حفاظت رقمی در کتابخانه های رقمی: مرور راهبردها

میترا صمیعی | سعید رضایی شریف‌آبادی

چکیده

هدف: **شناسایی راهبردهای حفاظت رقمی موجود برای جهت بخشی به مجموعه فعالیت‌های مدیریت شده‌ای است که برای تضمین حفاظت رقمی و دستیابی مستمر به اشیای رقمی به‌کارگرفته می‌شوند.**

روش/ رویکرد پژوهش: در این مقاله از روش کتابخانه‌ای و مرور متون مرتبط با موضوع حفاظت رقمی استفاده شده است. همچنین پژوهش در مورد ارزیابی این راهبردها و معرفی مؤلفه‌های کلیدی برای برنامه‌ریزی در به‌کارگیری این راهبردها برای حفاظت بلندمدت درکتابخانه‌های ملی انجام شده است.

یافته‌ها : راهبردهای متفاوتی برای انواع متفاوت مواد رقمی وجود دارد. در منابع پیچیده و نرم‌افزارهای کاربردی مانند بازی‌های رایانه‌ای حفاظت فناوری و شبیه‌سازی یک رویکرد مناسب است. در منابع ساده و در جایی که دانش مربوط به فرمت کافی است، راهبرد انتقال و بسته‌بندی مناسب است. شناسگرهای دائمی برای دستیابی به منبع در صورت تغییر مکان منبع، مناسب است. تبعیت از استانداردها، پیچیدگی و هزینه‌های راهبردهای حفاظت بلندمدت را کاهش می‌دهدو درنهایت باستان‌شناسی رقمی برای نجات اطلاعات از رسانه‌های منسوخ و خراب، مناسب است.

نتیجه‌گیری: برای حفاظت رقمی موفق، به‌کارگیری ترکیبی از راهبردهای متفاوت مثلاً (انتقال، بسته‌بندی، شناسگرهای دائمی، تبعیت از استانداردها) بایستی مدنظر قرار داده‌شود. بدین معنا که یک راهبرد ممکن است برخی از جنبه‌های راهبردهای دیگر را شامل شود.

کلیدواژه‌ها

حفاظت رقمی، راهبردها، تضمین دستیابی

حفاظت رقمی درکتابخانه‌های رقمی: مرور راهبردها

میترا صمیعی[1] | سعید رضایی شریف‌آبادی[2]

دریافت: ۱۳۸۹/۳/۱۰ پذیرش: ۱۳۸۹/۵/۲۶

مقدمه

منابع رقمی، شبکه جهان‌گستر وب، و اینترنت بخش اساسی و اصلی محیط اطلاعاتی در دنیای کنونی هستند. اغلب کتابخانه‌های ملی نقش مهمی در گردآوری بخش کوچکی از این منابع جهانی و امکان دسترسی به آنها را، در آینده، دارند. با توجه به حجم زیاد اطلاعات و کمبود فضا برای نگهداری آنها، چشم‌انداز آینده به نظر ترسناک می‌آید، ولی نمونه‌های بسیاری در سراسر دنیا نشان می‌دهد که برای حل تمامی این مشکلات می‌توان از طریق برنامه‌ریزی در حوزه حفاظت رقمی اقدام کرد. حفاظت رقمی، فرایندهایی را شامل می‌شود. که هدف آن اطمینان از دسترسی مداوم به منابع رقمی است، این به معنی حفظ تماس با جریان اطلاعات و وسایل خواندن و تفسیر آنها و ارائه مجدد منابعی است که اصل آنها به کاربران ارائه شده است (گاتن بای[3]، ۲۰۰۵، ص ٦٠،٦٦).

شناخت درست خصوصیات منابع و تهدیدهای احتمالی برای دسترسی مداوم به آن منابع، نکته اصلی در حصول این هدف است. رسانه‌های ذخیره‌سازی رقمی، از لحاظ صدمه دیدن و از دست دادن کیفیت، آسیب‌پذیر هستند و شیوه دقیقی برای پشتیبانی و نوسازی سخت‌افزارها و نرم‌افزارها و محمل‌های اطلاعاتی جدید وجود ندارد. لذا شیوه‌ها و راهبردهای جدیدی باید طراحی و اجراشوند (گاتن بای، ۲۰۰۵، ص ٦٧). مسئله دیگر، عرضه اقلام رقمی ذخیره شده در آینده است. اکنون این سؤال مطرح است که چگونه

۱. عضو هیئت علمی سازمان اسناد و کتابخانه ملی جمهوری اسلامی ایران ودانشجوی دکتری کتابداری و اطلاع رسانی دانشگاه آزاد اسلامی، واحد علوم و تحقیقات تهران
m-samiei@nlai.ir
۲. دانشیار گروه کتابداری و اطلاع رسانی دانشگاه الزاهرا ومعاون پژوهشی و آموزشی دانشگاه‌الزهرا
srezaei@alzahra.ac.ir
3. Gatenby

می‌توان ازوجود امکان دیدن و استفاده مواد رقمی در ۵ یا ۱۰ یا ۱۵ سال آینده اطمینان حاصل کنیم؟ بسیاری از کتابخانه‌ها با چالش تضمین دسترس‌پذیری بلندمدت اطلاعات صحیح و معتبر رقمی روبه‌رو هستند. این اطلاعات معمولاً بر روی رسانه‌های رقمی‌ای ذخیره می‌شوند که در معرض کهنگی فناورانه قرار دارند. بنابراین، در صورتی که در مورد اصلاح و نوسازی این رسانه‌های رقمی اقدامی صورت نگیرد، اطلاعات ذخیره شده بر روی آنها غیرقابل بازیابی خواهند شد. با توجه به این حقیقت که اغلب کتابخانه‌ها در حال رقمی‌سازی منابع خود هستند و در آینده نزدیک دیگر سند و شاهد کاغذی در کتابخانه‌ها وجود نخواهند داشت، اهمیت این مسئله را تشدید می‌کند. بنابراین، لازم و ضروری است که کتابخانه‌های رقمی راهبرد مناسب تعریف شده‌ای برای فراهم‌آوری حفاظت بلندمدت و بازیابی اطلاعات رقمی موثق ایجاد کنند (سازمان جهانی استاندارد[4]، ۲۰۰۵، ص۳).

اغلب کتابخانه‌های رقمی احساس می‌کنند که هیچ راهبرد منحصربه‌فردی برای حفاظت بلندمدت و دستیابی به انواع مختلف اشیای رقمی وجود ندارد. به همین دلیل، توسعه راهبردهای گوناگون، همراه با پژوهش در مورد ارزیابی این راهبردها و برنامه‌ریزی برای به‌کارگیری آنها برای حفاظت بلندمدت، مدت زمانی است که در قالب پروژه‌های تحقیقاتی، در بسیاری از کتابخانه‌های ملی رقمی آغاز شده است. همزمان با آن، تمامی کتابخانه‌ها تصریح می‌کنند که اساس ذخیره‌سازی بلندمدت به شیوه‌ها و راهبردهای مناسب برای نوسازی رسانه‌ها و تهیه پشتیبان‌های مناسب نیاز دارد (میور[5]، ۲۰۰۴، ص۹۰– ۹۴؛ مقایسه شیوه‌ها و هزینه‌های حفاظت رقمی[6]، ۲۰۰۵). از جمله راهبردها و شیوه‌های متعارف حفاظت رقمی، که در این مقاله مورد بررسی قرار گرفته است، حفاظت سطح بیت[7]، انتقال اطلاعات[8]، شبیه‌سازی فناوری[9]، حفاظت فناوری[10]، و بسته‌بندی کردن اطلاعات[11] است.

شیوه‌ها و راهبردهای حفاظت رقمی

قبل از پرداختن به راهبردها و شیوه‌های متعارف حفاظت رقمی، لازم است که به یکی از راهبردهای معمول و ساده حفاظت رقمی اشاره‌شود که در اغلب کتابخانه‌ها استفاده می‌شود.

۱. حفاظت سطح ـ بیت، نرمال‌سازی[12]، و تبدیل

معمول‌ترین و قدیمی‌ترین راهبرد حفاظت رقمی استفاده شده در اکثر کتابخانه‌ها، حفاظت بیت‌ها و بایت‌ها یا «حفاظت سطح ـ بیت» است. این نوع راهبرد حفاظت به تأمین ذخیره‌سازی امن همراه با شیوه‌های مناسب نظیر پشتیبان‌گیری و نوسازی اشاره دارد. پس از ذخیره‌سازی امن، بحث ایجاد ممنوعیت و محدودیت‌هایی در زمینه تحویل اطلاعات

4. International Standard Organization(ISO)
5. Muir
6. Comparison of methods & costs of digital preservation
7. Bit-level preservation
8. Information migration
9. Technology emulation
10. Technology preservation
11. Information encapsulation
12. Normalization

به کاربران در فرمت‌های مناسب و استاندارد یعنی (نپذیرفتن تمامی فرمت‌ها) مطرح می‌شود. نرمال‌سازی (تبدیل فرمت‌ها به یک فرمت قابل قبول) دومین شیوه و راهبرد معمول حفاظت رقمی است. متأسفانه کتابخانه‌ها در گزینش فرمت‌های ذخیره‌سازی خود در بسیاری از موارد تحت تأثیر انتشارات رقمی هستند. در حال حاضر، اغلب ناشران فایل‌های خود را در فرمت‌های مورد قبول خود ذخیره می‌کنند، لذا کتابخانه‌های ملی، طبق قانون واسپاری، ناگزیر به پذیرفتن فرمتی هستند که توسط ناشران انتخاب و استفاده شده است. بنابراین، کتابخانه‌ها ناچار هستند آن فایل‌ها را به فرمت مورد استفاده در کتابخانه خود تبدیل کنند. امروزه، گرایش روزافزونی نسبت به ارتقای فرمت‌های مرجح خاصی وجود دارد و ناشران نیز ظاهراً به همکاری برای این کار علاقه‌مندند. ولی در کنار این گرایش، بحث ابرداده‌ها، به‌ویژه ابرداده فنی و نحوه قراردادن آنها در این فرمت‌ها، موضوع مهمی است که باید به آن توجه کرد (ورهییول[13]، ۲۰۰۶، ص ۵۱).

۲. حفاظت از فناوری

این راهبرد، ابزاری برای غلبه بر متروک ماندن فناورانه از طریق حفظ سخت‌افزار و نرم‌افزار به‌کاررفته برای دستیابی مستمر به یک منبع رقمی است. این راهبرد برای تمامی مؤسساتی که لازم است هم سخت‌افزار و هم نرم‌افزار موجود خود را حفظ کنند، کاربرد دارد. این راهبرد به تمامی کتابخانه‌هایی پیشنهاد می‌شود که قصد دارند تجهیزات منسوخ و قدیمی خود را برای الگوسازی و تکثیر پیکربندی قدیمی نرم‌افزار و سخت‌افزار نگهداری کنند. همچنین، شامل حفاظت یک برنامه اولیه کاربردی، نرم‌افزار سیستم عملگرا و سیستم عامل سخت‌افزاری می‌شود. راهبرد حفاظت فناوری یک راهبرد بلندمدت و پویا نیست، بلکه به‌عنوان یک راهبرد کوتاه‌مدت و موقتی مطرح است (کاچرو[14]، ۲۰۰۶، ص۳۳۴– ۳۳۵).

طرفداران این راهبرد براین باورند که برای اجرای آن به یک محیط اولیه نیاز است تا رفتار و همچنین ظاهر و حس شیء رقمی، واقعاً حفظ‌شود. برای برخی از اشیای رقمی، این راهبرد، در کوتاه‌مدت، ممکن است بهترین راه‌حل باشد؛ چرا که تضمین می‌کند که ماده موردنظر از طریق حفظ ابزارهای دستیابی و همچنین خود شیء قابل دسترس است.

هرچند که مشکلات بسیاری از جمله فضا، نگهداری، و هزینه‌ها ممکن است این امر را در بلندمدت غیرممکن سازد؛ باید توجه داشت که تجهیزات رایانه‌ای فرسوده شده و می‌شکنند، سندپردازی ناپدید می‌شود، حمایت فروشنده تجهیزات رایانه‌ای در آینده قطع می‌شود، و رسانه ذخیره‌سازی و همچنین تجهیزات مربوط به استفاده از آنها نابود می‌شوند. بنابراین، به کارگیری راهبردی که برای دستیابی به منابع رقمی به حفظ سخت‌افزار و

13. Varheul
14. Cathro

نرم‌افزار کمک کند، ضرورت می‌یابد (لی، ۲۰۰۲، ص۹۶؛ ورما، ۲۰۰۵، ص؛ مدیریت حفاظت رقمی، راهبردها[۱۵]،۲۰۰۷، ائتلاف حفاظت رقمی[۱۶]، ۲۰۰۹).

۳. شبیه‌سازی فناوری

این راهبرد وجوه اشتراک متعددی با راهبرد حفاظت از فناوری دارد. شبیه‌سازی فناوری نیز وسیله‌ای است جهت غلبه بر متروک ماندن فناورانه سخت‌افزاری و نرم‌افزاری از طریق ایجاد شیوه‌هایی برای تقلید از نظام‌های منسوخ بر روی رایانه‌های نسل آینده است (ائتلاف حفاظت رقمی، ۲۰۰۹؛ کاچرو، ۲۰۰۵؛ شارپ[۱۷]، ۲۰۰۷).

برنامه‌های شبیه‌سازی می‌توانند بر روی سیستم‌های عامل رایانه آینده طراحی شده و پیاده‌شوند. شبیه‌ساز[۱۸] به‌گونه‌ای برنامه‌ریزی شده است تا رفتار سیستم‌های عامل سخت‌افزار قدیمی و نرم‌افزار سیستم عملگرا برای بازی‌ها و فایل‌های قابل اجرا را شبیه‌سازی کند. هرچند که این راهبرد حفاظت، سخت‌افزار در حال فرسودگی و نرم‌افزار سیستم عملگرای اولیه را دربرنمی‌گیرد. راهبرد شبیه‌سازی برای غلبه بر متروک ماندن فناورانه از طریق تقلید نرم‌افزار و سخت‌افزارِ منسوخ شده استفاده می‌شود و بیشترین موفقیت خود را در صنعت بازی‌های ویدئویی و رایانه‌ای داشته است (گرانجر[۱۹]، ۲۰۰۰).

روتنبرگ[۲۰](۲۰۰۰)، یکی از طرفداران رویکرد شبیه‌سازی بر این باور است که شبیه‌سازی تنها شیوه قابل اعتماد برای بازسازی کارآیی ظاهر و حس اصلی و اولیه سند رقمی است. راهبرد شبیه‌سازی امکان می‌دهد که نرم‌افزار اصلی در چارچوب نظام یا نظام‌های ناشناخته آینده اداره‌شود، حتی اگر نرم‌افزار اولیه منسوخ شده‌باشد. روتنبرگ به سه پاره اطلاعاتی اشاره می‌کند که لازم است ثبت‌شوند. این سه پاره اطلاعاتی عبارت اند از:

۱) خود شیء رقمی و نرم‌افزار اولیه (اصلی) که در آن شیء موردنظر ایجاد شده است (شامل سیستم عمل‌کننده)؛

۲) مختصات شبیه‌ساز برای سیستم عامل رایانه‌ای اولیه یا اصلی شیء؛ و

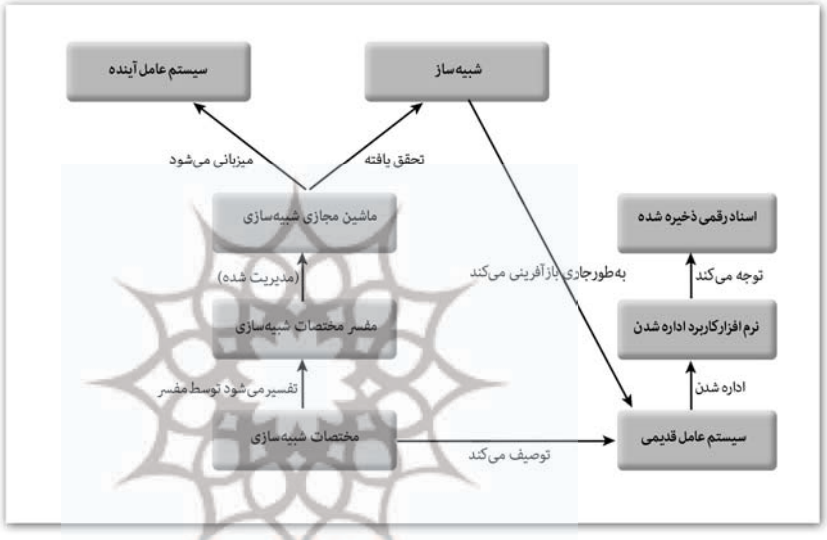
۳) اطلاعات توضیحی مانند ابرداده، منشأ، و دکومانتوسیون برای نرم‌افزار و سخت‌افزار شبیه‌سازی نشده.

همچنین، روتنبرگ به منظور حفظ اشیای رقمی چهار مرحله متوالی را شناسایی کرده است. این چهار مرحله عبارت‌اند از: حاشیه‌نویسی[۲۱]، بسته‌بندی[۲۲]، حرف‌نویسی[۲۳]، و شبیه‌سازی[۲۴]. نخستین مرحله، به ایجاد هرگونه اطلاعات بافتی یا حواشی اشاره می‌کند که جهت باز کردن و استفاده از اطلاعات بسته‌بندی شده ضروری است. در مرحله دوم سه نوع اطلاعات با شیء رقمی برای مدیریت حفاظت بسته‌بندی می‌شود. مرحله سوم، که روتنبرگ آن را حرف‌نویسی نام نهاده است، به چرخه‌های نوسازی رسانه‌ها مربوط

15. Digital preservation management: Strategies
16. Digital Preservation Coalition(DPC)
17. Sharpe
18. Emulator
19. Granger
20. Rothenberg
21. Annotate
22. Encapsulate
23. Transliterate
24. Emulate

می‌شود، یعنی هنگامی که اطلاعات بسته‌بندی شده به رسانه‌های جدید کپی می‌شوند. و مرحله نهایی، آزمودن و استفاده از شبیه‌ساز از طریق اداره آن در چارچوب نظام‌های آینده است. مطابق نظر روتنبرگ، توالی و ترتیب این وقایع باید این امکان را فراهم آورد که اشیای رقمی منسوخ شده در هر نظام رایانه‌ای آینده قابل خواندن باشند (نوردلند[۲۵]، ۲۰۰۷، ص ۷۵– ۷۶).

روتنبرگ، چشم‌انداز مفهومی ارتباطات یا روابط مابین عناصر فرایند شبیه‌سازی را به تصویر می‌کشد که در شکل ۱ قابل ملاحظه است :



شکل ۱

حفاظت مبتنی بر شبیه‌سازی روتنبرگ (لی، ۲۰۰۲، ص ۹۵؛ روتنبرگ، ۲۰۰۰، ص ۸۵)

هندلی[۲۶]، به شبیه‌سازی در حکم یک راهبرد کوتاه‌مدت و یا یک راهبرد تخصصی نگاه می‌کند. واف[۲۷] و دیگران اشاره می‌کنند که نرم‌افزار کاربردی می‌تواند ویروس‌هایی را دربرداشته‌باشد که به مرور زمان منجر به از دست رفتن اطلاعات‌شود. آنها، به‌خصوص، متوجه می‌شوند که شبیه‌سازی مستلزم حفظ بخش قابل توجهی از اطلاعات است (لی، ۲۰۰۲، ص۹۶؛ راهنمای عملی خوب...[۲۸]، ۲۰۰۴؛ ورما، ۲۰۰۵، ص ۱۲۵– ۱۲۸).

یکی از معروف‌ترین و موفق‌ترین پروژه‌های حوزه حفاظت رقمی، که از راهبرد شبیه‌سازی استفاده کرده است، پروژه کامیلئون[۲۹] (آرشیوسازی خلاق در میشیگان و لیدز، شبیه‌سازی مواد قدیمی بر روی مواد جدید) است. در این پروژه، شبیه‌سازی به‌عنوان وسیله‌ای مورد بررسی قرار گرفته است که به حفظ کارآیی، ظاهر، و حس اولیه اشیای رقمی کمک می‌کند. اگرچه در راهبرد شبیه‌سازی فقط بخشی از کارآیی، ظاهر، و حس ماده می‌تواند بازسازی‌شود. معمولاً شبیه‌سازها نیز در معرض متروک شدن فناورانه قرار

25. Nordland
26. Hendley
27.Waugh
28.Goode practice guide for developers of culture heritage web services:Digital preservation
29. CAMILEON, http://www.si. Unich. Edu/ CAMILEON/ html.

دارند، بنابراین، لازم است که شبیه‌سازها روزآمدشوند تا بتوانند بر روی رایانه‌های جدید قابل استفاده باشند. در واقع، باید گفت که با هر تغییر الگویی در فناوری (مثلاً تغییر دیسک لرزان به لوح‌های فشرده یا وردستار[30] به ورد مایکروسافت[31]) یک شبیه‌ساز جدید باید ساخته‌شود (نوردلند، ۲۰۰۷، ص۷۷– ۷۸).

۴. انتقال اطلاعات

یکی از رایج‌ترین و متداول‌ترین شیوه‌ها و راهبردهای مدیریت و حفاظت اشیای رقمی انتقال اطلاعات است (ائتلاف حفاظت رقمی، ۲۰۰۹؛ لی،۲۰۰۲، ص۹۶– ۹۷؛ ورهییول، ۲۰۰۶، ص۵۲– ۵۳). راهبرد انتقال اطلاعات رقمی بر جابه‌جایی دوره‌ای مواد رقمی از یک پیکربندی نرم‌افزاری و سخت‌افزاری به دیگری و یا از یک نسل فناوری رایانه به یک نسل دیگر است. هدفِ انتقال، حفظ تمامیت اشیای رقمی و حفظ‌توانایی کاربران در بازیابی و استفاده از اشیای رقمی، به‌رغم فناوری دائماً در حال تغییر است.

برای تضمین آنکه اشیای رقمی به درستی انتقال یافته و تبدیل‌شوند لازم است خط‌مشی‌ها، رویه‌ها، و دستورالعمل‌های مکتوبی برای آنها ایجادشود؛ نظارت کیفی بر اجرای آن انجام گیرد؛ رویه‌های انتقال با سندپردازی بسیار دقیق و جدی انجام‌شود؛ ودر نهایت ابرداده حفاظتی نیز ثبت‌شود (نوردلند، ۲۰۰۷، ص ۸۱ – ۸۲). انتقال توسط مگی جونز و نایل بیگری[32] در دستنامه مدیریت حفاظت مواد رقمی[33] اینگونه تعریف شده است:

«انتقال وسیله‌ای است جهت غلبه بر متروک ماندن فناورانه از طریق منتقل ساختن منابع رقمی از یک نسل نرم‌افزاری یا سخت‌افزاری به نسل دیگر. هدف انتقال، حفظ محتوای معنوی اشیای رقمی و نگهداری قابلیت دستیابی برای کاربران، به منظور بازیابی و استفاده از آن است. انتقال، از آن جهت با نوسازی رسانه‌های ذخیره‌سازی متفاوت است که در راهبرد انتقال تولید یک نسخه رقمی دقیق و یا تکثیر ویژگی‌های اصلی، ظاهر، وحس نسخه رقمی و حفظ و تناسب آن نسخه با نسل جدید فناوری همواره ممکن نیست» (بیگری و جونز، ۲۰۰۸).

تا این تاریخ، راهبرد انتقال به‌عنوان یک شیوه مؤثر حفظ سند رقمی و حفظ دستیابی به اطلاعات آزمایش خود را پس داده است. راهبرد انتقال باید هر ۲ تا ۳ سال یک بار انجام‌شود، و نیز انتقال فرمت‌های ساده به‌طور خودکار انجام‌شود. زیرا در این صورت هزینه‌های نیروی یدی کاهش می‌یابد و راهبرد انتقال برای کتابخانه می‌تواند مقرون به‌صرفه‌باشد.

در فرایند انتقال، سند اصلی یا مادر باید حفظ‌شود و همچنین باید فناوری خاصی

30. Wordstar
31. Microsoft word
32. Maggie Jones & Neil Beagrie
33. Preservation management of digital materials: A Hand book

وجود داشته‌باشد قادر به خواندن دقیق سندباشد. در کنار آن باید یک نسخه دستیابی یا پژوهشی ایجادشود و در یکی از فرمت‌های فایل که برای حفاظت بلندمدت توصیه شده مانند پی.دی.اف/ اِی یا اسکی[۳۴] حفظ‌شود. یک رویکرد جدید برای تبدیل و انتقال منابع، جدا ساختن محتوا از ارائه است. بدان معنا که برای اسناد متنی، بهتر است محتوا به یک فرمت مانند اسکی یا یونی کد[۳۵] تبدیل‌شود تا به‌صورت تمام‌متن جست‌وجوپذیرباشد. حال آنکه برای حفظ حس و ظاهر سند موردنظر می‌توان آن را در فرمت تی.آی.اف.اف. ذخیره کرد و نشان داد. کاربر، فرمت تی.آی.اف.اف. یا نسخه دستیابی را بر روی صفحه نمایشگر می‌بیند، اما می‌تواند آن را در نسخه محتوا جست‌وجو کند.

بنابراین، لازم است در راهبرد انتقال سه نسخه از سند ذخیره، نگهداری، و حفظ‌شود:

۱) نسخه محتوا،

۲) نسخه ارائه، و

۳) نسخه اصلی یا مادر.

در این صورت، این رویکرد نتایج بهتر جست‌وجو را میسر می‌سازد و بسامد موارد اشتباه را به حداقل می‌رساند. از آنجاکه ذخیره‌سازی و نگهداری سند در فرمت پی.دی.اف/ اِی ارزان است، بهتر است که محتوا در فرمت پی.دی.اف/ اِی ذخیره‌شود. اگر سند، با استفاده از دستگاه‌های اسکنر و دوربین رقمی اسکن‌شود و به‌صورت تصویری در فرمت پی.دی.اف. ذخیره‌شود، قابل جست‌وجو نخواهد بود مگرآنکه از نرم‌افزار اُ.سی.آر. (تشخیص کاراکتر نوری)[۳۶] برای جست‌وجو در متن استفاده‌شود. به دنبال انتقال فایل‌ها باید یک چک سام[۳۷] تکمیل‌شود تا تأیید کند که درحین انجام انتقال، هیچ‌یک از فایل‌ها از بین نرفته است. همچنین، نتایج انتقال باید در ابرداده فایل ثبت‌شود (نوردلند، ۲۰۰۷، ص ۸۵– ۸۷).

۵. انواع انتقال

چهار نوع انتقال رقمی اولیه شناسایی شده‌اند که عبارت‌اند از:

۱. نوسازی[۳۸]: نوعی انتقال رقمی است که برای دربرگرفتن اِی.آی.پی‌ها و مدیریت و دستیابی با کپی کردن بیت‌ها به رسانه جدید مورد استفاده قرار می‌گیرد. در نوسازی احتمال کمی برای فقدان اطلاعات وجود دارد؛ زیرا هیچ‌یک از بیت‌های مورد استفاده اطلاعات اِی.آی.پی. برای پشتیبانی از موجودی و دستیابی به ای.آی.پی‌ها تغییر نکرده است.

۲. تکثیر[۳۹]: نوعی انتقال رقمی است و در جایی انجام می‌شود. که اطلاعات بسته‌بندی، اطلاعات محتوا، و اطلاعات توصیفی دستخوش هیچ تغییر و تحولی نمی‌شود. در فرایند

34. ASCII
35. Unicode
36. OCR (Optical Character Recognition)
۳۷. یك ارزش الگوریتمی است که برای چك کردن داده‌های انتقال داده شده برای اشتباهات و اغلاط استفاده می‌شود.
38. Refreshment
39. Replication

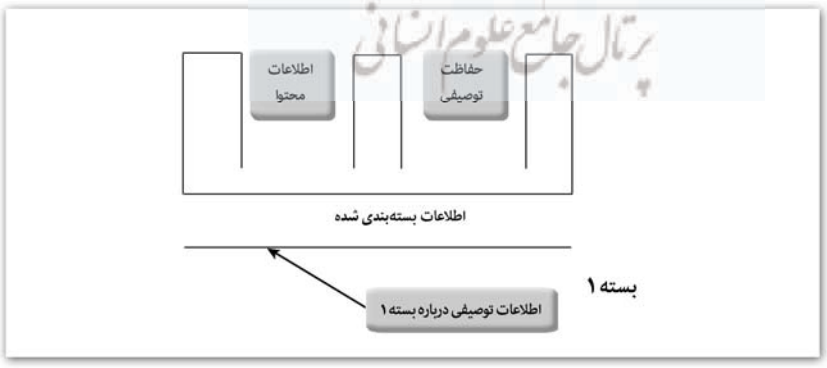
تکثیر احتمال کمی برای فقدان اطلاعات وجود دارد، زیرا بیت‌های مورد استفاده برای انتقال این اشیای اطلاعاتی به همان رسانه و یا گونه جدیدی از رسانه، حفظ می‌شوند.

۳. بسته‌بندی‌دوباره[۴۰]: نوعی انتقال رقمی است و زمانی رخ می‌دهد که در بیت‌های اطلاعات بسته‌بندی، تغییری در حال وقوع است.

۴. تبدیل[۴۱]: نوعی انتقال رقمی است و زمانی انجام می‌گیرد که در اطلاعات محتوا و یا بیت‌های اطلاعات توصیفی حفاظت تغییری در حال وقوع است. در این نوع انتقال سعی بر آن است که محتوای کامل اطلاعات حفظ‌شود (کمیته مشورتی[۴۲]...، ۲۰۰۲).

۵. بسته‌بندی‌کردن: راهبرد دیگر حفاظت رقمی، بسته‌بندی کردن است. این نوع راهبرد عبارت است از کنار هم قرار دادن یک منبع رقمی و هر آنچه که برای حفظ دستیابی به آن منبع لازم است. بسته‌بندی کردن، اطلاعات لازم برای حفظ یک سند را گروه‌بندی می‌کند (ائتلاف حفاظت رقمی، ۲۰۰۹).این اطلاعات ممکن است شامل ابرداده، ناظرها[۴۳] یا کارت‌خوان‌ها[۴۴]، و فایل‌های جداگانه‌ای‌باشد که منبع رقمی را تشکیل می‌دهد. بسته‌بندی کردن نیز همچون شبیه‌سازی، راهبرد موفقی برای حفاظت رقمی بوده است. در استرالیا، اساس و پایه راهبرد اسناد الکترونیکی ویکتوریایی یا ورس[۴۵]، فرمت شیء بسته‌بندی شده ورس به نام وی.ای.اُ.[۴۶] است که برای مدیریت و حفاظت اشیای رقمی در آرشیو رقمی پایدار کاربرد دارد.

اشیای بسته‌بندی شده را می‌توان در الگوی مرجع اُ.ای.آی.اس. مشاهده کرد. معمولاً بسته اطلاعاتی، که شامل اطلاعات محتوا و اطلاعات توصیفی حفاظت است، در داخل اطلاعات بسته‌بندی پیچیده می‌شود. مطابق الگوی مرجع اُ.ای.آی.اس. اطلاعات محتوا و اطلاعات توصیفی حفاظت به‌عنوان اطلاعات بسته‌بندی شده درنظر گرفته می‌شوند. شکل ۲ پیوند بین ظرف (یعنی مفهوم یا بسته) و اطلاعات توصیفی در الگوی مرجع اُ.ای.آی.اس. را از طریق فلش نشان می‌دهد:



40. Repackaging
41. Transformation
42. Consultant Committee for Space Data Systems
۴۳. Viewer= برنامه‌ای کاربردی که اطلاعاتی را چاپ می‌کند مانند برنامه‌ای که تصاویر ذخیره شده را به صورت GIF یا JPEG نمایش می‌دهد.
۴۴. Reader= یك وسیله ورودی که معمولاً برای اهداف شناسایی استفاده می‌شود. و اطلاعات کدبندی شده در دو شیار روی کارت پلاستیکی مانند یك کارت اعتباری یا کارت شناسایی پرسنلی را می‌خواند.
45. The Victorian Electronic Records Strategy (VERS)
46. VERS Eccapsulated Object (VEO)

شکل ۲

مفاهیم و ارتباطات بسته اطلاعاتی (یولمان،۲۰۰۴)

پس از آنکه رویکرد بسته‌بندی اتخاذ شد، اطلاعات توصیفی باید در شیء بسته‌بندی، گنجانده شده و در یک مکان ثبت و ذخیره‌شوند؛ مانند مکان‌هایی که برای ثبت ابرداده‌ها مورد استفاده قرار می‌گیرند. علاوه بر مدیریت شیء بسته‌بندی شده در داخل آرشیوهای رقمی، پیوندهای بین اطلاعات توصیفی و شیء نیز باید حفظ‌شوند تا دستیابی به فایل‌ها تضمین‌شود. از آنجا که اشیای بسته‌بندی شده تمامی اطلاعات لازم برای حفاظت و مدیریت بلندمدت شیء رقمی را حفظ می‌کنند، منابع بیشتری بر روی عناصر و اطلاعات لازم برای دستیابی و حفاظت متمرکز می‌شوند (لی، ۲۰۰۲، ص۹۶– ۹۷؛ نوردلند، ۲۰۰۷، ص ۸۰).

از آنجا که بسته‌بندی کردن، به‌عنوان راهبرد حفاظت رقمی، در معرض متروک شدن فناورانه است، به نوعی مدیریت بلندمدت حفاظت مانند راهبرد شبیه‌سازی نیاز دارد (ائتلاف حفاظت رقمی، ۲۰۰۹؛ چن[47]، ۲۰۰۲، ص ۲٤).

سایر راهبردهای حفاظت

شامل چهار راهبرد به شرح زیر است:

۱. شناسگرهای دائمی: ابزاری است جهت مکان‌یابی یک شیء رقمی حتی زمانی که جای آن تغییر می‌کند. نمونه‌های شناسگرهای دائمی عبارت است از نام‌های منبع یکسان (یو.آر.ان.)[48]، دستگیره‌ها[49]، شناسگرهای شیء رقمی (دی.اُ.آی.)[50]، و مکان‌یاب‌های منبع یکسان ثابت (پی.یو.آر.ال.)[51] (ائتلاف حفاظت رقمی، ۲۰۰۹).

۲. تبدیل به فرمت آنالوگ پایدار: راهبرد تبدیل به فرمت آنالوگ پایدار، عبارت است از تبدیل منابع رقمی ارزشمند مشخصی به یک رسانه آنالوگ پایدار حفاظتی مانند کاغذ و یا ریزفیلم و یا خیلی جدیدتر دیسک نیکلی قابل خواندن توسط میکروسکوپ الکترونیکی. این فرایند نمی‌تواند در حکم یک راهبرد مطرح‌شود، ولی در حال حاضر عملی‌ترین راهبرد برای حجم کم منابع است (ائتلاف حفاظت رقمی، ۲۰۰۹).

۳. باستان‌شناسی رقمی[52]: گاهی ممکن است نجات منبعی که انتقال نیافته اما دربردارنده اطلاعات باارزشی است، ضرورت یابد. گاهی بر روی دیسک‌ها یا نوارهای قدیمی داده‌هایی کشف می‌شوند که به‌طور اتفاقی حفظ شده‌اند و باستان‌شناسی داده‌ای، با موفقیت آنها را نجات داده است (دیگان و تانر، ۱۳۸۲، ص ۲۸۵–۲۸٦). نجات منابع رقمی، باستان‌شناسی رقمی است که در نتیجه متروک شدن فناورانه و یا تنزل رسانه‌ها غیرقابل دسترس شده‌اند. باستان‌شناس رقمی به خودی خود یک راهبرد نیست، بلکه جایگزینی برای راهبرد حفاظتی است و زمانی رخ می‌دهد که مواد رقمی از حیطه یک برنامه حفاظت نظام‌مند خارج شده‌اند (ائتلاف حفاظت رقمی، ۲۰۰۹).

47. Chen
48. Uniform Resource Names (URNs)
۴۹. Handles= اشاره‌گری که به یك اشاره‌گر دیگر اشاره می‌کند یعنی متغیری که دارای آدرس متغیر دیگر است.
50. Digital Object Identifiers (DOI's)
51. Persistent Uniform Resource Locators (PURL)
52. Digital Archaeology

بین باستان‌شناسی داده‌ای و شبیه‌سازی فناوری شباهت‌های بسیاری وجود دارد. درواقع، شبیه‌سازی فناوری به‌عنوان روشی برای بازیافت منابع گمشده ارائه شده است؛ ولی باستان‌شناسی رقمی آخرین راهبرد برای بازیافت و روزآمد کردن داده‌ها و برنامه‌های باارزش است و برای دسترسی دوباره به اطلاعات، ساختارهای داده‌ای و ارتباطی را با تلاش بسیار ایجاد می‌کند و طاقت‌فرساترین روش نجات منبع رقمی است (دیگان و تانر، ۱۳۸۲، ص۲۸۶).

۴. تبعیت از استانداردها[53]: عبارت است از پیروی از استانداردهای باز پایدار و پذیرفته شده در سطح وسیع، هنگام تولید و آرشیوسازی منابع رقمی. اینها به سیستم‌های عامل نرم‌افزار و سخت‌افزار خاصی متصل نیستند، پس می‌توانند عدم دسترس‌پذیری منبع رقمی را به‌واسطه متروک ماندن فناورانه به تعویق بیندازند.

نتیجه‌گیری

در این مقاله، راهبردهای حفاظت رقمی به تفضیل مورد بحث قرار گرفتند. هریک از این راهبردها و شیوه‌ها دارای معایب و محاسنی هستند. در این مقاله به معایب و مزایای چهار راهبرد اصلی پرداختیم که به‌طور خلاصه در جدول ۱ نشان داده شده‌اند.

راهبردهای متفاوتی برای انواع مواد رقمی وجود دارد. در منابع پیچیده و نرم‌افزارهای کاربردی مانند بازی‌های رایانه‌ای، و نیز در جایی که دانش کافی در مورد فرمت اطلاعات رقمی موجود نیست و ظاهر و حس اطلاعات رقمی از اهمیت برخوردار است؛ حفاظت فناوری و شبیه‌سازی رویکرد مناسبی است.

از سوی دیگر، انتقال یا بسته‌بندی کردن برای منابع رقمی در جایی مناسب است که دانش مربوط به فرمت کافی است و منبع موردنظر نسبتاً ساده است. انتقال، به‌طور اخص، برای منابعی مناسب است که فعالانه مورد دسترسی قرار گرفته و مدیریت می‌شوند. فرایند بسته‌بندی کردن نیز برای منابعی مناسب است که به احتمال بسیار ضعیف به‌طور فعال مورد دسترسی قرار می‌گیرند. شناسگرهای دائمی، امکان دستیابی به یک منبع را ـ حتی در صورتی که جای آنها تغییر کند ـ فراهم می سازد و برای اشیای رقمی استفاده از آنها لازم و ضروری است. تبعیت از استانداردها، پیچیدگی و هزینه‌های راهبردهای حفاظت بلندمدت را کاهش می‌دهد. همچنین، انتقال داده‌ها را ساده می‌کند و می‌تواند هم برای پدیدآورندگان و هم برای خود حفاظت بلندمدت مفید واقع‌شود و به توزیع بخشی از کوشش‌ها در چرخه حیات منابع کمک کند. باستان‌شناسی رقمی داده‌ها نیز می‌تواند اطلاعات را از رسانه‌های منسوخ و خراب نجات‌دهد. شکل ۳ یک نمودار شماتیک را برای انتخاب

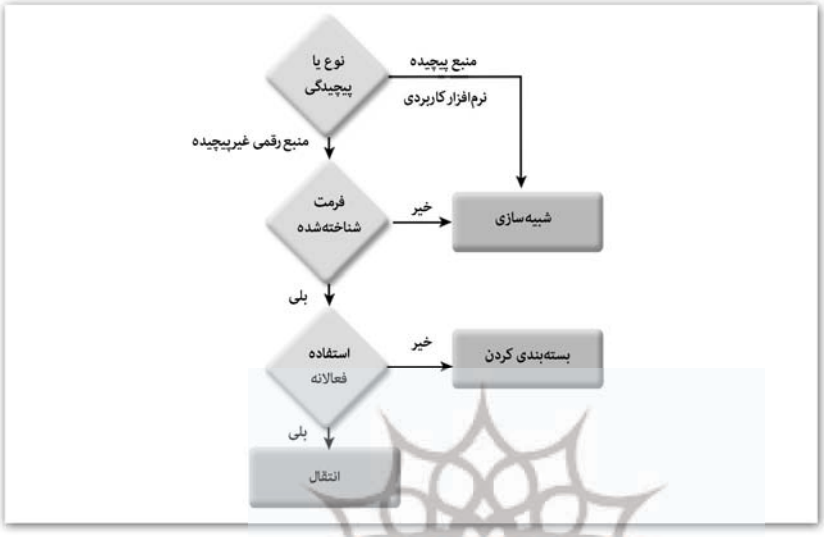
53.Reliance on standards

راهبرد	مزایا و محاسن	معایب	حیطه و قلمرو	ملزومات
حفاظت فناوری	۱. این راهبرد ذخیره‌سازی، کارآیی، ظاهر و حس اولیه سند را حفظ می‌کند. ۲. ذخیره‌سازی به شکل تأخیری انجام می‌گیرد. ۳. عملی‌ترین راهبرد ذخیره‌سازی منابع رقمی پیچیده است.	۱. راهبرد کوتاه مدت و موقتی است. ۲. پشتیبانی فنی در این راهبرد در مدت نسبتاً کوتاه قطع می‌شود. ۳. دستیابی در بلندمدت در این راهبرد مشکل‌آفرین خواهد شد.		۱. خط‌مشی‌ها و دستورالعمل‌های مربوط به دستیابی ۲. دکومانتاسیون نرم‌افزار و سخت‌افزار حفظ شده ۳. ابرداده لازم جهت حفظ نرم‌افزار و سخت‌افزار
شبیه سازی فناوری	۱. این راهبرد کارآیی، ظاهر و حس نسخه اولیه سند را بازسازی می‌کند؛ ۲. از هزینه‌های تکراری مرتبط با انتقال اجتناب می‌کند. ۳. ممکن است بهترین چشم‌اندازها را برای منابع رقمی پیچیده‌تر ارائه دهد.	۱. هنوز در مقطع پژوهش است و به آزمون و سنجش عملی بیشتری نیاز دارد. ۲. بخشی از کارآیی، ظاهر و حس اولیه سند را می‌تواند شبیه‌سازی کند. ۳. بسیار هزینه‌بر و گران است. ۴. لازم است شبیه‌سازهای جدید همراه با تغییرات فناورانه در سخت‌افزار و نرم‌افزار ساخته شوند، که این هزینه‌ها حتی از هزینه‌های ذخیره‌سازی و انتقال‌های تکراری نیز فراتر می‌رود. ۵. چالش‌های حقوق مالکیت معنوی و به‌ویژه حق مؤلف با این راهبرد حل نشده است. ۶. نیاز به دکومانتاسیون دقیق ملزومات و نیازهای نرم‌افزاری و سخت‌افزاری دارد.	۱. نرم‌افزار کاربردی ۲. منابع رقمی پیچیده ۳. منابعی که دارای کمبود دانش کافی هستند. ۴. منابعی که ارزش آنها نامعلوم و کاربرد آنها در آینده نامحتمل است ۵. منابعی که ظاهر و حس آنها مهم است.	۱. ذخیره‌سازی و شیوه‌های نگهداری مناسب؛ ۲. خط‌مشی‌ها دستورالعمل‌های مکتوب؛ ۳. ابرداده حفاظت؛ ۴. دکومانتاسیون مبسوط راجع به مختصات نرم‌افزاری و سخت‌افزاری
انتقال اطلاعات	۱. طراحی دقیق شیوه‌ها و رویه‌های انتقال. ۲. در حال حاضر راهبرد مرجح برای بیشتر آرشیوهای رقمی است. ۱.۲ راهبرد انتقال با تغییرات فن اورانه و ساده شدن آنها می‌تواند ساده انجام گیرد. ۳. دستیابی فعال و مدیریت حفاظت را تقویت می‌کند.	۱. نیاز به برنامه نرم‌افزاری خاص برای انتقال منابع پیچیده. ۲. بسیار وقت‌گیر و پیچیده است. ۳. احتمال دارد در فرایند انتقال بخشی از کارآیی، ظاهر و حس اولیه شیء رقمی از دست برود. ۴. ممکن است در فرایند انتقال تمامیت مواد اصلی از بین برود. ۵. راهبرد انتقال برای منابع رقمی پیچیده با از دست رفتن جزئی اطلاعات قابل اجراست. ۶. معمولاً در فواصل معینی در سراسر (حیات) یک منبع رقمی رخ می‌دهد.	۱. منابعی که فعالانه مورد دستیابی و مدیریت قرار می‌دهند. مثلاً داده‌ها یا پایگاه داده‌های علمی ۲. منابعی که فرمت آنها به زائد اندازهٔ کافی شناخته و متعارف است.	۱. خط‌مشی‌های مکتوب و دستورالعمل‌ها شامل خط‌مشی گزینش موادی که باید انتقال داده‌شوند. ۲. روش‌های کنترل کیفیت دقیق و جدی و سنجش برنامه انتقال با مقیاس چک سام ۳. سندپردازی سفت و سخت برای شیوه‌ها و رویه‌های انتقال ۴. ابرداده حفاظت. ۵. نگهداری نسخه‌هایی از منبع رقمی در فرمت اصلی. در صورتی که منبع موردنظر از دست رفت و یا آنکه در انتقال دستخوش دگرگونی شد.
بسته بندی کردن اطلاعات	۱. این راهبرد تضمین می‌نماید که تمامی اطلاعات بسته‌بندی شده برای دستیابی به شیء رقمی حفظ می‌شود؛ ۲. می‌تواند بالقوه بر برخی از عیوب اصلی راهبردهای دیگر غلبه کند؛ ۳. وسیله کارآمدی برای متمرکز ساختن توجه بر روی عناصری است که برای دستیابی لازم و ضروری هستند.	۱. می‌تواند فایل‌های بسیار بزرگی با تکثیر زیاد (نظیر ناظرها) در سراسر مجموعه ایجاد کند. ۲. در این راهبرد، نرم‌افزار بسته‌بندی کردن در معرض متروک شدن فناورانه است.	۱. منابعی مناسب هستند که فرمت‌های آنها به اندازه کافی متعارف و شناخته شده هستند	——

جدول ۱

معایب و مزایای راهبردهای مهم و اصلی حفاظت رقمی

شیوه‌های مناسب و استاندارد حفاظت منابع رقمی و مطابق با نوع و پیچیدگی اطلاعات رقمی و همچنین دسترس‌پذیری فرمت داده و کاربرد آن نشان می‌دهد (البته در این شکل سه راهبرد اصلی و کاربردی در اکثر کتابخانه‌ها، مدنظر قرار گرفته است):



شکل ۳

نمودار شماتیک برای انتخاب راهبردهای حفاظت رقمی

همان‌طور که اشاره شد، هدف حفاظت رقمی بلندمدت، تضمین دستیابی مداوم به اطلاعات رقمیِ ذخیره شده است. کاربران آینده قادر خواهند بود که به اطلاعات رقمی دستیابی پیدا کنند، اطلاعاتی که توسط کتابخانه‌های رقمی از طریق محیط‌های رایانه‌ای خود و یا وسایل قابل حمل خواندن حفظ خواهند شد. این بدان معناست که شاید لازم‌باشد اطلاعات رقمی، برای حفاظت بلندمدت رقمی، منتقل‌شوند؛ حتی اگر برخی شیوه‌های شبیه‌سازی را از قبل به کار بسته شده باشند. بنابراین، برای حفاظت و دستیابی بلندمدت به منابع رقمی گاهی اوقات لازم است که چندین شیوه و راهبرد حفاظت رقمی را همزمان با هم به‌کارگیریم. به عبارت دیگر، برای حفاظت رقمی موفق، به‌کارگیری ترکیبی از راهبردهای متفاوت (انتقال، بسته‌بندی، شناسگرهای دائمی، تبعیت از استانداردها) باید مدنظر قرار داده‌شوند. بدین معنا که یک راهبرد ممکن است برخی از جنبه‌های راهبردهای دیگر را شامل‌شود.

تبعیت از استانداردها برای اغلب راهبردها، نظیر حفاظت فناوری، شبیه‌سازی، و بسته‌بندی، موردنیاز هستند. استانداردهای متعارف مبتنی بر شیوه‌های گوناگون رمزگذاری الگوها، بسته به انواع مختلف منابع رقمی متفاوت هستند. ایکس.ام.ال.، به واسطه به رسمیت شناخته شدن محاسن خود مانند عدم وابستگی به نرم‌افزار و سخت‌افزار و همچنین اشاعه

یا اعتلای گسترده آن، هم اکنون به‌عنوان یک استاندارد جهانی در عرصه‌های مختلف در حال استفاده است. استانداردهای مبتنی بر ایکس.ام.ال.، پشتیبانی از اینترنت و وب را تسهیل می‌نماید. برای مثال، استاندارد ارائه رقمی کتاب‌های کاغذی مبتنی بر ایکس.ام.ال. است.

از آنجا که انتظار می‌رود کاربرد ایکس.ام.ال. در حوزه‌های میان‌کنشی و تبادلی داده‌ها رشد و توسعه پیدا کند، به‌کارگیری استانداردهای حفاظت رقمی مبتنی بر ایکس.ام.ال.، مبرم و ضروری خواهد بود. استانداردهای حفاظت رقمی مبتنی بر ایکس.ام.ال.، هنگام اجرا یا پیاده‌سازی یک نظام حفاظت یک فرمت استاندارد و مطلوب خواهند بود.

یکی از موفق‌ترین راهبردهای حفاظت رقمی یعنی انتقال، در سازمان جهانی استاندارد تأیید و در سال ۲۰۰۵ با شماره ایزو/تی.آر۱۸۴۹۲منتشر شد. در این استاندارد به عناصر و شیوه‌های انتقال منابع رقمی مرکب از داده‌های ساده پرداخته شده است. جامعه حفاظت به‌تازگی شروع به پرداختن به بحث شیوه‌های انتقال اشیای رقمی پیچیده‌تر کرده است. برای آزمودن کارآیی و قابلیت اجرای رویکردهای گوناگون نسبت به انتقال و همچنین سایر راهبردهای حفاظت رقمی، تعیین هزینه‌های مرتبط با این رویکردها و وضع ملاک‌ها یا معیارها و بهترین طرز عمل‌ها و نیزانجام پژوهش‌های بیشتر راجع به این راهبردها لازم و ضروری است.

منابع

دیگان، ماریلین؛ تانر، سیمون (۱۳۸۲). ***آینده دیجیتالی کتابخانه‌ها: راهبردهایی برای عصر اطلاعات***. ترجمه عباس گیلوری. تهران: دبیزش، چاپار.

Beagrie, Neil; Jones,Maggie (2008). "Preservation management of digital materials: The handbook". from; http://www.dpconline.org/graphics/ handbook

Cathro, Warwick (2005)."The role of a national library in supporting research information infrastructure". ***Ifla Journal***, 32 (4):333 – 339.

Chen, S. S. (2000). "The paradox of digital preservation". ***IEEE Computer***, 34 (3): 24 - 28.

"Comparison of methods & costs of digital preservation" (2005). from: http://www.dig-preservation-good-grad1.mht

Consultant committee for space data systems (2002). "Reference model for an open archival information system". from: http://ssdoo. gsfc.nasa.gov/nost/wwwclassic/....

Digital preservation coalition (2009). "Organisational activities: Storage and presservation". from: http:// www.dpconline.org/ graphics/ orgact/ storage.html

"Digital preservation management: Strategies" (2007). from: http:// www. icpsr.umich.edu/ dpm/dpm-eng/terminology/strategies.html

Gatenby, P. (2005). "Getting started: What needs to be in place to maintain access to digital collections". from: http://archive.ifla. org/ vifla71/papers/032e-Gatenby.pdf

"Goode practice guide for developers of culture heritage web services: Digital preservation". (2004). from: http://www.ukoln.ac.uk/interop-focus/ gpg/ Preservation/

Granger, J. A. (2000). ***Adapting preservation policy in archives to the digital age***. Canada: Queen's University

International Standard Organization (2005). "Long - term preservation of electronic document-based information". ISO/TR 18492. Switzerland: ISO.

Lee, Kyong-Ho … [et.al]. "The state of the art and practice in digital preservation". ***Journal of Research of the National Institute of Standards and Technology***, 107 (1): 93 – 106.

Muir, Adrienne. "Digital preservation: Awareness, responsibility and rights issues". ***Journal of Information Science***, 30 (1): 73 - 92. from: http://jis.sagepub.com/cgi/content/abstract/30/1/73

Nordland,Lori Podolsky (2007)."The long and short of IT: The international development research centre as a case study for a long-term digital preservation strategy".A Thesis MA.Winnipeg:University of Winnipeg and University of Manitoba.

Rothenberg, J. (2000). ***An experiment in using emulation to preserve digital publications***. Hague: Koninklijike Bibliotheek.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی