، مصاحبه‌شوندگان، مدیران سامانه‌ها که در به ثمر رساندن این پژوهش همکاری نمودند، قدردانی کرده و از نظرات و پیشنهادهای ارزشمند داوران محترم سپاسگزاری می‌شود.

فهرست منابع

آقاسیدجوادی، پریچهر، و مهدی علیپور حافظی. ۱۳۹۵. بهره‌گیری از فناوری مدیریت حقوق دیجیتالی در سامانه مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوری اطلاعات ایران. *تعامل انسان و اطلاعات* ۳ (۱): ۲۰-۳۲.

آموزگار، سیما، علیرضا نوروزی، و مریم صراف‌زاده. ۱۴۰۱. تحلیل مسائل و چالش‌های حق مؤلف منابع دیجیتالی متنی از دیدگاه مدیران کتابخانه‌های دیجیتالی شهر تهران. *فصلنامه کتابداری و اطلاع‌رسانی* ۲۵ (۱): ۲۹-۵۹.

پاپی، زینب. ۱۳۹۴. حق مؤلف در فضای سایبری با تأکید بر حقوق مؤلفان در جمهوری اسلامی ایران: ارائه الگوی پیشنهادی جهت اجرای حقوق سایبر مؤلفان پایان‌نامه‌ها در سامانه ملی پایان‌نامه‌ها. رساله دکتری، دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران.

تقوا، محمدرضا، و ماندانا ایزدی. ۱۳۹۲. بررسی امنیت در سیستم‌های اطلاعاتی توسعه‌یافته (SOA) با روش معماری سرویس گرا. *مدیریت فناوری اطلاعات* ۵ (۳): ۲۵-۴۲.

حبیبی، آرش، و صنم آفریدی. ۱۴۰۱. *تصمیم‌گیری چندشاخصه*. تهران: انتشارات نارون.

حریری، نجلا، و زهرا نظری. ۱۳۹۱. امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران. *کتابداری و اطلاع‌رسانی* ۱۵ (۲): ۶۱-۹۰.

رحمانی، سحر. ۱۳۹۰. نظام مدیریت دیجیتال (DRM) و حمایت از آثار ادبی و هنری با استفاده از آن. پایان‌نامه کارشناسی ارشد، دانشگاه قم.

سازمان ملی استاندارد ایران. ۱۳۹۴. *فناوری اطلاعات- فنون امنیتی- سامانه مدیریت امنیت اطلاعات- الزامات: ایزو آی‌ای‌سی ۲۷۰۰۱*. تهران: سازمان ملی استاندارد ایران.

کمالی، یحیی. ۱۳۹۷. روش‌شناسی تحلیل مضمون و کاربرد آن در مطالعات سیاست‌گذاری عمومی. *فصلنامه علمی-پژوهشی سیاست‌گذاری عمومی* ۴ (۲): ۱۸۹-۲۰۸.

کوکبی، مرتضی، و منصور کوهی رستمی. ۱۳۹۴. امنیت اطلاعات سامانه‌های تحت وب نهاد کتابخانه‌های عمومی کشور. *فصلنامه تحقیقات اطلاع‌رسانی و کتابخانه‌های عمومی* ۲۱ (۱): ۸۹-۱۰۷.

مدنی بروجنی، سید احمد، و احمدرضا نصر. ۱۳۸۸. سه‌سوسازی: راهبردی برای نوآوری در پژوهش‌های آموزشی. *فصلنامه نوآوری‌های آموزشی* ۳۰ (۸): ۵۳-۷۳.

نوروزی، علیرضا. ۱۳۸۱. *حقوق مالکیت فکری: حق مؤلف و مالکیت صنعتی*. تهران: نشر چاپار.

نوروزی، یعقوب. ۱۳۹۰. محورهای توسعه کتابخانه‌های دیجیتالی. *فصلنامه تحقیقات اطلاع‌رسانی و کتابخانه‌های عمومی* ۱۷ (۳، پیاپی ۶۴): ۱۲۹-۱۵۳.

References

Abu Sirhan, A., K. M. Abdrabbo, S. Ahmed Ali Al Tawalbeh, M. Hamdi Ahmed, and M. Ali Helalat. 2019. Digital rights management (DRM) in libraries of public universities in Jordan", *Library Management* 40 (8/9): 496-502. https://doi.org/10.1108/LM-05-2018-0044 (accessed November 24, 2021).

Albatli, L, S. Aldossary, F. Almhdood, B. Alhothail, M. Alshimer, Sh. Alotaibi, R. Iqahtani, et al. 2023. Comparison between Windows and Linux Operating System by Analyzing the Related Security Features. *Journal Not Specified*. https://www.mdpi.com/journal/notspecified (accessed June 23, 2023).

Batt, S., T. Grealis, O. Harmon, & P. Tomolonis. 2020. Learning Tableau: A data visualization tool, *The Journal of Economic Education* 51:3-4, 317-328, DOI: 10.1080/00220485.2020.1804503 (accessed November 5, 2022).

Conroy, M. 2006. A comparative study of technological protection measures in copyright law. PhD diss., University of South Africa.

Crews, K. 2008. Study on copyright limitations and exceptions for libraries and archives. Presented at 17th STANDING COMMITTEE ON COPYRIGHT AND RELATED RIGHTS, WIPO. Geneva.

Day, J. M. 2017. Proxy Servers: Basics and Resources. https://libtechlaunchpad.com/2017/04/25/proxy-servers-basics-and-resources/ (accessed June 17, 2023).

Digital Rights Management and Technical Protection Measures. 2006. https://www.priv.gc.ca/resource/fs-fi/02_05_d_32_e.asp (accessed November 24, 2021).

European Commission. 2011. *Information System Security Policy C (2006) 3602: STANDARD ON ACCESS CONTROL AND AUTHENTICATION*. https://b2n.ir/a06212 (accessed November 13, 2022).

Hassanein, M. S., & Gh. Ghinea. 2013. Fingerprint Scheme for Digital Text. *International Journal Multimedia and Image Processing (IJMIP*) 3 (3/4), DOI:10.20533/ijmip.2042.4647.2013.0021 (accessed 27 August. 2022).

Huiming, Ch. 2021. Research on Limitations and Exceptions of Technical Measures for Long-term Preservation of Library Digital Resources: Considerations Based on the “Technical Path” of Copyright Protection [J]. *Libraly Journal* 40 (1): 48-56.

Jean-Mary, Ch. 2020. An Overview of X.509 Certificates, https://www.ibm.com/support/pages/system/files/inline- files/An_Overview_of_x.509_certificates.pdf (accessed November 24, 2021).

Keplinger, M. 2001. Part 1: Technological Measures for Protection of and Related Rights on the Internet-Present and Future Technologies, Part II: Enforcement of copyright and Related Rights in Digital Networks, the Technology and Its possibilities for Infringement and Surveillance. The Enforcement Rules under the WCT and the WPPT. Presented at Regional Workshop for countries of Asia and the Pacific on the WIPO Internet Treaties and Electronic commerce by WIPO. Manila.

OCLC. 2023. Streamline and secure access to e-resources. https://www.oclc.org/en/ezproxy.html (accessed June 17, 2023).

Rathje, B. D, M. McGrory, C. Pollitt, & P. Voutilainen. 2005. Designing and Building Integrated Digital Library Systems – Guidelines. IFLA Professional Reports. International Federation of Library Associations and Institutions. https://b2n.ir/u07812 (accessed June 25, 2023).

Skalka, Ch. 2005. Programming languages and systems security. *THE IEEE COMPUTER SOCIETY*. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1439509 (accessed June 5, 2023).

Stabingis, L., L. Šarlauskiene, N. and Čepaitien. 2014. Measures for plagiarism prevention in students’ written works: case study of ASU experience. *Procedia - Social and Behavioral Sciences* 110 (2014): 689 – 699.

Technological Protection Measures and the Copyright Amendment Act 2006. The Official Guide to Copyright Issues for Australian Schools and TAFE.

www8.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/num_act/caa2006213/sch12.html (accessed November 5, 2023).

Wazirali, R., R. Ahmad, A. Al-Amayreh, M. Al-Madi, and A. Khalifeh. 2021. Secure Watermarking Schemes and Their Approaches in the IoT Technology: An Overview. *Electronics 2021*, 10, 1744. https:// doi.org/10.3390/electronics10141744 (accessed November 24, 2021).

زینب پاپی

متولد سال ۱۳۶۱، و دارای مدرک تحصیلی دکتری در رشته علم اطلاعات و دانش‌شناسی است. ایشان هم‌اکنون استادیار گروه پژوهشی مدیریت اطلاعات و سازماندهی دانش، سازمان اسناد و کتابخانه ملی ایران است.

کپی‌رایت، حقوق دیجیتال، کتابخانه دیجیتال، فراداده و روش‌شناسی پژوهش کیفی از جمله علایق پژوهشی وی است.

پژوهش‌نامه
پردازش و مدیریت اطلاعات