Library and Information Sciences
Print ISSN: 1680-9637
Online ISSN: 5977-2676

Identification and Analysis of Technical Threats Affecting the Copyright Protection of Information Resources in the Information Systems of Libraries: Case Study of the National Library and Archives of Iran (NLAI)

Zeinab Papi
Assistant Professor, Information Management and Knowledge Organization Department, National Library and Archives of Iran (NLAI), Tehran, Iran. E-mail: zeinab.papi12@gmail.com

Abstract

Objective: The purpose of current research is to identify technical risks and threats to copyright protection of information resources in the systems examined in order to prevent the infringement of the rights of creators of information resources by identifying technical risks.

Methodology: Current research is applied, and a qualitative approach was used to collect needed data. In the qualitative approach, according to the purpose and problem of the research, methods of documentary analysis, thematic analysis and Fuzzy Delphi were used. 11 specialists and experts participated in the Delphi panel and 6 experts for interview; and 7 information systems in the National Library were selected as research community. In data analysis, MAXQDA and Tableau software were used.

Findings: Using the thematic analysis method, 17 indicators were obtained in 8 components related to technological threats to copyright protection in the systems studied. Following confirmation and finalization of the checklist using the Fuzzy Delphi method, 16 indicators in 7 components related to technical risks were approved by experts.

Deliberate employee sabotage, weak server resources, miscellaneous malware such as viruses, worms, etc., not having back up the main program, not having a mirror website (network security); Loss of equipment and infrastructure support (such as inability to develop software or loss of software support team); The weakness of DRM in duplication and long-term protection of works, the lack of DRM software in the systems, Lack of updated systems and problems in the construction of storage space (technical infrastructure); Use of clear watermark (copy control); URL tampering (digital protection); Not using authentication for all content sections and pages (authentication); Not define the copyright policy in the digitization process (rights metadata); Lack of quality control of digital content and lack of attention to the stages of digital object preparation (digitalization process) are among the effective technical threats in the studied systems. After identifying the indicators, in May 2023, the systems were evaluated from the perspective of technical risks to protect the copyright of information sources. The studied systems were placed in two groups, digital and bibliographic, according to the type of activity, their

structure and function. The Digital Library system, Iranian Newspaper System (SANA) and Iranian Scientific Publications System are included in the digital category. Other systems, i.e., National libraries network, National document center network, Iran Publications database, Manuscript database are included in the bibliographic category. Bibliographic systems only provide bibliographic information and are considered a type of database. In general, the findings showed that none of the 16 technical risk indicators have been observed in the studied systems.
Conclusion: Paying attention to technical considerations to protect the copyright of information sources in the systems can be described as the basis of the development and expansion of the systems in the libraries.

Keywords: technical threats, information systems, copyright, National Library and Archives of Iran

Article type: Research

How to cite:
Papi, Z. (2023). Identification and Analysis of Technical Threats Affecting the Copyright Protection of Information Resources in the Information Systems of Libraries: Case Study of the National Library and Archives of Iran (NLAI). *Library and Information Sciences*, 26(4), 5-32.

A R T I C L E I N F O

Article history:
Received: 09/10/2022 Received in revised form: 30/10/2023
Accepted: 09/11/2023 Available online: 17/03/2024

Publisher: Central Library of Astan Quds Razavi
Library and Information Sciences, 2023, Vol. 26, No. 4, pp. 5-32.

کتابداری و اطلاع رسانی

شاپا چـاپـی: ۹۶۳۷-۱۶۸۰
شاپا الکترونیکی: ۲۶۷۶-۵۹۷۷

شناسایی و تحلیل تهدیدات فنی اثرگذار بر حفاظت از کپی‌رایت منابع اطلاعاتی در سامانه‌های اطلاعاتی کتابخانه‌ها: مورد مطالعه سازمان اسناد و کتابخانه ملی ایران

زینب پاپی
دکتری علم اطلاعات و دانش‌شناسی، استادیار گروه پژوهشی مدیریت اطلاعات و سازماندهی دانش، سازمان اسناد و کتابخانه ملی ایران، تهران، ایران. رایانامه: zeinab.papi12@gmail.com

چکیده

هدف: هدف پژوهش کنونی، شناسایی مخاطرات و تهدیدات فنی اثرگذار بر حق مؤلف منابع اطلاعاتی در سامانه‌های مورد مطالعه است.

روش پژوهش: پژوهش کنونی از نظر هدف کاربردی است و برای گردآوری داده‌ها از رویکرد کیفی و روش‌های تحلیل اسنادی، تحلیل مضمون و دلفی فازی استفاده شد. برای کشف بهتر مفاهیم، با ۶ نفر از متخصصان حوزه‌های سامانه‌های اطلاعاتی، حق مؤلف و کتابخانه‌های دیجیتالی مصاحبه انجام شد. در تحلیل مضمون برای کشف مضامین، کدگذاری از داده‌ها انجام شد. در روش دلفی فازی، پنل در دو دور انجام شد، ۱۱ نفر خبره و متخصص انتخاب شدند. برای ترسیم داده‌ها، نسخه ۲۰۲۰ نرم‌افزار مکس.کیو.دی.ای و نرم‌افزار تبلو نسخه ۲۰۱۸ استفاده شد.

یافته‌ها: خرابکاری عمدی کارکنان، پایین بودن منبع سرورها، بدافزارهای مختلف مانند ویروس‌ها، کرم‌ها و مانند آن، نداشتن پشتیبان از برنامه اصلی، نداشتن وبگاه آینه‌ای (امنیت شبکه)؛ ضعف و نقصان دی.آر.ام (DRM) در نسخه‌برداری و حفاظت طولانی مدت از آثار، روزآمد نبودن سامانه‌ها و مشکل در فضای ذخیره‌سازی (زیرساخت فنی)؛ دستکاری‌کردن یو آر ال (حفاظت دیجیتال)؛ استفاده نکردن از احراز هویت برای تمام بخش‌ها و صفحات محتوا (احراز هویت)؛ نبود کنترل کیفی محتواهای دیجیتالی و کم‌توجهی به مراحل آماده‌سازی شیء دیجیتالی (فرایند دیجیتال‌سازی) از جمله تهدیدات فنی اثرگذار در سامانه‌های مورد مطالعه محسوب می‌شوند.

نتیجه‌گیری: تحلیل حاصل از ارزیابی سامانه‌ها در خصوص مخاطرات فنی تأثیرگذار بر حق مؤلف منابع اطلاعاتی در سامانه‌های مورد مطالعه نشان‌دهنده کمرنگ بودن توجه به پیشگیری از خطرات فنی پیرامون حفاظت از حقوق پدیدآورندگان و ذینفعان آثار در سامانه‌هاست. چرا که اقدامات قانونی و تصویب قوانین حق مؤلف تنها بخشی از حمایت‌های قانونی از پدیدآورندگان آثار را پوشش می‌دهد؛ بخشی دیگر، مربوط به اقدامات فنی و پیشگیری از تهدیدات فنی است که نبود آن‌ها نیز نقض حق مؤلف منابع اطلاعاتی در سامانه‌های اطلاعاتی را به همراه دارد.

کلیدواژه‌ها: تهدیدات فنی، سامانه‌های اطلاعاتی، منابع اطلاعاتی، حق مؤلف، سازمان اسناد و کتابخانه ملی ایران

نوع مقاله: پژوهشی

استناد:
پاپی، زینب (۱۴۰۲). شناسایی و تحلیل تهدیدات فنی اثرگذار بر حفاظت از کپی‌رایت منابع اطلاعاتی در سامانه‌های اطلاعاتی کتابخانه‌ها: مورد مطالعه سازمان اسناد و کتابخانه ملی ایران. *کتابداری و اطلاع‌رسانی*، ۲۶(۴)، ۵-۳۲.

تاریخچه مقاله:
تاریخ دریافت: ۱۴۰۲/۷/۱۷ تاریخ ویرایش: ۱۴۰۲/۸/۸ تاریخ پذیرش: ۱۴۰۲/۸/۱۸ تاریخ انتشار: ۱۴۰۲/۱۲/۲۷

ناشر: کتابخانه مرکزی آستان قدس رضوی
کتابداری و اطلاع‌رسانی، ۱۴۰۲، دوره ۲۶، شماره ۴، شماره پیاپی ۱۰۴، صص. ۵-۳۲.

۱. پژوهش حاضر برگرفته از طرح پژوهشی موظف پژوهشگر در شورای پژوهشی سازمان اسناد و کتابخانه ملی ایران مصوب خرداد ۱۴۰۱ 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.

مقدمه

دیجیتالی شدن، مفاهیم سنتی قانون حق مؤلف مانند دسته‌بندی آثار مختلف از جمله چندرسانه‌ای‌ها را به چالش کشیده است. انتقال بی‌وقفه آثار دیجیتال و سهولت تکثیر آثار به شکل دیجیتال، چالش‌های مبهمی را برای قانون حق مؤلف ایجاد می‌کند. نگرانی‌های مربوط به تأثیر دیجیتالی شدن بر قانون حق مؤلف چنان بود که منجر به تصویب برخی معاهدات مانند معاهده حق مؤلف وایپو[1]توسط سازمان جهانی مالکیت فکری (وایپو)[2] در سال ۱۹۹۶ شد. از جمله ویژگی این معاهده، حق ارتباط با عموم،[3] حق دسترسی،[4] مدیریت اطلاعات حقوق[5] و مقررات ضد دورزدن[6] را می‌توان اشاره کرد (پیستاریوس و اموِیم،[7] ۲۰۱۹). اجرای چنین معاهده‌ای در محیط دیجیتال، نیازمند استفاده از اقدامات حفاظتی فناورانه است.

اقدامات حفاظتی فناورانه[8] برای آثار حق مؤلف به شکل دیجیتال برای جلوگیری از نقض اثر اعمال می‌شود. دور زدن این اقدامات غیرقانونی است (پیستاریوس، اموِیم، ۲۰۱۹). بنابراین، ظهور اینترنت و پیشرفت فناوری‌های چندرسانه‌ای موجب متنوع‌تر شدن محتوای سامانه‌های اطلاعاتی شد. امروزه ذخیره، مبادله و بازیابی اطلاعات چندرسانه‌ای در سامانه‌های اطلاعاتی، به یک امر متداول تبدیل شده است. سامانه‌های اطلاعاتی وب-پایه بیشتر از سایر سامانه‌ها با محتواهای چندرسانه‌ای عجین شده‌اند. البته در مقطع کنونی با ظهور فناوری‌های جدید مانند متاورس، مسائلی همچون مالکیت معنوی و امنیت محتوا گریبان‌گیر سامانه‌های اطلاعاتی شده است (حسن‌زاده، ۱۴۰۱). به همین ترتیب، در کنار قوانین و معاهداتی که برای حفاظت از آثار در محیط دیجیتال وجود دارد، استفاده از اقدامات فناورانه و ترکیب حقوق و فناوری می‌تواند فضای دیجیتال را قانونمند کند.

با توصیفی که بیان شد، یکی از موضوعات اصلی در حوزه فناوری دیجیتال، نقض آثار دیجیتال است که می‌تواند به حقوق صاحبان داده‌ها آسیب جدی وارد کند و بر اشتیاق صاحبان آن‌ها برای خلق اثر اصلی تأثیر بگذارد. بنابراین، برای حمایت از حق مؤلف آثار در محیط دیجیتال به توجه بیشتری نیاز است، زیرا بر توسعه جامعه تأثیرگذار است. بسیاری از اقدامات حفاظتی فناورانه در حمایت از حق مؤلف در محیط دیجیتال در گذشته و تاکنون توسعه یافته‌اند (لیو، جانگ، وو و پاتهان،[9] ۲۰۲۱)، اقدامات فناورانه‌ای نظیر گواهینامه

1. WIPO Copyright Treaty (WCT)
2. World Intellectual Property Organization (WIPO)
3. Right of communication to the public
4. Available right
5. Management of rights information
6. Anti-circumvention provisions
7. Pistorius & Mwim
8. Technological protection measures (TPMs)
9. Liu, Zhang, Wu & Pathan

دیجیتال[1] ته‌نقش دیجیتال[2] فناوری بلاک‌چین[3] رمزنگاری[4] پنهان و نظیر آن (جین‌مری[5] ۲۰۲۰؛ پچ[6] ۲۰۲۰؛ وزیرعلی، احمد، آمیره، مادی و خلیفه[7] ۲۰۲۱) تا حدودی می‌تواند از نقض آثار در محیط دیجیتال جلوگیری به عمل آورد، «اما هنوز هم، حفره‌های زیادی در سامانه‌های اطلاعاتی وجود دارد که باید پوشش داده شوند» (لیو، جانگ، وو و پاتهان، ۲۰۲۱). بنابراین، ترکیب حقوق و فناوری می‌تواند حمایت از حقوق پدیدآورندگان آثار و کاربران را به ویژه در سامانه‌های اطلاعاتی کتابخانه‌ها که حاوی منابع مختلف و متنوع اطلاعاتی هستند به همراه داشته باشد. اهمیت سامانه‌های اطلاعاتی در کتابخانه‌ها با توجه به وظایف ذاتی آن‌ها در فراهم‌آوری، سازماندهی و پردازش و اشاعه اطلاعات بر کسی پوشیده نیست. کتابخانه‌ها در نیل به وظایف دیرینه خود همواره در تلاشند تا به بهترین شکل منابع اطلاعاتی در کتابخانه‌ها را در اختیار کاربر به شیوه‌های مختلف قرار دهند. از جمله اقدامات می‌توان به پیاده‌سازی سامانه‌های اطلاعاتی در کتابخانه‌ها اشاره کرد که بسیاری از منابع اطلاعاتی را برای دسترسی به کاربر تحت پوشش قرار می‌دهند. البته به مرور زمان و با استفاده بیشتر، با تهدیدات و خطرات فنی برای حفاظت از حقوق پدیدآورندگان آثار مواجه می‌شوند.

اجرای انواع الزامات فناورانه به منظور پیشگیری از انواع خطرات فنی در حق مؤلف منابع اطلاعاتی سامانه‌ها تأثیرگذار است. سازمان اسناد و کتابخانه ملی ایران با توجه به وظیفه ذاتی و مطابق قانون اساسنامه خود که بر گردآوری، سازماندهی و پردازش، حفاظت و اشاعه اطلاعات تأکید می‌کند، پیاده‌سازی سامانه‌های اطلاعاتی مختلف را با توجه به انواع منابع اطلاعاتی در دستور کار خود قرار داده است. سامانه‌های اطلاعاتی دیجیتال ملی، نشریات ایران (سنا)، نشریات علمی ایران، بانک نشریات ایران، شبکه مراکز اسناد کشور، فهرستگان نسخ خطی و شبکه کتابخانه‌های کشور از این دست محسوب می‌شوند. این سامانه‌ها منابع اطلاعاتی مختلف مانند کتاب، نشریات، پایان‌نامه‌ها و رساله‌ها، نسخ خطی و سنگی، طرح پژوهشی، اسناد و نظیر آن را شامل می‌شوند. بنابراین، سازمان اسناد و کتابخانه ملی ایران با توجه به تنوع منابع اطلاعاتی در سامانه‌های فوق و حفظ حقوق پدیدآور، می‌بایست در شناسایی و پایش مخاطرات فنی برای حق مؤلف منابع اطلاعاتی سامانه‌ها پیش‌قدم شود.

با توجه به این که قوانین حق مؤلف تنها بعد از وقوع نقض آثار کاربرد دارند؛ بنابراین، اهمیت اقدامات فنی در حمایت از حق مؤلف کمتر از قوانین موضوعه در این ارتباط نیست و با توجه به افزایش محتوای دیجیتال در سامانه‌های اطلاعاتی، حمایت از حق مؤلف با به کارگیری اقدامات فنی اهمیت دوچندانی یافته است. بر این

1. Digital certificate
2. Digital watermark
3. Blockchain
4. Encryption
5. Jean-Mary
6. Pech
7. Wazirali; Ahmad; Al-Amayreh; Al-Madi & Khalifeh

اساس، هدف پژوهش کنونی، شناسایی مخاطرات و تهدیدات فنی اثرگذار بر حق مؤلف منابع اطلاعاتی در سامانه‌های یاد شده است تا با شناسایی و تحلیل خطرات فنی و ارائه راه‌حل بتوان از نقض حقوق پدیدآورندگان منابع اطلاعاتی در سامانه‌ها جلوگیری به عمل آورد. به همین منظور با توجه به مسئله و هدف پژوهش، مطالعه حاضر در تلاش برای پاسخ به دو پرسش زیر است:

۱. تهدیدهای فنی اثرگذار بر حق مؤلف منابع اطلاعاتی در سامانه‌های مورد مطالعه از دید خبرگان کدام است؟

۲. وضعیت سامانه‌های سازمان اسناد و کتابخانه ملی ایران از نظر تهدیدات و مخاطرات فنی بر حق مؤلف منابع اطلاعاتی چگونه است؟

پیشینه پژوهش

بیشتر پژوهش‌های انجام شده در موضوع تهدیدات و مخاطرات امنیتی در سامانه‌های اطلاعاتی یا ارزیابی امنیت اطلاعات در کتابخانه‌های دیجیتالی مورد کنکاش قرار گرفته بود. بنابراین، پژوهش‌هایی در ادامه بیان می‌شود که صرفاً برخی از شاخص‌های مرتبط با حق مؤلف و تهدیدات فنی را در برگرفته است، چرا که در جستجوها پژوهش و مطالعه‌ای که مشابه پژوهش کنونی باشد، یافت نشد.

نوروزی (۱۳۹۰) در پژوهشی، استفاده از الزامات فناوری مانند دیواره آتش، سیستم تشخیص نفوذ و نرم‌افزارهای ضد ویروس را از جمله محورهای توسعه کتابخانه‌های دیجیتالی در بعد فناوری برشمرده است. وی با استفاده از تحلیل اسنادی (کتابخانه‌ای) مطالعات مختلف مرتبط را بررسی کرده است. پژوهشگر معتقد است که در رابطه با تمهیدات امنیتی و امکان پیاده‌سازی آن بر روی فناوری‌های موجود در حوزه کتابخانه‌های دیجیتالی باید بررسی‌های لازم انجام گیرد تا در صورت لزوم و توسعه بتوان بدون محدودیت مباحث امنیتی را اعمال کرد.

پژوهش حریری و نظری (۱۳۹۱) با هدف شناخت وضعیت امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران انجام شد. در این پژوهش از روش پیمایشی تحلیلی استفاده شد. پژوهشگران از استاندارد ISO/IEC27002 استفاده کردند. این استاندارد شامل یازده شاخص و ۷۹ زیرشاخص، امنیت اطلاعات را مورد سنجش قرار دادند. شاخص‌های ارزیابی شامل خط مشی امنیت، سازماندهی امنیت اطلاعات، مدیریت دارایی‌ها، امنیت منابع انسانی، امنیت فیزیکی و محیطی، مدیریت ارتباطات و عملیات، کنترل دسترسی، تهیه، توسعه و نگهداری سامانه‌های اطلاعاتی، مدیریت حوادث و نظیر آن است. ۵۸ کتابخانه دیجیتالی فعال در ایران نیز جامعه پژوهش را شکل داد. یافته‌های پژوهش نشان داد که کتابخانه دیجیتال ملی ایران از نظر شاخص‌های امنیت فوق در سطح قوی قرار دارد. پژوهشگران یکی از شاخص‌های آسیب‌پذیر نقاط امنیتی را در امنیت نیروی انسانی می‌دانند.

سامانه‌های نهاد کتابخانه‌های عمومی در پژوهش کوکبی و کوهی رستمی (۱۳۹۴) از نظر امنیتی ارزیابی شدند. نتیجه مطالعه نشان داد که امنیت اطلاعات در سامانه‌ها در حد متوسطی قرار دارد. همچنین شاخص وضعیت کنترل دسترسی در این سامانه‌ها امتیاز متوسط را کسب نمود. پژوهشگران در نهایت توصیه‌هایی را برای ارتقاء سامانه‌ها ارائه دادند: دسترسی به اطلاعات و پردازش‌ها بر اساس نیاز سازمانی و امنیتی کنترل شود؛ قواعد دسترسی و روش اعطای حق دسترسی مشخص شود؛ حفاظت از اطلاعات سازمان در مکانی امن؛ و امضای پیمان‌نامه عدم افشای اسرار توسط کارکنان اشخاص ثالث استفاده‌کننده از تجهیزات پردازش اطلاعات و نظیر آن.

عیدی قلعه‌شیری (۱۳۹۵) در پژوهشی به ارزیابی چالش‌های امنیتی در طراحی کتابخانه دیجیتالی آستان قدس رضوی پرداخته است. این ارزیابی که با استفاده از استاندارد OWASP انجام شده، به این نتیجه دست یافت که مؤلفه‌هایی مانند حملات ویروسی و بدافزارها (اسب‌های تراوا و کرم‌ها و ...) و جعل آدرس آی پی از جمله چالش‌های امنیتی شناسایی شده هستند.

نتیجه پژوهش رضوانی (۱۳۹۷) مبنی بر مدیریت امنیت در کتابخانه‌های دیجیتالی ایران به روش توصیفی همبستگی نشان داد که امنیت منابع انسانی و حفاظت محتوا، خط مشی امنیت اطلاعات، معماری اطلاعات، سازماندهی امنیت اطلاعات و توسعه سامانه‌های اطلاعاتی بر امنیت اطلاعات در کتابخانه‌های دیجیتالی تأثیرگذار است.

پژوهش آموزگار، نوروزی و صراف‌زاده (۱۴۰۱)، چالش‌های حق مؤلف منابع دیجیتالی متنی را مورد کنکاش قرار داد. این پژوهش با روش پیمایشی-تحلیلی و با نظرخواهی از مدیران کتابخانه‌های دیجیتالی انجام شد. پژوهشگران دریافتند که فناوری‌های حفاظتی، سیستمی و شبکه‌ای، از جمله چالش‌های حق مؤلف منابع یاد شده است.

پاپی (۱۴۰۲) در پژوهش خود با عنوان «ارائه چارچوب پیشنهادی الزامات فنی حمایت از حق مؤلف منابع اطلاعاتی در سامانه‌های اطلاعاتی سازمان اسناد و کتابخانه ملی ایران؛ با تکنیک دلفی فازی» که با رویکرد کیفی انجام داده بود به این نتیجه رسید که الزامات فنی 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 در حق مؤلف منابع اطلاعاتی را شکل داده‌اند. همچنین، یافته‌های پژوهش حاکی از آن است که سامانه‌های دیجیتالی و کتابشناختی از نظر بهره‌گیری از الزامات فنی پیشگیرانه برای رعایت حق مؤلف نیز در سطح ضعیفی قرار دارند. این پژوهش استفاده از الزامات فنی ریزدانگی، تدوین سیاست حق مؤلف و استفاده از فراداده حقوقی، توسعه و روزآمد نگه‌داشتن سامانه‌ها و

ارتباط و تعامل با شرکت پشتیبان نرم‌افزار، استاندارد متس و بهره‌گیری از مخزن دیجیتالی را در سامانه‌های مورد مطالعه به منظور حفاظت از حقوق پدیدآورندگان و ذینفعان آثار را پیشنهاد می‌دهد.

در پژوهش دیگری، امنیت سامانه‌های اطلاعاتی در کتابخانه‌های عمومی و تخصصی در مالزی توسط اسماعیل و زینب[1](۲۰۱۱) مورد بررسی قرار گرفت. یافته‌های پژوهش حاکی از پیاده‌سازی بیش از ۹۵ درصد کتابخانه‌ها در خصوص فناوری‌های امنیتی است. برای ارزیابی سامانه‌ها از سیاهه وارسی استفاده شده است.

پژوهش انجام‌شده توسط هان، هوانگ و رن[2](۲۰۱۶)، ریسک امنیت اطلاعات کتابخانه دیجیتال، در یکی از عالی‌ترین کتابخانه‌های دیجیتال در گوانگدونگ[3]چین با استفاده از استاندارد ISO27000 مورد ارزیابی قرار گرفت. یافته‌های حاصل از ارزیابی حاکی از آن است که ۲۶ نوع تهدید و ۱۳ نوع آسیب‌پذیری در امنیت اطلاعات به دست آمد. خرابکاری کارکنان، رمزعبور، نفوذ مخرب، تهاجم و دستکاری، دسترسی غیرمجاز، نقص در مکانیزم پشتیبانی از سامانه، نبود مدیریت دارایی و قوانین مالکیت در کتابخانه دیجیتال از جمله تهدیدات در کتابخانه دیجیتال مورد مطالعه به شمار می‌روند.

پاپی، رضایی شریف‌آبادی، محمداسماعیل و حریری[4](۲۰۱۷) در پژوهشی به شناسایی الزامات فناورانه برای حفاظت از حق مؤلف در سامانه گنج ایرانداک پرداخته بودند. این پژوهش با رویکرد کیفی و روش گراندد تئوری انجام شد. یافته‌های تحلیل با کدگذاری باز، محوری و انتخابی حاکی از آن است که شاخص‌های کنترل دسترسی، کنترل کپی، استانداردهای حفاظتی، پروتکل انتقال ایمن، مجوز، گواهینامه امنیتی، شناساگر شیء دیجیتال و نرم‌افزار مدیریت حقوق دیجیتال به عنوان برخی از شاخص‌های مهم در حفاظت از حق مؤلف پایان‌نامه‌ها و رساله‌ها در سامانه گنج شناسایی شدند.

پژوهش دیگری توسط اوکیکه و آدتورو[5](۲۰۱۹) با هدف بررسی امنیت اطلاعات در سامانه‌های اطلاعاتی کتابخانه‌ها و تأثیر آن بر مهارت‌های فنی کتابداران نیجریه‌ای به روش پیمایش انجام شد. نتایج تحلیل نشان داد که کتابداران در کسب مهارت‌های فنی پیشرفته دچار ضعف هستند. بر همین اساس، اکثر حملات امنیتی به سامانه‌های اطلاعاتی از سوی افراد داخلی به دلیل فقدان مهارت در حفاظت از سامانه‌ها انجام می‌گیرد.

مطالعه‌ای توسط لیو، جانگ، وو و پاتهان (۲۰۲۱) با هدف بررسی حمایت از کپی‌رایت دیجیتال بر اساس یکی از قالب‌های فناوری بلاک‌چین یعنی هایپرلجر فابریک[6]با استفاده از روش تحلیل مقایسه‌ای انجام شد.

1. Ismail & Zainab
2. Han, Huang & Ren
3. Guangdong
4. Papi, Rezaei Sharifabadi, Mohammad esmaeil & Hariri
5. Okike & Adetoro
6. Hyperledger Fabric

پژوهشگران با درک و آشنایی با نقض آثار در محیط دیجیتال، پیشنهاد استفاده از فناوری قرارداد هوشمند فابریک و سامانه پیشنهادی مبتنی بر بلاک‌چین را می‌دهند. در سامانه پیشنهادی که بر اساس قالب یاد شده انجام شده، از فناوری بلاک‌چین به منظور ردیابی نقض آثار و حفاظت از کپی‌رایت دیجیتال بهره می‌برد.

کمیسیون اروپا (۲۰۲۲)، طرحی با مطالعه کپی‌رایت و فناوری‌های جدید با هدف مدیریت کپی‌رایت داده و هوش مصنوعی انجام داد. این طرح که با تحلیل وضعیت موجود در بخش‌های مختلف آثار خلاقانه صورت گرفت، به این نتیجه دست یافت که با وجود پیشرفت قابل توجه در بسیاری از حوزه‌ها، چالش‌های مربوط به مدیریت داده‌های حقوق همچنان ادامه دارد. این گزارش برای بهبود، پیشنهاد استفاده از ابرداده، چارچوب‌های داده، استفاده از فناوری‌های جدید مانند هوش مصنوعی را می‌دهد. استفاده از هوش مصنوعی برای تکثیر، داده‌کاوی، رفع چالش‌های انتساب (حق معنوی) نادرست آثار می‌تواند به کار رود (کمیسیون اروپا، ۲۰۲۲).

نتایج پژوهش فرید، وارایچ و افتخار[1] (۲۰۲۳) که با روش مرور نظام‌مند و فراترکیب سیاست مدیریت امنیت اطلاعات دیجیتال را در کتابخانه‌های دانشگاهی طی سال‌های ۲۰۲۲-۲۰۱۰ مطالعه کرده بودند، نشان می‌دهد که در برخی از کتابخانه‌های دانشگاهی در دنیا در زمینه حفاظت از داده‌ها، منسوخ‌شدن نرم‌افزار و سخت‌افزار، ذخیره‌سازی، اشتراک‌گذاری و امنیت داده‌ها، پشتیبان‌گیری از داده‌ها، حفاظت از داده‌ها در برابر بدافزارها و ویروس‌ها، به‌روزنبودن ابزارها در کتابخانه‌ها با مشکل مواجه هستند. این مسائل بیشتر در کتابخانه‌های کشورهای در حال توسعه به چشم می‌خورد. برخی از سامانه‌ها در کشورهایی مانند غنا، پاکستان، نیجریه، هند و عمان فاقد سیاست مدیریت امنیت برای اطلاعات دیجیتال هستند. اما در کتابخانه‌های کشورهایی مانند بریتانیا، ایالات متحده، چین و امارات، سیاست‌ها، اقدامات و قوانینی برای امنیت اطلاعات دیجیتال تدوین شده است. تصویری توصیفی از پژوهش‌ها در جدول ۱ نیز قابل مشاهده است.

جدول ۱. تصویری توصیفی از پژوهش‌ها و مطالعات انجام‌شده

نویسنده/گان	موضوع	روش	نتیجه‌گیری
نوروزی (۱۳۹۰)	کتابخانه‌های دیجیتالی	تحلیل اسنادی (کتابخانه‌ای)	استفاده از دیواره آتش، سیستم تشخیص نفوذ و نرم‌افزارهای ضد ویروس را از جمله محورهای توسعه کتابخانه‌های دیجیتالی در بعد فناوری برشمرده است.
حریری و نظری (۱۳۹۱)	امنیت اطلاعات در کتابخانه‌های دیجیتالی	پیمایشی تحلیلی	کتابخانه دیجیتال ملی ایران از نظر شاخص‌های امنیت فوق در سطح قوی قرار دارد. پژوهشگران یکی از شاخص‌های آسیب‌پذیر نقاط امنیتی را در امنیت نیروی انسانی می‌دانند.
کوکبی و کوهی رستمی (۱۳۹۴)	سامانه تحت وب نهاد کتابخانه‌های عمومی کشور	ارزیابانه	امنیت اطلاعات در سامانه‌ها در حد متوسطی قرار دارد. همچنین شاخص وضعیت کنترل دسترسی در این سامانه‌ها امتیاز متوسط را کسب نمود.

1. Farid, Warraich & Iftikhar

عیدی قلعه‌شیری (۱۳۹۵)	چالش‌های امنیتی در طراحی کتابخانه دیجیتالی	ارزیابانه	مؤلفه‌هایی مانند حملات ویروسی و بدافزارها (اسب‌های تراوا و کرم‌ها و ...) و جعل آدرس آی پی از جمله چالش‌های امنیتی شناسایی شده هستند.
رضوانی (۱۳۹۷)	امنیت در کتابخانه‌های دیجیتالی	توصیفی همبستگی	امنیت منابع انسانی و حفاظت محتوا، خط مشیء امنیت اطلاعات، معماری اطلاعات، سازماندهی امنیت اطلاعات و توسعه سامانه‌های اطلاعاتی بر امنیت اطلاعات در کتابخانه‌های دیجیتالی تأثیرگذار است.
آموزگار، نوروزی و صراف‌زاده (۱۴۰۱)	حق مؤلف منابع دیجیتالی متنی	پیمایشی–تحلیلی	پژوهشگران دریافتند که فناوری‌های حفاظتی، سیستمی و شبکه‌ای، از جمله چالش‌های حق مؤلف منابع یاد شده است.
پاپی (۱۴۰۲)	شناسایی الزامات فنی در سامانه‌های اطلاعاتی سازمان اسناد و کتابخانه ملی ایران	رویکرد کیفی و دلفی فازی	الزامات فنی 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 در حق مؤلف منابع اطلاعاتی شکل داده‌اند.
اسماعیل و زینب (۲۰۱۱)	امنیت سامانه‌های اطلاعاتی در کتابخانه‌های عمومی و تخصصی	ارزیابانه	یافته‌های پژوهش حاکی از پیاده‌سازی بیش از ۹۵ درصد کتابخانه‌های عمومی و تخصصی مالزی در خصوص فناوری‌های امنیتی است.
هان، هوانگ و رن (۲۰۱۶)	امنیت اطلاعات کتابخانه دیجیتال	ارزیابانه	خرابکاری کارکنان، رمزعبور، نفوذ مخرب، تهاجم و دستکاری، دسترسی غیرمجاز، نقص در مکانیزم پشتیبانی از سامانه، نبود مدیریت دارایی و قوانین مالکیت در کتابخانه دیجیتال از جمله تهدیدات در کتابخانه دیجیتال مورد مطالعه به شمار می‌روند.
پاپی، رضایی شریف‌آبادی، محمداسماعیل و حریری (۲۰۱۷)	الزامات فناورانه برای حفاظت از حق مؤلف در سامانه گنج	رویکرد کیفی و روش گراندد تئوری	شاخص‌های کنترل دسترسی، کنترل کپی، استانداردهای حفاظتی، پروتکل انتقال ایمن، مجوز، گواهینامه امنیتی، شناساگر شیء دیجیتال و نرم‌افزار مدیریت حقوق دیجیتال به عنوان برخی از شاخص‌های مهم در حفاظت از حق مؤلف پایان‌نامه‌ها و رساله‌ها در سامانه گنج شناسایی شدند.
اوکیکه و آدتورو (۲۰۱۹)	امنیت اطلاعات در سامانه‌های اطلاعاتی کتابخانه‌ها	کمی/ پیمایشی	کتابداران در کسب مهارت‌های فنی پیشرفته دچار ضعف هستند. بر همین اساس، اکثر حملات امنیتی به سامانه‌های اطلاعاتی از سوی افراد داخلی به دلیل فقدان مهارت در حفاظت از سامانه‌ها انجام می‌گیرد.
لیو، جانگ، وو و پاتهان (۲۰۲۱)	کپی‌رایت دیجیتال و فناوری بلاک‌چین در حمایت از آثار	تحلیل مقایسه‌ای	پیشنهاد استفاده از فناوری قرارداد هوشمند فابریک و سامانه پیشنهادی مبتنی بر بلاک‌چین ارائه شد. در سامانه پیشنهادی، از فناوری بلاک‌چین به منظور ردیابی نقض آثار و حفاظت از کپی‌رایت دیجیتال بهره می‌برد.
کمیسیون اروپا (۲۰۲۲)	کپی‌رایت و فناوری‌های جدید با هدف مدیریت کپی‌رایت داده و هوش مصنوعی		پیشنهاد استفاده از ابرداده، چارچوب‌های داده، استفاده از فناوری‌های جدید مانند هوش مصنوعی را می‌دهد. استفاده از هوش مصنوعی برای تکثیر، داده‌کاوی، رفع چالش‌های انتساب (حق معنوی) نادرست آثار می‌تواند به کار رود.
فرید، وارایچ و افتخار (۲۰۲۳)	امنیت اطلاعات دیجیتال در کتابخانه‌های دانشگاهی	روش مرور نظام‌مند و فراترکیب	حفاظت از داده‌ها، منسوخ‌شدن نرم‌افزار و سخت‌افزار، ذخیره‌سازی، اشتراک‌گذاری و امنیت داده‌ها، پشتیبان‌گیری از داده‌ها، حفاظت از داده‌ها در برابر بدافزارها و ویروس‌ها، به‌روزنبودن ابزارها در کتابخانه‌ها و نبود سیاست مدیریت امنیت برای اطلاعات دیجیتال از جمله مشکلات گریبانگیر کتابخانه‌ها هستند.

همان‌طور که در مرور مطالعات پیشین مشاهده شد، اغلب پژوهش‌های صورت‌گرفته با تمرکز بر امنیت در کتابخانه‌های دیجیتالی انجام شده است. به عبارتی، چهار رویکرد در انجام مطالعات یافت‌شده وجود دارد. رویکرد نخست؛ امنیت کتابخانه‌های دیجیتالی، رویکرد دوم؛ امنیت در سامانه‌های اطلاعاتی کتابخانه‌ها، رویکرد سوم؛ به فناوری‌های جدید مانند بلاک‌چین و هوش مصنوعی در ارتباط با کپی‌رایت آثار می‌پردازد؛ و رویکرد چهارم، اجرای الزامات فنی حفاظتی در سامانه‌های اطلاعاتی را مدنظر قرار داده است.

در رویکرد نخست، پژوهش‌هایی مانند فرید، وارایچ و افتخار (۲۰۲۳)؛ هان، هوانگ و رن (۲۰۱۶)؛ نوروزی (۱۳۹۰)؛ حریری و نظری (۱۳۹۱)؛ عیدی قلعه‌شیری (۱۳۹۵)؛ رضوانی (۱۳۹۷) به نبود برخی از مؤلفه‌های امنیتی در کتابخانه‌های دیجیتال مانند نبود سیاست برای امنیت اطلاعات، بدافزارها، منسوخ‌شدن نرم‌افزارها، خرابکاری‌های نیروی انسانی و نظیر آن اشاره می‌کنند. تنها وجود و فقدان برخی از شاخص‌های مربوط به امنیت در اجرای حق مؤلف در سامانه‌های اطلاعاتی می‌تواند نقش داشته باشد. پژوهش‌های کوکبی و کوهی‌رستمی (۱۳۹۴)؛ اسماعیل و زینب (۲۰۱۶) و اوکیکه و آدتورو (۲۰۱۹)؛ رویکرد دوم را پوشش می‌دهند. مطالعات انجام شده توسط لیو، جانگ، وو و پاتهان (۲۰۲۱) و کمیسیون اروپا (۲۰۲۲) بر فناوری‌های بلاک‌چین و هوش مصنوعی در جلوگیری از نقض آثار می‌پردازد.

پژوهش‌های پاپی، رضایی شریف آبادی، محمداسماعیل و حریری (۲۰۱۷)؛ آموزگار، نوروزی و صراف‌زاده (۱۴۰۱) و پاپی (۱۴۰۲) به رویکرد چهارم اختصاص دارند. در پژوهش نخست، پژوهشگران برخی الزامات فناورانه برای حفاظت از حق مؤلف در سامانه گنج ایرانداک که حاوی رساله‌ها و پایان‌نامه‌هاست را پیشنهاد می‌دهند. در پژوهش آموزگار، نوروزی و صراف‌زاده (۱۴۰۱) نیز فقط الزامات حفاظتی سیستمی و شبکه‌ای را در حق مؤلف منابع ضروری می‌دانند و در پژوهش پاپی (۱۴۰۲) هم الزامات فنی اثرگذار بر حق مؤلف منابع در سامانه‌های اطلاعاتی کتابخانه ملی ایران شناسایی شده‌اند و به تهدیدات فنی که موضوع و مسئله پژوهش کنونی است، پرداخته نشده است. بنابراین، با تحلیل مطالعات انجام‌گرفته می‌توان پی برد که تاکنون چنین پژوهشی که هدف از آن شناسایی تهدیدات فنی بر حق مؤلف منابع اطلاعاتی در سامانه‌های اطلاعاتی کتابخانه‌ها باشد، انجام نشده است.

روش‌شناسی پژوهش

پژوهش کنونی از نظر هدف کاربردی است و برای گردآوری داده‌ها از رویکرد کیفی استفاده کرده است. در رویکرد کیفی، با توجه به هدف و مسئله پژوهش از روش‌های تحلیل اسنادی، تحلیل مضمون و دلفی فازی استفاده شد. برای بررسی و تحلیل منابع و پژوهش‌ها از پایگاه‌های داخلی و خارجی نظیر اپک سازمان اسناد و

کتابخانه ملی ایران، گنج ایرانداک، مرکز اطلاعات علمی جهاد دانشگاهی و پرتال علمی جهاد دانشگاهی با به کارگیری عبارات و کلیدواژه‌های فارسی "مخاطرات فنی"، "تهدیدات فنی سامانه‌های اطلاعاتی"، " حق مؤلف و کتابخانه‌های دیجیتالی" و "حق مؤلف و سامانه‌های اطلاعاتی" و پایگاه‌های خارجی نظیر گوگل اسکالر[1]، ساینس دایرکت[2]، امرالد[3]، sagepub و eprints in LIS با استفاده از کلیدواژه‌های: "technical threats in information systems or digital libraries", "technical risks in information" systems or digital libraries", "copyright and information systems or digital libraries", "threats to Information Systems in libraries"، متون و منابع پژوهشی مختلفی به دست آمد. ضمن این که برخی مؤلفه‌های استاندارد ISO/IEC 27001 مانند کنترل دسترسی و رمزنگاری (سازمان ملی استاندارد، ۱۳۹۴) در تدوین سیاهه وارسی به کار برده شد.

تحلیل اسنادی از جمله روش‌های کیفی است که به صورت نظام‌مند به بررسی و ارزیابی اسناد می‌پردازد. این روش شامل بررسی، خواندن و تفسیر متون است (بوئن[4]، ۲۰۰۹). پس از این مرحله، برای کشف بهتر مفاهیم، با ۶ نفر از متخصصان حوزه‌های سامانه‌های اطلاعاتی، حق مؤلف و کتابخانه‌های دیجیتالی مصاحبه انجام شد (جدول ۳). مصاحبه‌ها به صورت حضوری و از طریق پست الکترونیک انجام گرفت.

جدول ۳. مشخصات مصاحبه‌شوندگان

ردیف	سطح تحصیلات	زمینه تخصصی	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 دیجیتالی	۱۷	ایران (تهران)
۵	Professor, Intellectual Property Management	Intellectual Property Rights (IPRs), digital technology	۳۰	India (Delhi)
۶	Ph.D in computer science	Digital Library Strategist & Metadata Architect	۲۵	United States (Pennsylvania)
۶ نفر	**مجموع**			

پس از پیاده‌سازی مصاحبه‌ها، برای تحلیل از کدگذاری باز و روش تحلیل مضمون استفاده شد. مصاحبه‌ها تا زمان اشباع داده‌ها ادامه یافت. به منظور حفظ حریم خصوصی مصاحبه‌شوندگان و بی‌نام‌بودن آن‌ها، از کد ۱ -۶ استفاده شد. پس از احصاء شاخص‌ها با استفاده از روش تحلیل اسنادی و تحلیل مضمون، سیاهه وارسی

1. Google Scholar
2. Science Direct
3. Emerald
4. Bowen

تدوین شد. برای سنجش اعتبار درونی سیاهه وارسی محقق‌ساخته از اعتبار محتوا استفاده شد. سیاهه در اختیار دو نفر از متخصصان در حوزه‌های مذکور قرار گرفت و نظرات آن‌ها، دریافت و در سیاهه وارسی اعمال شد. همچنین از آلفای کرونباخ برای سنجش پایایی شاخص‌ها استفاده شد. پایایی ابزار اندازه‌گیری با استفاده از نرم‌افزار SPSS نسخه ۲۴ انجام شد. مقدار آلفای به دست آمده عددی برابر ۰/۹۹ است که اعتبار بسیار بالای سیاهه وارسی را نشان می‌دهد. به منظور استفاده از دانش متخصصان، اعتبارسنجی شاخص‌ها و رسیدن به اجماع گروهی از دلفی فازی استفاده شد. به همین منظور تعداد ۱۱ نفر از متخصصان با داشتن دانش تخصصی در حوزه‌های کتابخانه‌های دیجیتالی و سامانه‌های اطلاعاتی، تجربه کاری بیش از ده سال، مدرک تحصیلی کارشناسی، کارشناسی ارشد و دکتری و در دسترس‌بودن انتخاب شدند. هر ۱۱ نفر در دو پنل دلفی مشارکت داشتند. مقیاس انتخابی برای پرسش‌های سیاهه وارسی نیز طیف لیکرت ۵ درجه‌ای بود که عدد ۱ به معنی بسیار کم و عدد ۵ به معنی بسیار زیاد است.

پس از قراردادن سیاهه وارسی در اختیار خبرگان، از آن‌ها درخواست شد تا نظرشان را درباره هر شاخص در قالب متغیرهای کلامی مندرج در پرسشنامه بیان کنند (جدول ۴). برای فازی‌سازی اعداد، ابتدا بر اساس طیف اعداد فازی مثلثی معادل طیف لیکرت ۵ درجه، به عدد فازی تبدیل می‌شوند.

جدول ۴. اعداد فازی مثلثی معادل طیف لیکرت ۵ درجه

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

سپس 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. نتایج کلیه محاسبات فازی‌سازی، در جدول ۸، ۹ و ۱۰ آورده شده است. در این پژوهش عدد آستانه ۰/۵ در نظر گرفته می‌شود. در روش دلفی فازی که حالت غربالگری دارد متغیرهایی تأیید می‌شود که حداقل توافق روی آن‌ها ۵۰ درصد باشد (حبیبی، فیروزی جهان‌تیغ و صراف‌رضی[1] ۲۰۱۵؛ حبیبی و آفریدی، ۱۴۰۱).

در دور اول، میانگین فازی شاخص"توصیفی‌بودن فراداده دوبلین‌کور" کمتر از ۰/۵ بود که حذف شد (جدول ۸). تحلیل دلفی فازی برای تمام شاخص‌های پذیرفته شده، در دور دوم ادامه پیدا کرد. در این دور ۱۶

1. Habibi, Firouzi Jahantigh & Sarafrazi

شاخص بر اساس دیدگاه ۱۱ خبره مجدد مورد ارزیابی قرار گرفت. در این دور هر ۱۶ شاخص تأیید شدند (جدول ۹). در صورتی که اختلاف میانگین امتیاز پرسش‌های دور اول و دور دوم از عدد ۰/۲ کوچکتر باشد، فرآیند نظرسنجی متوقف می‌شود (حبیبی و آفریدی، ۱۴۰۱). پس از اعتبارسنجی و تأیید نهایی شاخص‌ها، ارزیابی ۷ سامانه سازمان اسناد و کتابخانه ملی ایران توسط پژوهشگر و مدیران سامانه‌ها انجام شد. بدین صورت که پژوهشگر با مشاهده سامانه‌ها، شاخص‌هایی که قابل رؤیت بود را با سامانه‌ها مطابقت داده و در صورت وجود و یا نبود شاخص‌ها، یکی از گزینه‌های بلی یا خیر انتخاب می‌شد. سپس سیاهه در اختیار مدیران سامانه‌ها قرار گرفت تا سایر شاخص‌ها که بر روی سامانه‌ها قابل رؤیت نیست و فقط مدیر سامانه‌ها در جریان وجود و نبود شاخص‌هاست، ارزیابی را انجام دهند. همان‌طور که بیان شد، رویکرد کیفی و نوع ارزیابانه آن برای پژوهش کنونی مناسب آمدند، چرا که سیاهه وارسی برای توصیف و ارزیابی وضعیت سامانه‌ها به کار رفت.

روی‌هم‌رفته جامعه پژوهش عبارت بودند از: الف) منابع و مطالعات پژوهشی برای استخراج شاخص‌ها به منظور استفاده در سیاهه وارسی؛ ب) تعداد ۶ نفر از متخصصان داخل و خارج از کشور برای انجام مصاحبه؛ ج) تعداد ۱۱ نفر از متخصصان و خبرگان برای حضور در پنل دلفی؛ و د) تعداد ۷ سامانه اطلاعاتی سازمان اسناد و کتابخانه ملی ایران به دلیل جامعیت منابع اطلاعاتی میان کتابخانه‌های ایرانی، مرجعیت کتابخانه ملی ایران همانند سایر کتابخانه‌های ملی کشورها، تنوع و گونه‌های مختلف منابع اطلاعاتی در سامانه‌های یاد شده به عنوان جامعه پژوهش انتخاب شدند (جدول ۵).

جدول ۵. فهرست سامانه‌های اطلاعاتی مورد مطالعه

سامانه دیجیتال ملی (کتابخانه دیجیتال)	https://dl.nlai.ir/ui/forms/index.aspx
سامانه نشریات ایران (سنا)	https://sana.nlai.ir/
سامانه نشریات علمی ایران	https://iranjournals.nlai.ir/
بانک نشریات ایران	https://mags.nlai.ir/
شبکه مراکز اسناد کشور	https://docs.nlai.ir/
سامانه فهرستگان نسخ خطی	https://scripts.nlai.ir/
شبکه کتابخانه‌های کشور	https://libs.nlai.ir/

همان‌طور که گفته شد، در تحلیل داده‌ها و هنگام استفاده از روش تحلیل مضمون، از روش دستی استفاده شد. اما برای ترسیم داده‌ها، نسخه ۲۰۲۰ نرم‌افزار مکس.کیو.دی.ای به کار گرفته شد. نرم‌افزار تبلو[1] نسخه ۲۰۱۸ آن نیز برای تجسم بهتر داده‌ها و ترسیم نمودارها استفاده شد. همچنین در دلفی فازی تمام محاسبات در نرم‌افزار صفحه گسترده اکسل نسخه ۲۰۱۶ انجام گرفت. به منظور اعتبارسنجی یافته‌های کیفی از روش

1. Tableau

مثلث‌سازی (سه‌سوسازی) روش‌شناختی استفاده شد. استفاده از روش‌ها و ابزارهای مختلف برای گردآوری داده‌ها از جمله تحلیل اسنادی، تحلیل مضمون، دلفی فازی و مصاحبه، مشاهده و سیاهه وارسی، به پژوهش کیفی اعتبار می‌بخشد.

مثلث‌سازی به عنوان یک راهبرد پژوهش کیفی برای اعتبارسنجی از طریق همگرایی اطلاعات منابع مختلف در نظر گرفته شده است. روش مثلث‌سازی شامل استفاده از روش‌های متعدد جمع‌آوری داده‌ها مانند مصاحبه، مشاهده و یادداشت‌های میدانی در مورد یک پدیده است (کارتر و دیگران،[1] ۲۰۱۴).

یافته‌های پژوهش

برای پاسخ به پرسش نخست پژوهش یعنی تهدیدات فنی در سامانه‌های مورد مطالعه از نظر خبرگان، شاخص‌های مختلفی نقش دارند. برای پاسخ به این پرسش، ابتدا سیاهه‌ای متشکل از ۱۷ شاخص مخاطرات فنی و ۸ مؤلفه با روش تحلیل اسنادی گردآوری و با روش تحلیل مضمون در دو سطح بررسی شد (جداول ۶ و ۷).

جدول ۶. نمونه‌ای از روش تحلیل اسنادی (تحلیل منابع و مطالعات)

اسناد و منابع انتخاب‌شده	تحلیل داده‌ها
یکی از بزرگترین تهدیدات به سرور کتابخانه دیجیتالی حملات ویروسی و حملات بدافزارها است. تاکنون تعداد زیادی ویروس کامپیوتری شناسایی شده که با حمله به فایل‌ها، آن‌ها را خراب، رمزنگاری و یا غیرقابل استفاده می‌نمایند (عیدی قلعه‌شیری، ۱۳۹۵، ص. ۹۲).	وجود بدافزارهای مختلف تهدیدی برای کتابخانه‌های دیجیتالی
Poor level of data backup policies in libraries. Libraries have no policies on data backup. Most of the libraries fail to take proper backup of the data on regular basis. (Farid, Warraich & Iftikhar, 2023, p. 9-10).	نداشتن پشتیبان از برنامه
Employee sabotage is often security threats to which are exposed information systems resources. As already mentioned insiders are persons that are the best familiar with system resources, performances and capabilities, so they are also familiar with information system areas where they can cause the most damage. If this is connected with unsatisfied employees there exists a real danger of sabotage actions from existing or former employee. Although the proportion of employee sabotage in total information system security threats is lower then the portion of fraud and theft, the consequences of this threat can be substantial (Geric & Hutinski, 2007, p. 53).	خرابکاری عمدی کارکنان در سامانه‌های اطلاعاتی
The network security for a library would need to disallow access to the IS from unauthorised users, while simultaneously ensuring full access to legitimate users (Ismail & Zainab, 2011, p. 50).	فقدان امنیت در شبکه

1. Carter & et al

جدول ۷. نمونه‌ای از روش تحلیل مضمون (کدگذاری مصاحبه‌ها)

کد مصاحبه	نمونه جمله	مفهوم	مقوله
کد ۳	همه تکنیک‌ها در کنارش راه دور زدنش وجود داره و ابزارش هست. مخصوصاً واترمارک‌های سنتی و کپچر کردن اون خیلی کار پیچیده‌ای نیست.	– استفاده از ته‌نقش[1]سنتی به عنوان یک تهدید فنی برای دورزدن	ته‌نقش آشکار
کد ۴	طرف اومده آرشیو دیجیتالی را برای سازمانی زده ده سال پیش، و یه پشتیبانی هم گفته انجام می‌ده اما اون پشتیبانیش در سطح توسعه نیست دیگه. یه سری از این تهدیدات جدیداً مشخص شده و قبلاً نبوده. خب حالا اگر بخواد جلوی این attack را بگیره دیگه نه اون برنامه‌نویس هست، نه تیمش هست، دیگه نه اون شرکت این نرم‌افزار را ساپورت می‌کنه که اون برنامه را از اول تغییر بده که کسی نتونه اون پارامترها را دستکاری کنه.	– در دسترس نبودن تیم برنامه‌نویس و پشتیبان نرم‌افزار	– در دسترس نبودن تیم برنامه‌نویس و پشتیبان نرم افزار
کد ۶	ریسک دیگه‌ای هستش ریسک کیفیت هست. این که کنترل کیفی می‌شه دقیقاً به همین دلیل هست، این هم یکی از مراحل اصلی دیجیتال‌سازی و فرایند آماده‌سازی شیء دیجیتال هست. خود این کنترل کیفی هم خیلی اهمیت داره اگر یک منبعی کنترل کیفی بشه و مشخص بشه مشکلاتی در نمایش، یا توی متادیتا، ناهمخوانی اطلاعات وجود داشته باشه باید اصلاح بشه و اگر این اتفاق نیفته خب ارجاع پذیری اون منبع دیجیتال دچار مشکل می‌شه.	–نبود کنترل کیفی محتواهای دیجیتالی – کم توجهی به مراحل آماده‌سازی شیء دیجیتالی – مشکلات در نمایش محتوا، فراداده، ناهمخوانی در اطلاعات – مشکل در ارجاع‌پذیری منبع دیجیتال	–نبود کنترل کیفی محتواهای دیجیتالی – کم توجهی به مراحل آماده‌سازی شیء دیجیتالی
Code 1	DRM also often makes works much more difficult to preserve. (For example, a DRM'd file might become unusable if its file format becomes obsolete, or support ends for the software required to use it, whereas we might be able to reformat or otherwise repurpose content that does not have such DRM.)	– ضعف DRM در حفاظت طولانی مدت از آثار – دشواری در پشتیبانی فایل‌ها و محتواهای با DRM های منسوخ شده	– ضعف و نقصان DRM در حفاظت طولانی مدت از آثار
Code 2	Technologies that facilitate breaking the codes and technological measures of protection applied to any work. There can be software by Viruses, Worms, Trojan Horses, Bots etc. Other malware are Adware, Spyware, Ransomware (e.g. WannaCry, NotPetya, SimpleLocker, TeslaCrypt, CryptoLocker, and PC Cyborg), Scareware, Rootkits, and Zombies.	– استفاده از فناوری شکستن کدها – استفاده از اقدامات حفاظتی فنی برای مقابله با بدافزارهای مختلف مانند ویروس‌ها، کرم‌ها	– مقابله با بدافزارهای مختلف مانند ویروس‌ها، کرم‌ها و مانند آن.

برای اعتبارسنجی شاخص‌ها، از روش دلفی فازی بهره گرفته شد. پس از تأیید و نهایی شدن سیاهه وارسی با روش دلفی فازی، ۱۶ شاخص مربوط به مخاطرات فنی از دید خبرگان تأیید شدند. ۱۶ شاخص و ۷ مؤلفه به عنوان تهدیدات فنی شناسایی شدند. اجماع نظر خبرگان در دو دور انجام شد (جداول ۸، ۹ و ۱۰).

1. Watermark

جدول ۸. یافته‌های حاصل از دلفی فازی (دور اول)

بعد	مؤلفه‌ها	شاخص‌ها	میانگین فازی مثلثی			میانگین فازی‌زدایی شده	وضعیت
			l	m	u		
تهدیدات فنی (۸)	استانداردها و چارچوب‌ها (۱)	توصیفی بودن فراداده دوبلین کور	۰/۲۲۷	۰/۴۷۷	۰/۷۲۷	۰/۴۷۷	رد
	امنیت شبکه (۵)	خرابکاری عمدی کارکنان	۰/۴۳۲	۰/۶۵۹	۰/۷۹۵	۰/۶۲۹	تأیید
		پایین بودن منبع سرورها	۰/۴۷۷	۰/۷۲۷	۰/۹۳۲	۰/۷۱۲	تأیید
		بدافزارهای مختلف مانند ویروس‌ها، کرم‌ها و مانند آن	۰/۵۰۰	۰/۷۵۰	۰/۹۰۹	۰/۷۲۰	تأیید
		نداشتن پشتیبان از برنامه اصلی	۰/۴۵۵	۰/۷۰۵	۰/۹۰۹	۰/۶۸۹	تأیید
		نداشتن وبگاه آینه‌ای	۰/۴۷۷	۰/۷۲۷	۰/۸۸۶	۰/۶۹۷	تأیید
	زیرساخت فنی (۵)	از دست‌دادن پشتیبانی فیزیکی و زیرساختی (مانند قابل توسعه نبودن نرم‌افزار یا از دست دادن تیم پشتیبان نرم‌افزار)	۰/۵۹۱	۰/۸۴۱	۰/۹۵۵	۰/۷۹۵	تأیید
		ضعف و نقصان دی.آر.ام (DRM) در نسخه‌برداری و حفاظت طولانی مدت از آثار	۰/۴۵۵	۰/۷۰۵	۰/۹۰۹	۰/۶۸۹	تأیید
		نبود نرم‌افزار دی.آر.ام (DRM) در سامانه‌ها	۰/۵۰۰	۰/۷۵۰	۰/۹۰۹	۰/۷۲۰	تأیید
		روزآمد نبودن سامانه‌ها	۰/۵۲۳	۰/۷۷۳	۰/۹۰۹	۰/۷۳۵	تأیید
		مشکل در فضای ذخیره‌سازی	۰/۵۲۳	۰/۷۷۳	۰/۹۳۲	۰/۷۴۲	تأیید
	کنترل کپی (۱)	استفاده از ته‌نقش آشکار	۰/۴۰۹	۰/۶۳۶	۰/۸۴۱	۰/۶۲۹	تأیید
	حفاظت دیجیتال (۱)	دستکاری‌کردن یو آر ال	۰/۳۸۶	۰/۶۳۶	۰/۸۴۱	۰/۶۲۱	تأیید
	احراز هویت (۱)	استفاده نکردن از احراز هویت برای تمام بخش‌ها و صفحات محتوا	۰/۴۷۷	۰/۷۲۷	۰/۹۰۹	۰/۷۰۵	تأیید
تهدیدات فنی	فراداده حقوقی (۱)	تعریف نشدن سیاست حق مؤلف در فرایند دیجیتال‌سازی	۰/۵۶۸	۰/۸۱۸	۰/۸۸۶	۰/۷۵۸	تأیید
	فرایند دیجیتال‌سازی (۲)	نبود کنترل کیفی محتواهای دیجیتالی	۰/۴۳۲	۰/۶۸۲	۰/۸۸۶	۰/۶۶۷	تأیید
		کم‌توجهی به مراحل آماده‌سازی شیء دیجیتالی	۰/۵۰۰	۰/۷۵۰	۰/۹۰۹	۰/۷۲۰	تأیید

جدول ۹. نتایج دلفی فازی (دور دوم)

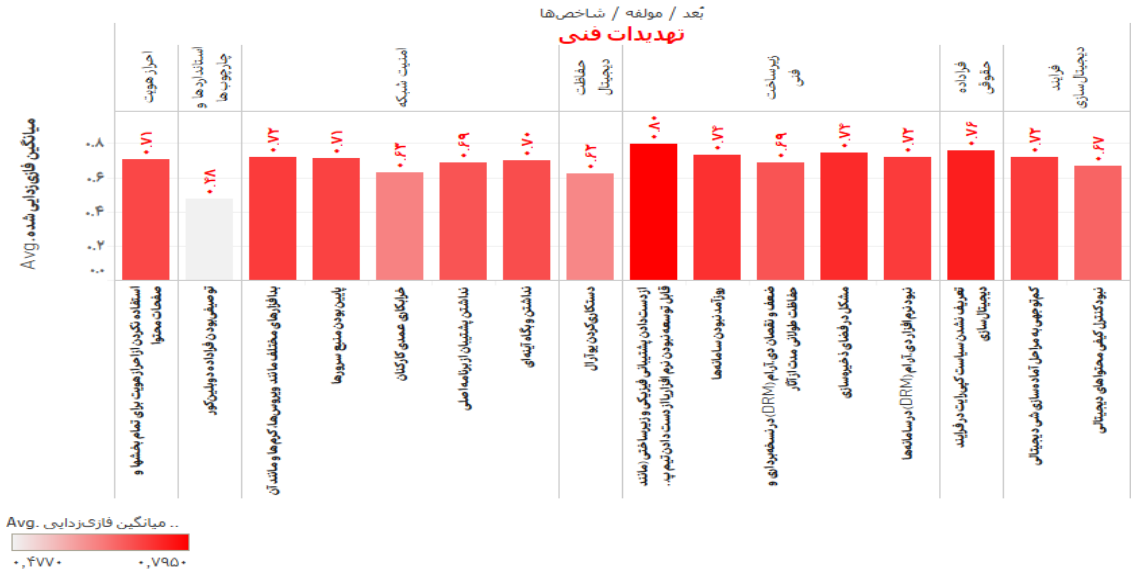
بعد	مؤلفه	شاخص‌ها	میانگین فازی مثلثی			میانگین فازی‌زدایی شده	وضعیت
			l	m	u		
تهدیدات فنی (۷ مؤلفه)	امنیت شبکه (۵)	خرابکاری عمدی کارکنان	۰/۳٤۱	۰/۵۹۱	۰/۸۱۸	۰/۵۸۳	تأیید
		پایین بودن منبع سرورها	۰/۵٤۵	۰/۷۹۵	۰/۹۷۷	۰/۷۷۳	تأیید
		بدافزارهای مختلف مانند ویروس‌ها، کرم‌ها و مانند آن	۰/۵٦۸	۰/۸۱۸	۱/۰۰۰	۰/۷۹۵	تأیید
		نداشتن پشتیبان از برنامه اصلی	۰/٦۱٤	۰/۸٦٤	۰/۹۷۷	۰/۸۱۸	تأیید
		نداشتن وبگاه آینه‌ای	۰/۵۰۰	۰/۷۵۰	۰/۹۳۲	۰/۷۲۷	تأیید
	زیرساخت فنی (۵)	از دست‌دادن پشتیبانی فیزیکی و زیرساختی (مانند قابل توسعه نبودن نرم‌افزار یا از دست دادن تیم پشتیبان نرم‌افزار	۰/٦۳٦	۰/۸۸٦	۰/۹۷۷	۰/۸۳۳	تأیید
		ضعف و نقصان دی.آر.ام (DRM) در نسخه‌برداری و حفاظت طولانی مدت از آثار	۰/۵۰۰	۰/۷۵۰	۰/۹۵۵	۰/۷۳۵	تأیید
		نبود نرم‌افزار دی.آر.ام (DRM) در سامانه‌ها	۰/٤۷۷	۰/۷۲۷	۰/۹۰۹	۰/۷۰۵	تأیید
		روزآمد نبودن سامانه‌ها	۰/۵٦۸	۰/۸۱۸	۰/۹۷۷	۰/۷۸۸	تأیید
		مشکل در فضای ذخیره‌سازی	۰/۵۹۱	۰/۸٤۱	۱/۰۰۰	۰/۸۱۱	تأیید
	کنترل کپی (۱)	استفاده از ته‌نقش آشکار	۰/٤۰۹	۰/٦۵۹	۰/۸۸٦	۰/٦۵۲	تأیید
	حفاظت دیجیتال (۱)	دستکاری‌کردن یو آر ال	۰/٤۰۹	۰/٦۵۹	۰/۸۸٦	۰/٦۵۲	تأیید
	احراز هویت (۱)	استفاده نکردن از احراز هویت برای تمام بخش‌ها و صفحات محتوا	۰/۵٤۵	۰/۷۹۵	۰/۹۷۷	۰/۷۷۳	تأیید
	فراداده حقوقی (۱)	تعریف نشدن سیاست حق مؤلف در فرایند دیجیتال‌سازی	۰/٦۱٤	۰/۸٦٤	۱/۰۰۰	۰/۸۲٦	تأیید
تهدیدات فنی	فرایند دیجیتال‌سازی (۲)	نبود کنترل کیفی محتواهای دیجیتالی	۰/٤۰۹	۰/٦۵۹	۰/۸۸٦	۰/٦۵۲	تأیید
		کم‌توجهی به مراحل آماده‌سازی شیء دیجیتالی	۰/۵۲۳	۰/۷۷۳	۰/۹۷۷	۰/۷۵۸	تأیید

جدول ۱۰. مقایسه دور اول و دوم

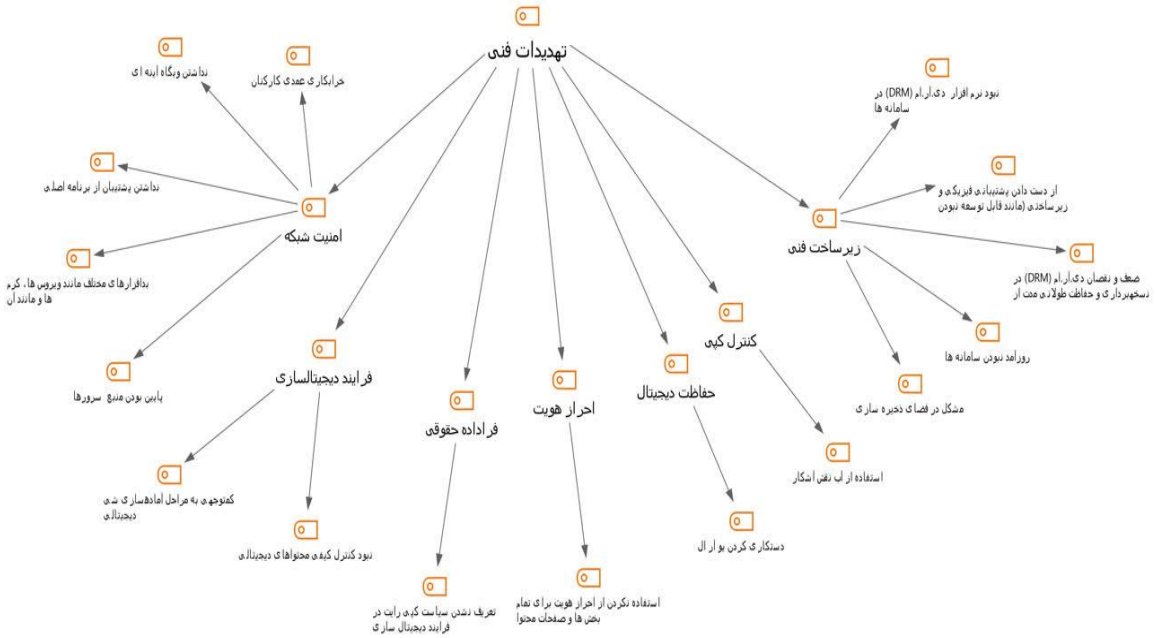
شاخص‌ها	میانگین فازی‌زدایی شده دور دوم	میانگین فازی‌زدایی شده دور اول	اختلاف	وضعیت
خرابکاری عمدی کارکنان	۰/۵۸۳	۰/۶۲۹	-۰/۰۴۵	توافق
از دست‌دادن پشتیبانی فیزیکی و زیرساختی (مانند قابل توسعه نبودن نرم‌افزار یا از دست دادن تیم پشتیبان نرم‌افزار	۰/۸۳۳	۰/۷۹۵	۰/۰۳۸	توافق
پایین بودن منبع سرورها	۰/۷۷۳	۰/۷۱۲	۰/۰۶۱	توافق
بدافزارهای مختلف مانند ویروس‌ها، کرم‌ها و مانند آن	۰/۷۹۵	۰/۷۲۰	۰/۰۷۶	توافق
ضعف و نقصان دی.آر.ام (DRM) در نسخه‌برداری و حفاظت طولانی مدت از آثار	۰/۷۳۵	۰/۶۸۹	۰/۰۴۵	توافق
نبود نرم‌افزار دی.آر.ام (DRM) در سامانه‌ها	۰/۷۰۵	۰/۷۲۰	-۰/۰۱۵	توافق
روزآمد نبودن سامانه‌ها	۰/۷۸۸	۰/۷۳۵	۰/۰۵۳	توافق
استفاده از ته‌نقش آشکار	۰/۶۵۲	۰/۶۲۹	۰/۰۲۳	توافق
دستکاری‌کردن یو آر ال	۰/۶۵۲	۰/۶۲۱	۰/۰۳۰	توافق
استفاده نکردن از احراز هویت برای تمام بخش‌ها و صفحات محتوا	۰/۷۷۳	۰/۷۰۵	۰/۰۶۸	توافق
تعریف نشدن سیاست حق مؤلف در فرایند دیجیتال‌سازی	۰/۸۲۶	۰/۷۵۸	۰/۰۶۸	توافق
نداشتن پشتیبان از برنامه اصلی	۰/۸۱۸	۰/۶۸۹	۰/۱۲۹	توافق
نداشتن وبگاه آینه‌ای	۰/۷۲۷	۰/۶۹۷	۰/۰۳۰	توافق
مشکل در فضای ذخیره‌سازی	۰/۸۱۱	۰/۷۴۲	۰/۰۶۸	توافق
نبود کنترل کیفی محتواهای دیجیتالی	۰/۶۵۲	۰/۶۶۷	-۰/۰۱۵	توافق
کم‌توجهی به مراحل آماده‌سازی شیء دیجیتالی	۰/۷۵۸	۰/۷۲۰	۰/۰۳۸	توافق

خرابکاری عمدی کارکنان، پایین بودن منبع سرورها، بدافزارهای مختلف مانند ویروس‌ها، کرم‌ها و مانند آن، نداشتن پشتیبان از برنامه اصلی، نداشتن وبگاه آینه‌ای (امنیت شبکه)؛ از دست‌دادن پشتیبانی فیزیکی و زیرساختی (مانند قابل توسعه نبودن نرم‌افزار یا از دست دادن تیم پشتیبان نرم‌افزار)، ضعف و نقصان دی.آر.ام (DRM) در نسخه‌برداری و حفاظت طولانی مدت از آثار، نبود نرم‌افزار دی.آر.ام (DRM) در سامانه‌ها، روزآمد نبودن سامانه‌ها و مشکل در فضای ذخیره‌سازی (زیرساخت فنی)؛ استفاده از ته‌نقش آشکار (کنترل کپی)؛ دستکاری‌کردن یو آر ال (حفاظت دیجیتال)؛ استفاده نکردن از احراز هویت برای تمام بخش‌ها و صفحات محتوا (احراز هویت)؛ تعریف نشدن سیاست حق مؤلف در فرایند دیجیتال‌سازی (فراداده حقوقی)؛ نبود کنترل کیفی محتواهای دیجیتالی و کم‌توجهی به مراحل آماده‌سازی شیء دیجیتالی (فرایند دیجیتال‌سازی) از جمله تهدیدات فنی اثرگذار در سامانه‌های مورد مطالعه محسوب می‌شوند. مخاطرات فنی یادشده به مؤلفه‌های احراز هویت،

امنیت شبکه، حفاظت دیجیتال، زیرساخت فنی، فراداده حقوقی و فرایند دیجیتال‌سازی اختصاص دارد. با توجه به میانگین فازی‌زدایی‌شده، هرچه میانگین مذکور بیشتر باشد، توافق بیشتری بر روی شاخص وجود داشته است. به جز شاخص "توصیفی بودن دوبلین کور" که میانگین فازی‌زدایی شده آن کمتر از ۰/۵ است (نمودار ۱)، سایر شاخص‌ها از اجماع نظر و توافق بیشتر برخوردار هستند (شکل ۱).



نمودار ۱. تهدیدات فنی اثرگذار بر حق مؤلف منابع اطلاعاتی در سامانه‌های مورد مطالعه از دید خبرگان



شکل ۱. تهدیدات فنی اثرگذار بر حق مؤلف منابع اطلاعاتی در سامانه‌های مورد مطالعه از دید خبرگان

پاسخ پرسش دوم: وضعیت سامانه‌های سازمان اسناد و کتابخانه ملی ایران از نظر تهدیدات و مخاطرات فنی برای حق مؤلف منابع اطلاعاتی

پس از شناسایی و تأیید شاخص‌ها توسط خبرگان با کمک روش دلفی فازی، ۱۶ شاخص و ۷ مؤلفه توسط خبرگان شناسایی شدند که در خرداد ماه ۱۴۰۲ سامانه‌ها از منظر تهدیدات و مخاطرات فنی برای حق مؤلف منابع اطلاعاتی مورد ارزیابی قرار گرفتند. سامانه‌های دیجیتال ملی، سامانه‌های نشریات ایران (سنا) و نشریات علمی ایران با توجه به عملکردشان دیجیتالی محسوب می‌شوند. همچنین سامانه‌های بانک نشریات ایران، شبکه مراکز اسناد کشور، فهرستگان نسخ خطی و شبکه کتابخانه‌های کشور در دسته کتابشناختی قرار می‌گیرند.

با توجه به یافته‌های حاصل از سیاهه وارسی در خصوص وضعیت سامانه‌های دیجیتالی یاد شده از نظر تهدیدات فنی برای حق مؤلف، با ۱۶ شاخص که از نظر اعضای پنل دلفی انتخاب شده‌اند، ارزیابی صورت گرفت. سامانه‌های دیجیتالی مورد مطالعه از سیستم عامل ویندوز و نرم‌افزار پاپیروس استفاده می‌کنند.

به طور کل، می‌توان اذعان نمود که هیچ یک از ۱۶ شاخص مخاطرات فنی، در سامانه‌های دیجیتالی در دست مطالعه رعایت نشده است. سایر مخاطراتی که به حوزه امنیت شبکه مربوط می‌شود، مانند خرابکاری عمدی کارکنان، پایین بودن منبع[1]سرورها، بدافزارهای مختلف مانند ویروس‌ها، کرم‌ها و مانند آن، نداشتن پشتیبان[2]از برنامه اصلی و نداشتن وبگاه آینه‌ای[3]به عنوان مخاطرات احتمالی در سیاهه اذعان شده و نمی‌توان از آن‌ها در امنیت شبکه غفلت نمود. سایر مخاطرات فنی که به عنوان زیرساخت فنی سامانه‌ها محسوب می‌شوند و در سامانه‌های فوق به عنوان خطر فنی اشاره شده است، عبارتند از: محدودیت فضای محاسباتی (سرورها، نرم‌افزار و ...) و کمبود فضای نگهداری موقت در سامانه‌ها. این دو شاخص در سامانه‌های دیجیتالی برای نگهداری داده‌های بزرگ در سازمان‌ها اهمیت دوچندانی دارند. استفاده از انواع داده و تنوع قالب‌ها در سامانه‌ها می‌تواند بر فضای نگهداری تأثیرگذار باشد. همچنین یافته‌ها نشان داد که از دست‌دادن پشتیبانی فیزیکی و زیرساختی (مانند قابل توسعه نبودن نرم‌افزار یا از دست دادن تیم پشتیبان نرم‌افزار، ضعف و نقصان دی.آر.ام (DRM) در نسخه‌برداری و حفاظت طولانی مدت از آثار، نبود نرم‌افزار دی.آر.ام (DRM) در سامانه‌ها، روزآمد نبودن سامانه‌ها و مشکل در فضای ذخیره‌سازی به عنوان مخاطراتی است که در سامانه‌های دیجیتالی مذکور وجود دارد. این شاخص‌ها را می‌توان از جمله زیرساخت‌های فنی سامانه‌ها نام برد که مستقیم یا غیرمستقیم بر حفاظت از حق مؤلف محتواهای دیجیتال تأثیرگذارند.

1. Resource
2. Backup
3. Website Mirroring

استفاده از ته‌نقش آشکار به عنوان شاخص مطرح شده در کنترل کپی بوده که به عنوان مخاطره فنی در سامانه‌های مورد بررسی بیان شده است. نبود مستندسازی دسترسی‌ها به عنوان یکی دیگر از تهدیدات و خطرات فنی برای سامانه‌های دیجیتالی اشاره شده است. مستندکردن دسترسی‌ها را می‌توان به عنوان چارچوبی فنی در سامانه‌ها برای رعایت حق مؤلف و دسترسی‌های قانونمند قلمداد کرد. یکی دیگر از مخاطرات فنی، استفاده نکردن از احراز هویت برای تمام بخش‌ها و صفحات محتواست. احراز هویت تا حدود زیادی مانع نقض حقوق پدیدآور می‌شود. در فرایند دیجیتال‌سازی، دو خطر فنی که می‌تواند سامانه‌های دیجیتالی را تهدید کند، نبود کنترل کیفی محتواهای دیجیتالی و کم‌توجهی به مراحل آماده‌سازی شیء دیجیتالی است که در سامانه‌های یادشده کم‌توجهی شده است. تعریف نشدن سیاست کپی‌رایت در فرایند دیجیتال‌سازی سامانه‌های مورد بررسی و دستکاری‌کردن[1] آر ال از مخاطرات فنی دیگری است که در فراداده حقوقی حق مؤلف و حفاظت دیجیتال سامانه‌های دیجیتالی مورد بررسی، نقش تعیین‌کننده‌ای را دارند.

در خصوص سایر سامانه‌ها یعنی سامانه‌های کتابشناختی که 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 دیجیتالی، از لینوکس استفاده می‌شود. خرابکاری عمدی کارکنان در سامانه‌های کتابشناختی مورد بررسی رخ نمی‌دهد. ضمن این که پایین بودن منبع سرورها، بدافزارهای مختلف مانند ویروس‌ها، کرم‌ها و مانند آن، نداشتن پشتیبان از برنامه اصلی، نداشتن وبگاه آینه‌ای به عنوان مخاطرات فنی در سامانه‌های ذکر شده عنوان شده‌اند. سامانه‌های مورد مطالعه از نظر زیرساخت فنی با محدودیت فضای محاسباتی (سرورها، نرم‌افزار و ...) در سامانه‌ها و کمبود فضای نگهداری موقت مواجه هستند. ضمن این که از نرم‌افزار مدیریت حقوق دیجیتال برای اجرای برخی از الزامات فنی به منظور رعایت حق مؤلف استفاده نمی‌شود. همچنین از دست‌دادن پشتیبانی فیزیکی و زیرساختی (مانند قابل توسعه نبودن نرم‌افزار یا از دست دادن تیم پشتیبان نرم‌افزار)، ضعف و نقصان دی.آر.ام (DRM) در نسخه‌برداری و حفاظت طولانی مدت از آثار، مشکل در فضای ذخیره‌سازی و روزآمد نبودن سامانه‌ها به عنوان سایر مخاطرات فنی در زیرساخت‌های فنی محسوب می‌شوند. بررسی دیگر شاخص‌ها نشان داد، استفاده از ته‌نقش آشکار که در کنترل کپی نقش دارد، در سامانه‌های مورد بررسی استفاده نمی‌شود و به عنوان مخاطره فنی بیان شده است. همانند سامانه‌های دیجیتالی، شاخص نبود مستندسازی دسترسی‌ها به عنوان چارچوب فنی در سامانه‌های مورد بررسی به عنوان یک خطر فنی بیان شده است. این شاخص‌ها شاید در حال حاضر به دلیل ارائه اطلاعات کتابشناختی سامانه‌ها کاربردی نداشته باشد، اما

1. Tampering

یکی از اهداف سامانه‌ها معمولاً توسعه و گسترش آن‌هاست که در آینده برای توسعه سامانه‌ها و دیجیتالی کردن منابع اطلاعاتی موجود در سامانه‌ها این نیاز احساس می‌شود.

ارزیابی سامانه‌های کتابشناختی در سایر شاخص‌ها مانند دستکاری‌کردن یو آر ال، استفاده نکردن از احراز هویت برای تمام بخش‌ها و صفحات محتوا، تعریف نشدن سیاست حق مؤلف در فرایند دیجیتال‌سازی، نبود کنترل کیفی محتواهای دیجیتالی و کم‌توجهی به مراحل آماده‌سازی شیء دیجیتالی به عنوان مخاطرات فنی عنوان شده‌اند. هر یک از شاخص‌ها را می‌توان در حفاظت دیجیتالی، احراز هویت، سیاست حق مؤلف و فرایند دیجیتال‌سازی مهم برشمرد. در کل، با ارزیابی انجام شده مشخص شد که همانند سامانه‌های دیجیتالی در حال حاضر مخاطرات و تهدیدات فنی برای این سامانه‌ها وجود دارد. یکی از خواسته‌های کاربران و مدیران سامانه‌ها، توسعه سامانه‌هاست. بنابراین، در این پژوهش به وضعیت آتی و توسعه سامانه‌ها نیز توجه شده است و توجه به برخی مخاطرات فنی پیش‌گفته برای آینده سامانه‌ها ضروری است.

بحث و نتیجه‌گیری

هدف اصلی پژوهش کنونی، بررسی وضعیت سامانه‌های اطلاعاتی سازمان اسناد و کتابخانه ملی ایران از نظر مخاطرات فنی اثرگذار بر حق مؤلف بود. با استفاده از روش تحلیل مضمون تعداد ۱۷ شاخص مخاطرات فنی شناسایی شدند و سپس این شاخص‌ها در اختیار ۱۱ خبره قرار گرفت و پس از دو دور انجام پنل دلفی، توافق بر روی ۱۶ شاخص که شامل ۷ مؤلفه بودند، صورت گرفت. شاخص "توصیفی‌بودن فراداده دوبلین‌کور" از سیاهه وارسی حذف شد. استفاده از روش‌ها و ابزارهای مختلف برای گردآوری شاخص‌های فنی با رویکرد مثلث‌سازی روش‌شناختی به پژوهش اعتبار می‌بخشد. پس از تأیید و نهایی‌شدن سیاهه وارسی، سامانه‌های مورد بررسی با توجه به نوع فعالیت، ساختار و عملکرد آن‌ها در دو گروه دیجیتالی و کتابشناختی قرار داده شدند. سامانه‌های دیجیتال ملی، سامانه‌های نشریات ایران (سنا) و نشریات علمی ایران در گروه دیجیتالی و سامانه‌های بانک نشریات ایران، شبکه مراکز اسناد کشور، فهرستگان نسخ خطی و شبکه کتابخانه‌های کشور در نوع کتابشناختی قرار گرفتند.

در سامانه کتابخانه دیجیتال، سنا و نشریات علمی ایران همانند اغلب کتابخانه‌های دیجیتالی، از ویندوز استفاده می‌شود. در حالی که در سایر سامانه‌ها از لینوکس استفاده شده است. در پژوهش عیدی قلعه‌شیری (۱۳۹۵) استفاده از لینوکس سرور را برای کتابخانه‌های دیجیتالی به دلیل امنیت بالای آن پیشنهاد می‌شود، چرا که امنیت منابع دیجیتالی را مهمتر از امنیت خدمات دیجیتالی بیان می‌کند.

از نظر مخاطرات فنی که سامانه‌های مورد بررسی را تهدید می‌کند، خرابکاری عمدی کارکنان نیز به عنوان یک مخاطره فنی در سامانه‌های کتابشناختی مطرح شده که با پژوهش‌های هان، هوانگ و رن (۲۰۱۶)؛ اوکیکه و آدتورو (۲۰۱۹)؛ حریری و نظری (۱۳۹۱) و رضوانی (۱۳۹۷) همسو ست. اما این شاخص یعنی خرابکاری عمدی کارکنان در سامانه‌های دیجیتالی به عنوان یک خطر فنی تجربه نشده است. سایر شاخص‌های فنی که به عنوان مخاطرات فنی در پژوهش به آن‌ها اشاره شده است، در تمام سامانه‌های مورد مطالعه به کار نرفته است. برخی از مخاطرات فنی را می‌شود فصل مشترک سامانه‌های کتابشناختی و دیجیتالی در نظر گرفت. محدودیت فضای محاسباتی (سرورها، نرم‌افزار و ...) و کمبود فضای نگهداری موقت در سامانه‌ها. این دو شاخص در سامانه‌های دیجیتالی و کتابشناختی برای نگهداری داده‌های بزرگ در سازمان‌ها اهمیت دوچندانی دارند. استفاده از انواع داده و تنوع قالب‌ها در سامانه‌ها می‌تواند بر فضای نگهداری تأثیرگذار باشد. همچنین بدافزارهای مختلف مانند ویروس‌ها، کرم‌ها و مانند آن که در این پژوهش به عنوان یکی از مخاطرات فنی در حق مؤلف تأثیرگذار بود با پژوهش‌های نوروزی (۱۳۹۰) و عیدی قلعه‌شیری (۱۳۹۵) سازگار است. ضمن این که استفاده از شاخص کنترل کپی و برخی از نرم‌افزارها در زیرساخت‌های فنی می‌تواند تا حدود زیادی به حفاظت از حق مؤلف منابع اطلاعاتی کمک نماید. استفاده از ته‌نقش آشکار به عنوان یکی از خطرات فنی در این پژوهش نام برده شده است که با پژوهش پاپی، رضایی شریف آبادی، محمداسماعیل و حریری (۲۰۱۷) مبنی بر استفاده از ته‌نقش آشکار در کنار پنهان آن ناهمخوان است و با استفاده از نرم‌افزار مدیریت حقوق دیجیتال در این پژوهش همسو است. استفاده از فناوری‌های جدید مانند بلاک‌چین و هوش مصنوعی برای جلوگیری از نقض آثار در محیط دیجیتال می‌تواند مانع دورزدن‌های غیرمجاز توسط کاربران شود. نتایج جدیدی که در پژوهش‌های لیو، جانگ، وو و پاتهان (۲۰۲۱) و کمیسیون اروپا (۲۰۲۲) بیان شد و می‌تواند مسیر جدیدی برای حفاظت از کپی‌رایت دیجیتال فراهم کند.

همچنین تعریف نشدن سیاست حق مؤلف در فرایند دیجیتال‌سازی و نداشتن پشتیبان از برنامه اصلی به عنوان دو خطر فنی گریبانگیر سامانه‌های مورد مطالعه است. در پژوهش فرید، وارایچ و افتخار (۲۰۱۳) و پاپی (۱۴۰۲) بر این مهم صحه گذاشتند و نتایج پژوهش آن‌ها با پژوهش کنونی مطابقت دارد. استفاده نکردن از احراز هویت برای تمام بخش‌ها و صفحات محتوا، از دست دادن پشتیبانی فیزیکی و زیرساختی (مانند قابل توسعه نبودن نرم‌افزار یا از دست دادن تیم پشتیبان نرم‌افزار)، روزآمد نبودن سامانه‌ها و مشکل در فضای ذخیره‌سازی و نبود مستندسازی دسترسی‌ها را می‌توان به عنوان مخاطرات فنی دیگری نام برد که هم در سامانه‌های کتابشناختی و هم در سامانه‌های دیجیتالی می‌بایست جدی‌تر مورد توجه قرار گیرند. در پژوهش گریک و هاتینسکی (۲۰۰۷) از دست دادن پشتیبانی فیزیکی و زیرساختی به عنوان تهدید امنیتی نام برده شده

است که با نتایج پژوهش کنونی در ارزیابی سامانه‌ها سازگار است. همچنین در مصاحبه‌های انجام شده به فضای پردازشی و نبود مستندسازی دسترسی‌ها اشاره شد:

"فضای ذخیره‌سازی بله خیلی فضای پردازشی، نیروی انسانی پردازشی برای منابعی که بدون مجوز کرول میشن و جمع‌آوری می‌شن، فضا فقط گرفته و دسترسی بهشون وجود نداره. بی فایده است که یه پردازش دیجیتال و محتوایی روش انجام می‌دین و چون پردازش کتابخانه‌ای نداره و پشتوانه‌ای نداره عملاً قابل استفاده نیست" (مصاحبه کد ۶).

"شاید نکته مهم‌تر بحث مستندسازی باشه این که ما برای هر کدام از فایل‌ها و دیتابیسمون باید مستند دسترسی داشته باشیم این مستند دسترسی مشخص می‌کنه که کیا دسترسی داشته باشن این را شاید ما در لایه فنی خیلی دقت نمی‌کنیم. خیلی وقت‌ها مباحث مربوط به دسترسی چون مباحثی هستن که مستند نشده و در ذهن افراد بسته شده و وقتی من نباشم یه مجموعه فایل می‌مونه که فرد جدید میاد نمی‌دونه چکارش بکنه و دسترسیشون چطور بوده و پروتکلهاش چی بوده که خیلی ما ضربه‌مون از این طریقه". (مصاحبه کد ۳).

هم فضای ذخیره‌سازی و هم مستندسازی دسترسی‌ها به عنوان دو الزام مهم بیان شده و غیبت این دو در سامانه‌ها را یک تهدید فنی برشمردند.

همچنین نبود کنترل کیفی محتواهای دیجیتالی و کم‌توجهی به مراحل آماده‌سازی شیء دیجیتالی در فرایند دیجیتال‌سازی می‌تواند حقوق معنوی پدیدآورندگان آثار را دچار خدشه نماید. اشتباه در مستندسازی فراداده شیء دیجیتالی، منشاء اثر و اشتباهات دیگر در برقراری ارتباط و پیوند بین فراداده و منبع دیجیتالی می‌تواند از جمله تضییع حقوق معنوی پدیدآور را به همراه داشته باشد. یکی از متخصصان در حوزه کتابخانه‌های دیجیتالی چنین بیان نمودند:

"ریسک دیگه‌ای هستش ریسک کیفیت هست. این که کنترل کیفی می‌شه دقیقاً به همین دلیل هست، این هم یکی از مراحل اصلی دیجیتال‌سازی و فرایند آماده‌سازی شیء دیجیتال هست. خود این کنترل کیفی هم خیلی اهمیت داره اگر یک منبعی کنترل کیفی بشه و مشخص بشه مشکلاتی در نمایش، یا توی متادیتا، ناهمخوانی اطلاعات وجود داشته باشه باید اصلاح بشه و اگر این اتفاق نیفته خب ارجاع‌پذیری اون منبع دیجیتال دچار مشکل می‌شه" (مصاحبه کد ۶).

تحلیل حاصل از ارزیابی سامانه‌ها در خصوص مخاطرات فنی تأثیرگذار بر حق مؤلف منابع اطلاعاتی در سامانه‌های مورد مطالعه نشان‌دهنده کمرنگ بودن توجه به پیشگیری از خطرات فنی پیرامون حفاظت از حقوق پدیدآورندگان و ذینفعان آثار در سامانه‌هاست. چرا که اقدامات قانونی و تصویب قوانین حق مؤلف تنها بخشی از حمایت‌های قانونی از پدیدآورندگان آثار را پوشش می‌دهد، بخشی دیگر، مربوط به اقدامات فنی و پیشگیری

از تهدیدات فنی است که نبود آن‌ها نیز نقض حق مؤلف منابع اطلاعاتی در سامانه‌های اطلاعاتی را به همراه دارد. به عبارتی، دقت نظر و در نظر گرفتن ملاحظات فنی برای حق مؤلف منابع اطلاعاتی در سامانه‌ها را می‌توان زیربنای توسعه و گسترش سامانه‌ها در کتابخانه‌ها توصیف کرد که در بلندمدت منافع بسیاری برای کتابخانه‌ها به ارمغان خواهد آورد.

با توجه به یافته‌های حاصل از پژوهش، پیشنهادهای زیر برای بهبود سامانه‌های دیجیتالی و کتابشناختی مورد مطالعه و رفع مخاطرات فنی آن‌ها در حال حاضر و در برنامه توسعه‌ای به شرح زیر است:

۱) تدوین سیاست حق مؤلف برای تمامی منابع دیجیتالی/ استفاده از فراداده حقوقی برای منابع دیجیتال؛ ۲) مستندکردن تمام دسترسی‌ها (مستندکردن نوع دسترسی با توجه به نوع منبع و تاریخ انتشار آن)؛ ۳) استفاده از احراز هویت برای تمام بخش‌ها و صفحات منابع دیجیتال؛ ۴) تهیه پشتیبان از برنامه اصلی؛ ۵) مدیریت در دریافت منابع دیجیتالی غیرقانونی ذخیره‌سازی‌شده (برای کاهش مشکل فضای ذخیره‌سازی)؛ ۶) نظارت بر مراحل آماده‌سازی شیء دیجیتالی؛ ۷) قطع دسترسی خروج دیتا از سرور برای کارکنان سامانه‌ها و ۸) کد کردن یو.آر.ال برای کنترل کپی. هر یک از پیشنهادهای کاربردی اشاره شده می‌تواند تا حدود زیادی از تهدیدات فنی بر حق مؤلف منابع اطلاعاتی در سامانه‌های اطلاعاتی کتابخانه‌ها پیشگیری کند.

سپاسگزاری

از مصاحبه‌شوندگان و شرکت‌کنندگان در پنل دلفی بسیار سپاسگزارم. همچنین از نظرات و پیشنهادهای ارزشمند داوران محترم قدردانی می‌شود.

منابع

آموزگار، سیما؛ نوروزی، علیرضا؛ صراف‌زاده، مریم (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 (۱۴۰۲). ارائه چارچوب پیشنهادی الزامات فنی حمایت از کپی‌رایت منابع اطلاعاتی در سامانه‌های اطلاعاتی سازمان اسناد و کتابخانه ملی ایران؛ با تکنیک دلفی فازی. *پژوهشنامه پردازش و مدیریت اطلاعات*، ۳۹(۲)، ۵۰۳-۵۳۳.

حبیبی، آرش؛ آفریدی، صنم (۱۴۰۱). *تصمیم‌گیری چندشاخصه*. تهران: انتشارات نارون.

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

حسن‌زاده، محمد (۱۴۰۱). سخن سردبیر: متاورس و سرنوشت سامانه‌های اطلاعاتی. فصلنامه *علوم و فنون مدیریت اطلاعات*، ۸(۱)، ۷-۱۴.

رضوانی، شهلا (۱۳۹۷). طراحی الگوی مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتالی. *پژوهشنامه کتابداری و اطلاع‌رسانی*، ۸(۱)، ۳۵۶-۳۳۷.

سازمان ملی استاندارد (۱۳۹۴). *فناوری اطلاعات- فنون امنیتی- سامانه مدیریت امنیت اطلاعات- الزامات: ایزو آی ای سی ۲۷۰۰۱*. تهران: سازمان ملی استاندارد ایران.

عیدی قلعه‌شیری، داود (۱۳۹۵). *ارزیابی چالش‌های امنیتی طراحی کتابخانه‌های دیجیتالی (مطالعه موردی: کتابخانه دیجیتالی آستان قدس رضوی)*. پایان‌نامه کارشناسی ارشد، دانشگاه گیلان.

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

نوروزی، یعقوب (۱۳۹۰). محورهای توسعه کتابخانه‌های دیجیتالی. *فصلنامه تحقیقات اطلاع‌رسانی و کتابخانه‌های عمومی*، ۱۷(۱/ پیاپی ۶۴)، ۱۲۹-۱۵۳.

References

Amouzgar, S., Noruzi, A., & Sarrafzadeh, M. (2022). Analysis of Issues and Challenges of Copyright of Textual Digital Resources from the Viewpoint of Managers of Academic Digital Libraries in Tehran. *Library and Information Sciences*, 25(1), 29-59. (in Persian)

Bowen, G. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, 9(2), 27-40.

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The Use of Triangulation in Qualitative Research. *Oncology Nursing Forum; Pittsburgh*, 41(5), 545-547. Retrieved 1 June 2023 from: https://www.ons.org/pubs/article/233796/download

Eidi Ghaleshiri, D. (2016). *Evaluation of the security challenges of designing digital libraries, case study: Astan Qods Razavi Digital Library*. Master's thesis, Faculty of Engineering, Gilan University. (in Persian)

European Commission (2022). *Study on copyright and new technologies: copyright data management and artificial intelligence*. Luxembourg: Publications Office of the European Union

Farid, G., Warraich, N. F., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science*, DOI: 1-15. 10.1177/01655515231160026.

Geric, S., & Hutinski, Ž. (2007). Information system security threats classifications. *Journal of Information and Organizational Scienc*es, 31.

Habibi A., & Afaridi S. (2022). *Multiple attribute decision making*. Tehran: Narvan Publications. (in Persian)

Habibi, A., Firouzi Jahantigh, F., & Sarafrazi, A. (2015). Fuzzy Delphi Technique for Forecasting and Screening Items. *Asian Journal of Research in Business Economics and Management*, 5(2), 130-143. (in Persian)

Han, Z., Huang, S., Li, H., & Ren, N. (2016). Risk assessment of digital library information security: a case study. *The Electronic Library*, 34(3), 471-487.

Hariri, N., & Nazari, Z. (2012). The information security in Iranian digital libraries. *Library and Information Sciences*, 15(2), 61-90. (in Persian)

Hassanzadeh, M. (2022). Metaverse and the Fate of Information Systems. *Sciences and Techniques of Information Management*, 8(1), 7-14. (in Persian)

Jean-Mary, C. (2020). An Overview of X.509 Certificates: https://www.ibm.com/support/pages/system/files/inline-files/of_x.509_certificates.pdf

Iran National Standards Organization (2015). The technology information- security technical-information security management system - requirements: ISO 27001. Tehran: Iran National Standards Organization. (in Persian)

Ismail, R., & Zainab, A. N. (2011). Information systems security in special and public libraries: an assessment of status. *Malaysian Journal of Library & Information Science*, 16(2), 45-62.

Kokabi, M., & Kohi Rostami, M. (2015). Information security of Web-based systems in Iran Institution of public libraries. *Research on Information Science and Public Libraries*, 21(1). http://publij.ir/article-1-1077-en.html. (in Persian)

Liu, Y., Zhang, J., Wu, S., & Pathan, M. S. (2021). Research on digital copyright protection based on the hyperledger fabric blockchain network technology. *PeerJ Comput. Sci*, 7, e709. DOI: 10.7717/peerj-cs.709

Norouzi, Y. (2011). Axes of Development in Digital Libraries. *Research on Information Science and Public Libraries*, 17(1),129-153. http://publij.ir/article-1-133-en.html. (in Persian)

Okike, B. O. I., & Adetoro. N. (2019). SECURING THE INFORMATION SYSTEMS OF LIBRARIES AND THE INFLUENCE OF TECH-SKILLS OF LIBRARIANS AND USERS. *Education and Information Technologies*, 24(1). DOI: 10.1007/s10639-018-9842-z

Papi, Z. (2023). A proposed framework technical requirements copyright protection for information resources in NLAI information systems: with Fuzzy Delphi Technique. *Iranian Journal of Information Processing and Management*, 39(2), 503-533. (in Persian)

Papi, Z., Rezaei Sharifabadi, S., Mohammadesmaeil, S., & Hariri, N. (2017). Technical requirements for copyright protection of electronic theses and dissertations in INSTD: A grounded theory study. *The Electronic Library*, 35(1), 21-35. DOI: org/10.1108/EL-11-2015-0226

Pistorius, T., & Mwim, O. S. (2019). The impact of digital copyright law and policy on access to knowledge and learning. *Reading & Writing*, 10(1), a196. https://doi.org/10.4102/rw. v10i1.196

Rezvani, S. (2018). Designing an Information Security Management Model in Digital Libraries. *Library and Information Science Research Journal*, 8(1). (in Persian)

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