تعامل انسان و اطلاعات، جلد۳ شماره۱
http://hii.khu.ac.ir
مقاله اصیل پژوهشی

بهره‌گیری از فناوری مدیریت حقوق دیجیتالی در سامانه مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوری اطلاعات ایران

پریچهر آقاسیدجوادی: دانشجوی کارشناسی ارشد علم اطلاعات و دانش‌شناسی، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات تهران، p.seyedjavadi@gmail.com
مهدی علیپورحافظی: دکتری علم اطلاعات و دانش شناسی، استادیار، گروه علم اطلاعات و دانش شناسی، دانشکده روانشناسی و علوم تربیتی، دانشگاه علامه طباطبائی

چکیده

دریافت: ۹۵/ ۰۱/۲۸
ویرایش: ۹۵/ ۰۳/۲۲
پذیرش: ۹۵/ ۰۴/۰۵

زمینه و هدف: تسهیل در امکان نقض حقوق مالکیت فکری و استفاده‌های غیر مجاز از منابع دیجیتالی، یکی از مهمترین پیامدهای توسعه فناوری‌های اطلاعاتی و ارتباطی نظیر اینترنت است. هدف این پژوهش، شناسایی وضعیت بهره‌گیری از فناوری مدیریت حقوق دیجیتالی در سامانهٔ مدیریت پایاننامه‌های پژوهشگاه علوم و فناوری اطلاعات ایران می باشد.

روش پژوهش: پژوهش حاضر، از نوع کاربردی است و به روش مطالعه موردی، به بررسی سامانهٔ مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوری اطلاعات ایران پرداخته است. ابزار مورد استفاده در این پژوهش سیاهه وارسی است که توسط NSA INFOSEC IAM تهیه شده است.

یافته‌ها: یافته‌های پژوهش در سه بخش به‌دست آمده‌اند. بخش اول، اطلاعات مورد نیاز برآورد و ارزیابی امنیت سامانه مدیریت پایان‌نامه‌ها است، که به روش مشاهده و مصاحبهٔ ساختار یافته نقاط قوت و ضعف درونی سازمان مشخص شده است. در بخش دوم جدول ماتریس OICM، رده‌های اطلاعاتی در گردش کاری سازمان و اهمیت هر یک در مأموریت سازمان مشخص شد. در بخش سوم نیز تهدیدهایی که سازمان با آن مواجه است و میزان تأثیرشان بر مأموریت سازمان مشخص گردید.

نتیجه‌گیری: نتایج حاصل از پژوهش نشان می‌دهد، پژوهشگاه علوم و فناوری اطلاعات ایران به لحاظ زیرساخت‌های امنیتی از وضعیت مطلوبی برخودار نیست و با تهدیدهایی نظیر دسترسی غیرمجاز، اشکال مدیریتی، عدم امکان پیگرد و ... مواجه است. لذا با توجه به رسالت سازمان در حفظ و نگهداری و اشاعهٔ اطلاعات، نیازمند بهره‌گیری از فناوری‌هایی نظیر مدیریت حقوق دیجیتال است.

کلیدواژه‌ها: مدیریت حقوق دیجیتال، حقوق مالکیت فکری، فناوری‌های اطلاعاتی و ارتباطی، فناوری امنیتی، منبع دیجیتالی، استفاده غیرمجاز

مقدمه

امروزه حجم فراوانی از اطلاعات در شبکه‌های اطلاع‌رسانی و اینترنت منتشر و با سرعت و سهولت در دسترس جوامع در سراسر دنیا قرار می‌گیرند، کم توجهی به کیفیت محتوا در انتشار آثار سبب به خطر افتادن حق صاحبان آثار در اثر استفاده غیرمجاز از آن‌ها شده‌است (مطلبی، ۱۳۸۷). به‌دلیل اهمیت حقوق مالکیت فکری، تلاش‌های بسیاری برای حفاظت از آثار در محیط دیجیتال صورت گرفته است، از جمله این فعالیت‌ها می‌توان به توافقنامه‌های جهانی نظیر: معاهدهٔ برن، معاهدهٔ حقوق مالکیت ادبی و هنری سازمان جهانی مالکیت فکری (وایپو)[1] و قانون حق اثر در هزارهٔ دیجیتال[2] اشاره کرد. حق مؤلف، نوعی حفاظت قانونی از حقوق مادی و معنوی مالکان آثار را به‌صورت چاپی و غیرچاپی فراهم می‌آورد. قانون حق مؤلف پدیدآورندگان را قادر می‌سازد، از راه‌های مختلف بر استفاده از آثارشان نظارت داشته باشند. به‌عنوان نمونه اجازهٔ نسخه‌برداری، استفاده به صورت پیوسته و غیره، اما هدف اصلی از قانون حقوق مالکیت فکری فراهم‌ساختن راهی در به‌دست آوردن پاداش مادی برای تلاش‌های خالقین آثار و تشویقی برای ایجاد آثار جدید است (کلندر و برسترم[3]، ۲۰۰۳).

به‌طورکلی حفاظت از حق مؤلف در محیط دیجیتال (خصوصاً اینترنت و فضای پیوسته وب) به چهار طریق امکان‌پذیر است: فناوری‌های نوین، قانون حق مؤلف، قراردادها و مجوزها و قوانین جدیدی که برای حفاظت از پایگاه‌های اطلاعاتی وضع شده است. همانگونه که بسیاری از متخصصان و صاحب نظران این حوزه اشاره کرده‌اند، بهترین راه‌حل، استفادهٔ ترکیبی از راه‌حل‌های قانونی و فناورانه

[1] WIPO
[2] Digital Millennium Copyright Act (DMCA)
[3] Callander and Burstrom

می‌باشد (تاج‌آبادی و رنجبری، ۱۳۸۹). از جمله فناوری‌های نوین ابداع شده برای حفاظت از حق مؤلف در محیط دیجیتال، مدیریت حقوق دیجیتالی[۴] است. مدیریت حقوق دیجیتالی دربرگیرنده توصیف، شناسایی، مدیریت مالی، حفاظت، کنترل و ردیابی تمامی آثار دارای حق مؤلف به صورت اشکال عینی (ملموس) و غیرعینی (ناملموس) و مدیریت روابط حقوقی آن‌ها است (پاتریکیو و دیگران[۵]، ۲۰۱۱).

این فناوری راه‌حل‌هایی قابل اطمینان در مقابل دسترسی‌های غیرمجاز ارائه می‌نماید. همچنین اجازه می‌دهد تا مالکان منابع دیجیتالی بتوانند دسترسی قانونی به آثار خود را مدیریت نمایند همچنین به افراد مجاز، اجازهٔ دسترسی به محتوای دیجیتالی را می‌دهد و استفاده‌کنندهٔ مجاز، کسانی هستند که مجوز استفاده از منابع دیجیتال را فراهم نموده‌اند و می‌توانند مطابق با میزان دسترسی تعیین شده در مجوز، به منابع مورد نیازشان دسترسی داشته باشند (گابر[۶]، ۲۰۱۲). به‌طورکلی رویکردهای متفاوتی برای حفاظت از یک منبع دیجیتالی، در مقابل استفاده‌های غیرمجاز وجود دارد اما می‌توان آن‌ها را در چهار گروه اصلی دسته‌بندی نمود.

- حفاظت از محتوای دیجیتالی، مانند فناوری واترمارکینگ[۷]، انگشت‌نگاری[۸] و ...
- حفاظت در دسترسی به محتوای دیجیتالی، مانند حفاظت دسترسی با احراز هویت[۹] و تعیین ورود و خروج اولیه و ...
- محدود یا متوقف نمودن نسخه‌برداری از محتوای دیجیتالی
- حفاظت در مقابل انتقال یک محتوای دیجیتالی از سیستمی به سیستم دیگر (تسل، ۲۰۰۶).

به‌طورکلی در پژوهش‌های مورد مطالعه که به حفاظت از مالکیت فکری پرداخته‌اند، دو مبحث عمده دیده می‌شود که مکمل هم بوده و در کنار یکدیگر می‌توانند به‌نحوی مؤثر به حمایت از حقوق مالکیت فکری در محیط دیجیتال بپردازند. این مباحث عبارتند از: ۱) مبحث قانونی؛ ۲) مبحث فناوری‌های امنیت اطلاعات نوین.

مطالعه در پژوهش‌های انجام شده نشان می‌دهد، در ایران مطالعاتی از بُعد حقوقی انجام گرفته است. مثلاً در تحقیقاتی که توسط کاراندیش (۱۳۸۵)، طباطبایی (۱۳۸۹)، فلاحتی مروست (۱۳۸۹)، دیهیمی (۱۳۹۱)، عنصری‌نژاد (۱۳۹۲)، انجام گرفته است، همگی به این نتیجه رسیده‌اند که قوانین ایران در مقایسه با قوانین بین‌المللی حقوق مالکیت فکری، دارای نواقص و خلاءهای فراوان در تجارت الکترونیک، نظام حقوقی توزیع در محیط مجازی، مسئولیت مدنی، حق مؤلف و نظایر آن است بنابراین لزوم بازنگری و اصلاح آن مشهود است. همچنین به‌نظر می‌رسد، رشد سریع فناوری‌های اطلاعاتی و ارتباطی، نظیر اینترنت و رشد صنعت نشر رومیزی و ... در مقابل، روزآمدی کُند قوانین نسبت به آن، عامل اصلی چالش در این زمینه بوده است. البته نمی‌توان ویژگی‌های محیط الکترونیک را از نظر دور داشت، که به دلیل قابلیت‌های خاص خود نظیر پیوندهای فرامتن، کادربندی و ... وضع و تصویب قوانین را بسیار مشکل نموده است.

مبحث دوم فناوری‌های حفاظتی نوینی می‌باشند که برای حمایت از حقوق مالکیت فکری در محیط دیجیتالی ابداع و گسترش یافته‌اند. بررسی پژوهش‌ها نشان می‌دهد، در ایران کمتر به این حوزه پرداخته شده است. خصوصاً مبحث فناوری مدیریت حقوق دیجیتالی که از مهمترین فناوری‌ها، برای حمایت از حقوق مالکیت فکری است. اما پژوهش‌های بسیاری در خارج از کشور در این حوزه انجام شده است. پس از ابداع این فناوری، پژوهش‌های انجام شده سعی در رفع نواقص و کاستی‌های آن داشته‌اند و همگام با تحولات فناوری‌های اطلاعاتی و ارتباطی توسعه یافته‌اند. چنانچه در تحقیق لیو، لیو و شائو[۱۰] (۲۰۱۴) آمده است، سیستم‌های مدیریت حقوق دیجیتالی برای ایجاد سلامت در صنعت محتوای دیجیتالی توسعه یافته‌اند. از اواسط سال ۱۹۹۰، تحقیقات و برنامه‌های کاربردی سیستم‌های مدیریت حقوق دیجیتال در محیط ناپیوسته[۱۱] و در محیط پیوسته[۱۲] مانند اینترنت، شبکه‌های توزیع محتوا و شبکه‌های نظیر به نظیر[۱۳] آزموده شده‌اند و در سال‌های اخیر، با ظهور فناوری محاسبات ابری چند رسانه‌ای[۱۴] در خدمات شبکه‌های اجتماعی چند رسانه‌ای، مانند «فیس‌بوک»[۱۵]، «توییتر»[۱۶] و نظایر آن‌ها، مورد بررسی هستند. از لحاظ روند توسعهٔ فناوری‌ها می‌توان گفت که سیستم‌های اولیه مدیریت حقوق دیجیتالی بر

4 Digital Rights Management (DRM)
5 Patriciu and et al.
6 Gaber
7 Watermark
8 Fingerprinting
9 Authentication
10 Lio, Lio and Shao
11 Offline
12 Online
13 Peer-to-peer network
14 Multimedia Cloud Computing Technology
15 Facebook
16 Twitter

رمزگذاری استوار بوده‌اند، اما رمزگذاری تا مرحله واگذاری منبع در اختیار استفاده‌کننده کاربرد دارد و بعد از آن، کاربر می‌تواند هرطور که بخواهد از منبع مورد نظر استفاده نماید و حتی آن را به‌راحتی توزیع نموده و استفادهٔ تجاری نماید. اما در پژوهش ولف، استینبچ و داینر[17] (۲۰۰۶) با واترمارک دیجیتالی سعی در رفع این نقیصه نموده‌اند و امکان نشانه‌گذاری، جستجو و بازیابی را برای حمایت از حق مؤلف پس از واگذاری منبع به کاربر فراهم آورده‌اند. در ایران نیز پژوهش‌هایی در این زمینه صورت گرفته است. مثلاً ریاضی احمدسرایی (۱۳۸۸) و نمازی (۱۳۹۰) در پایان‌نامهٔ خود به بررسی واترمارکینگ و روش‌های ارتقای آن در جهت حفاظت از منابع دیجیتالی پرداخته‌اند.

همچنین تحقیقات اولیه بیشتر معطوف بر حمایت از حقوق مالکان آثار بوده است و به حقوق کاربران و حقوق مرتبط (حقوق تولیدکنندگان و توزیع‌کنندگان منابع دیجیتالی) توجهی نداشته‌اند. سیر پژوهش‌ها، نشان دهندهٔ توجه بیشتر به انعطاف‌پذیری و قابلیت تعامل بیشتر و افزایش پژوهش‌ها در زمینه مدل‌های کسب و کار و ... برای دسترسی به منابع است. در حقیقت هرچه از لحاظ تاریخی به جلو حرکت کنیم این مسئله مشهودتر می‌شود و پژوهش‌ها به سمت رفع خلاءهای موجود، در ارتباط با حقوق کاربران و حقوق مرتبط است. چنانچه زهانگ و دیگران[18] (۲۰۰۹) در پژوهش خود به چهار جزء اصلی در زنجیرهٔ ارزشی پرداخته و به این نتیجه رسیده‌اند یک تعامل موفقیت‌آمیز محتوای دیجیتالی به روابط مطمئن و تعادل مناسب در میان شرکای گوناگون در زنجیرهٔ ارزشی بستگی دارد. همچنین، گابر (۲۰۱۲) در پژوهش خود به حمایت از حقوق مصرف‌کننده در توزیع مجدد مجوزهای دیجیتالی پرداخته است. وی بیان می‌کند، سیستم‌های مدیریت حقوق دیجیتال موجود اصولاً بر حفاظت از حقوق مالکان تمرکز دارند و به حقوق استفاده‌کنندگان توجه نداشته‌اند. این سیستم‌ها به کاربران اجازهٔ فروش مجدد مجوز خریداری شده را نمی‌دهند اما گاهی اوقات استفاده‌کننده حق فروش مجدد را تحت نظریه فروش اولیه[19] دارد. با توجه به پژوهش‌های اشاره شده در این بخش، این پژوهش که دربارهٔ بهره‌برداری از سیستم مدیریت حقوق دیجیتال است، برای اولین‌بار در ایران به این مبحث پرداخته است. در این راستا راه‌حل‌های موجود، مورد مطالعه قرار گرفته تا مناسب‌ترین آن‌ها برای حفاظت از حق مؤلف در سامانهٔ مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوری اطلاعات مورد استفاده قرار گیرد.

پژوهشگاه علوم و فناوری اطلاعات ایران چند سالی است که اقدام به گردآوری و تولید سامانهٔ مدیریت پایان‌نامه‌های تحصیلات تکمیلی در کشور نموده است و در حال حاضر به عنوان مرکز اصلی گردآوری پایان‌نامه‌های سراسر کشور، امکان دسترسی به اطلاعات پایان‌نامه‌ها را به‌صورت تمام متن برای دانشگاه‌ها فراهم‌آورده است. لذا برای حفاظت از استفاده غیر مجاز از پایان‌نامه‌ها و جلوگیری از استفاده‌های نامناسب و توزیع غیرقانونی آن‌ها، نیازمند استفاده از فناوری هایی نظیر مدیریت حقوق دیجیتالی می‌باشد. اما از ملزومات بهره‌برداری از این فناوری بررسی امکانات و شرایط موجود و مورد نیاز به لحاظ امنیتی، برای پیاده‌سازی فناوری مورد نظر می‌باشد. لذا این پژوهش در نظر دارد با بررسی شرایط موجود و مورد نیاز به شناسایی وضعیت بهره‌برداری از فناوری مدیریت حقوق دیجیتالی در سامانهٔ مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوی اطلاعات ایران بپردازد. در این راستا پرسش‌هایی به شرح زیر مطرح شدند و پژوهش حاضر در پی پاسخ‌گویی به این پرسش‌ها به اجرا درآمد:

۱. در سامانهٔ مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوری اطلاعات ایران چه امکانات و تجهیزاتی به لحاظ زیرساخت‌های امنیتی مورد نیاز برای مدیریت حقوق دیجیتالی موجود است؟

۲. چه عواملی بر مدیریت حقوق دیجیتالی در سامانهٔ مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوری اطلاعات ایران تأثیرگذار هستند؟

۳. چه تهدیدهایی با چه ضریب تأثیری بر مدیریت حقوق دیجیتالی در سامانهٔ مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوری اطلاعات ایران وجود دارند؟

برای بهبود وضعیت موجود از نظر مدیریت حقوق دیجیتالی، پژوهشگاه علوم و فناوری اطلاعات ایران چه اقداماتی می‌تواند در سامانهٔ مدیریت پایان‌نامه‌ها ایجاد نمایند؟

روش

پژوهش حاضر از نظر هدف کاربردی است. برای رسیدن به اهداف پژوهش، با استفاده از رویکرد ترکیبی به بررسی و تحلیل سامانهٔ مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوری اطلاعات ایران پرداخته شده است و تمامی شرایط و امکانات موجود از طریق تحلیل استقرایی داده‌های گردآوری شده، شناسایی شده‌اند. از آنجاکه در این پژوهش یک واحد مشخص از ابعاد گوناگون مورد مطالعه و بررسی دقیق قرار

17 Wolf, Steinebach & Diener
18 Zhang & et al.
19 First sale doctrine

گرفته است، روش مورد استفاده، مطالعه موردی می‌باشد. بنابراین پژوهش حاضر از نوع میدانی بوده و به شیوهٔ ارزیابانه انجام گرفته است.

- پژوهشگاه علوم و فناوری اطلاعات ایران به‌عنوان یگانه مرکز نگهداری پایان‌نامه‌های دانشگاه‌های کل کشور، رسالت بزرگی در نگهداری و اشاعه بهینه اطلاعات پایان‌نامه‌ها برای تمامی پژوهشگران، در سراسر کشور بر عهده دارد. لذا امنیت محتوا و توزیع امن اطلاعات و رعایت حق مؤلف در آن، بسیار حائز اهمیت است. به همین دلیل این مرکز به‌عنوان جامعهٔ آماری، برای مطالعه سیستم مدیریت حقوق دیجیتالی انتخاب شده است. محدودهٔ پژوهش نیز در ارتباط با امنیت محتوای نگهداری شده و توزیع امن اطلاعات پایان‌نامه‌ها و فناوری‌های مورد استفاده در این راستا، با هدف حمایت از حقوق مالکیت فکری است.
- در این پژوهش هدف اصلی، شناسایی وضعیت بهره‌برداری از مدیریت حقوق دیجیتالی در سامانهٔ مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوری اطلاعات ایران است. لذا تمامی ابعاد و امکانات موجود و مورد نیاز در سامانهٔ مدیریت پایان نامه‌های پژوهشگاه علوم و فناوری اطلاعات ایران، با استفاده از سیاههٔ وارسی که توسط NSA INFOSEC IAM، تهیه شده است، شناسایی و مورد بررسی قرار گرفته است. در زمینه شناسایی سیاهه وارسی مذکور لازم به ذکر است که مطالعه در این زمینه نشان داد که غیر از سیاهه مذکور سیاهه یا ابزار مناسب دیگری در راستای اهداف این پژوهش شناسایی نشد. سیاهه وارسی مورد استفاده در این پژوهش، الگویی است که توسط NSA INFOSEC IAM، تهیه شده است و برای سنجش میزان امنیت شبکه و فناوری‌های امنیتی حفاظت از اطلاعات، مورد استفاده قرار می‌گیرد. برحسب نیاز پژوهش حاضر، تغییراتی در این الگو ایجاد شد، سپس با توجه به ارتباط موضوع مورد بررسی در پژوهش حاضر، به دو حوزهٔ علوم کامپیوتر و علم اطلاعات و دانش‌شناسی، صحت آن توسط ۳ نفر از متخصصان رشته کامپیوتر و علم اطلاعات و دانش‌شناسی مورد بررسی قرار گرفت و روایی آن تأیید شد. همچنین برای مطالعه وضعیت سامانهٔ مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوری اطلاعات و گردآوری داده‌ها از ابزار مشاهده و مصاحبه استفاده شده است.

سیاهه وارسی مورد استفاده از سه قسمت مجزا تشکیل شده است:

بخش اول: جدول اطلاعات مورد نیاز برآورد و ارزیابی امنیت سیستم‌های اطلاعاتی؛ شامل سئوالاتی است که با استفاده از ابزار مشاهده و مصاحبه ساختار یافته با سه نفر از مسئولین مدیریت فناوری اطلاعات، میزان امنیت موجود در سازمان مورد مطالعه مشخص شد (نقاط قوت و ضعف درونی سازمان).

بخش دوم: جدول اُ.آی.سی.ام.[20] با شناسه‌های تأثیر[21] است. در این جدول رده‌های اطلاعاتی موجود در سازمان بر حسب شناسه‌های تأثیر مورد بررسی و ارزیابی قرار گرفتند. این شناسه‌ها با کمیت‌های عددی صفر الی پنج مقداردهی شدند. عدد پنج نشانگر حداکثر اهمیت و عدد صفر نشانگر کمترین اهمیت است. لازم به ذکر است که امتیازدهی صورت گرفته بر اساس دستورالعمل ماتریس اُ.آی.سی.ام. انجام گرفت.

بخش سوم: شامل جدولی از فهرست تهدیدات به همراه ضریب تأثیر آن‌ها است. این بخش از آن جهت حائز اهمیت است که با شناخت تهدیدات و ضریب تأثیر آن در مأموریت سازمان، می‌توان دربارهٔ سیستم‌های امنیتی مورد نیاز سازمان تصمیم درستی اتخاذ نمود. ضریب تأثیر در این بخش برحسب اهمیت هر تهدید در مأموریت سازمان، در سه سطح بالا، متوسط و پایین تعیین شد. همچنین نواقص در امنیت و علت آن به تفکیک بیان شد که می‌تواند در چگونگی تصمیم‌گیری برای رفع آن‌ها سودمند باشد.

در پژوهش حاضر، گردآوری داده‌ها و مستندات در سه مرحله انجام گرفت و در هر مرحله توصیفی از آن‌ها ارائه شده است سپس هر مرحله با توجه به مستندات و داده‌های گردآوری شده مورد تجزیه و تحلیل قرار گرفت. سپس نتایج حاصل از تحلیل مراحل پژوهش، مورد بررسی و ارزیابی قرار گرفته و نتیجه نهایی ارائه شده است.

یافته‌ها

با توجه به محوریت چهار پرسش اساسی در این پژوهش، در اینجا یافته‌های پژوهش در سه بخش مستقل ارائه شده است. پاسخ به پرسش چهارم منوط به پاسخگویی به سه پرسش نخست است. لذا پاسخ به پرسش چهارم در بخش بعدی مقاله حاضر ارائه شده است. بنابراین ابتدا پرسش اساسی پژوهش بیان شده است و در ادامه یافته‌های مرتبط با آن پرسش ارائه شده است.

20 OICM= Organizational Information Criticality Matrix
21 Impact Attributes

در سامانهٔ مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوری اطلاعات ایران چه امکانات و تجهیزاتی به لحاظ زیرساخت امنیتی موجود است؟

پاسخ به این پرسش، از سئوالات باز قسمت اول سیاهه وارسی با عنوان: اطلاعات مورد نیاز گروه برآورد و ارزیابی امنیت سیستم‌های اطلاعاتی به‌دست آمده است.

- به لحاظ جغرافیایی، پژوهشگاه علوم و فناوری اطلاعات ایران با تمامی دانشگاه‌های دولتی و غیردولتی ایران در ارتباط بوده و در حفظ و نگهداری پایان‌نامه‌های دانشگاه‌ها و ارائه خدمات بر اساس آن‌ها، با دانشگاه‌ها همکاری دارد.
- از سیستم عامل Linux و زبان برنامه‌نویسی PHP استفاده می‌شود و پایگاه داده‌های آن My SQL است.
- در معماری شبکهٔ پژوهشگاه علوم و فناوری اطلاعات ایران از دیواره آتش استفاده می‌شود و دیواره آتش مورد استفاده، سیستم تشخیص نفوذ IDS را در همهٔ سطوح پوشش می‌دهد.
- برای احراز هویت از RAS Server استفاده نمی‌شود، همچنین فاقد لایهٔ سوکت امن[22] در ارتباطات شبکه‌ای است. اما از فناوری VPN بهره می‌برد.
- تمامی کارکنان سازمان به اینترنت متصل هستند و آموزشی در ارتباط با نحوهٔ نگهداری اطلاعات و اهمیت امنیت منابع اطلاعاتی سازمان نداشته‌اند.
- برای زمان بحران، هنگامی‌که حمله موفقی به منابع اطلاعاتی سازمان صورت می‌گیرد، تدابیر امنیتی خاصی اندیشیده نشده است. تنها فایل پشتیبان به‌صورت نرم‌افزاری و در فاصله زمانی نامنظم تهیه می‌شود.
- سازمان ثالثی مانند بانک و ... به منابع اطلاعاتی سازمان دسترسی ندارد. مجوزهای صادر شده برای کاربران بر حسب محدودهٔ IP معرفی شده است.
- برای شناسایی موجودیت‌ها در محتواهای دیجیتالی سازمان، از شناسه‌های منحصر به‌فرد استفاده شده است اما ابزارهای استانداردی در تعریف آن‌ها به‌کار نرفته است.
- نیروی متخصصی برای استفاده از زبان بیان حقوقی در سازمان وجود ندارد اما به لحاظ فنی برنامهٔ کاربردی طراحی شده تمام زبان‌های برنامه‌نویسی را پوشش می‌دهد.
- از واترمارکینگ و انگشت‌نگاری دیجیتالی در محتواهای اطلاعاتی پژوهشگاه علوم و فناوری اطلاعات ایران استفاده نمی‌شود.

رمزنگاری، امضای دیجیتالی، زیرساخت کلید عمومی در سطح مقدماتی انجام می‌گیرد. کلیدهای عمومی و خصوصی در سازمان و توسط برنامه‌نویس سازمان تعریف شده‌اند.

احراز هویت، با استفاده از محدودهٔ IP معرفی شده انجام می‌گیرد. سطوح دسترسی خاصی برای کاربران تعریف نشده است، اما امکان آن به لحاظ فنی وجود دارد.

بهره‌برداری از برنامهٔ حفاظت نسخه‌برداری و تراکنش‌های مالی نیز در نظر گرفته نشده است.

چه عواملی بر مدیریت حقوق دیجیتالی در سامانهٔ مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوری اطلاعات ایران تأثیرگذار هستند؟

پاسخ این پرسش از قسمت دوم سیاهه وارسی که جدول ماتریس او.آی.سی.ام. نام دارد حاصل شده است. جدول ماتریس ابزاری کارآمد برای ارزیابی و برآورد اهمیت منابع اطلاعاتی موجود در گردش کاری سازمان برحسب شناسه‌های تأثیر است. هدف از ارائه جدول ماتریس (جدول ۱) در این پژوهش، تفکیک رده‌های اطلاعاتی سازمان بر اساس تأثیرگذاری آن‌ها بر مأموریت پژوهشگاه علوم و فناوری اطلاعات ایران است. داده‌های کمی این جدول با مشورت مدیران مربوطه و در راستای اهداف و مأموریت سازمان تعیین شده است.

- منابع اطلاعاتی نظیر اطلاعات پایان‌نامه‌ها، شبکه و سرویس‌دهنده‌ها، حساب‌های کاربری (مجوزها) و اطلاعات مالی و حسابداری برحسب مجموع شناسه‌های تأثیر، بیشترین امتیاز را در این جدول کسب نموده‌اند.
- اطلاعات منابع انسانی سازمان و اطلاعات پژوهشگران، به ترتیب با کسب ۳۲ و ۳۱ امتیاز در رده‌های پایین‌تری به لحاظ مجموع شناسه‌های تأثیر قرار دارند. اطلاعات نحوهٔ نگهداری از نرم‌افزارها و سخت‌افزارها با کسب ۳۰ امتیاز و اطلاعات مشتریان سازمان با کسب ۲۵ امتیاز در رتبه‌های بعدی قرار گرفته‌اند.
- اطلاعات ارتباط با سازمان‌های خارجی نیز با کسب ۱۵ امتیاز، حائز پایین‌ترین امتیاز در جدول شناخته شده است.
- در کمیت منظور شده برای هریک از شناسه‌های تأثیر در رده‌های اطلاعاتی سازمان تفاوت وجود دارد.
- در شناسهٔ محرمانگی، اطلاعات مشتریان سازمان و ارتباط با سازمان‌های خارجی، کمترین امتیاز را کسب کرده‌اند

22 SSL

جدول ۱. ماتریس OICM با شناسه‌های تأثیر.

	شناسه کنترل دسترسی	شناسه ممیزی	شناسه جواز	انکار ناپذیری	قابلیت حسابرسی	دسترس پذیری	صحت اطلاعات	محرمانگی
اطلاعات پایان‌نامه‌ها (متن کامل)	۵	۵	۵	۵	۵	۵	۵	۵
اطلاعات مشتریان سازمان (دانشگاه، دانشکده، گروه و ...)	۱	۳	۳	۵	۵	۳	۵	۰
اطلاعات منابع انسانی سازمان	۵	۵	۵	۴	۴	۲	۴	۳
اطلاعات پژوهشگران (نویسنده، استاد راهنما، مشاور و ...)	۴	۳	۴	۴	۴	۵	۴	۳
اطلاعات شبکه و سرویس‌دهنده‌ها	۵	۵	۵	۵	۵	۵	۵	۵
اطلاعات حساب‌های کاربری (مجوزها)	۵	۵	۵	۵	۵	۵	۵	۵
اطلاعات ارتباط با سازمان‌های خارجی	۱	۱	۱	۴	۱	۱	۵	۱
اطلاعات نحوهٔ نگهداری از نرم‌افزارها وسخت‌افزارها	۰	۳	۵	۵	۴	۳	۵	۵
اطلاعات مالی و حسابداری	۵	۵	۵	۵	۵	۵	۵	۵

و اطلاعات مشتریان سازمان و پژوهشگران سطح متوسط و مابقی امتیاز بالایی گرفته‌اند.

- در شناسهٔ صحت اطلاعات، به تمامی رده‌های اطلاعاتی حداکثر امتیاز تعلق گرفته است. اطلاعات منابع انسانی سازمان و پژوهشگران با کسب ۴ امتیاز در مرتبه پایین‌تر قرار دارند.
- در شناسهٔ دسترس‌پذیری، اطلاعات پایان‌نامه‌ها، شبکه و سرویس‌دهنده‌ها، حساب‌های کاربری (مجوزها) و مالی و حسابداری بیشترین امتیاز را کسب کرده‌اند و سایر رده‌های اطلاعاتی در مرتبهٔ پایین‌تر قرار گرفته‌اند.
- در شناسهٔ قابلیت حسابرسی، برای تمامی رده‌های اطلاعاتی حداکثر امتیاز در نظر گرفته شده است. تنها برای اطلاعات ارتباط با سازمان‌های خارجی، حداقل امتیاز در نظر گرفته شده است.
- در گزینهٔ انکارناپذیری، برای تمامی رده‌های اطلاعاتی امتیاز بالایی در نظر گرفته شده است. به‌جز اطلاعات ارتباط با سازمان‌های خارجی، منابع انسانی سازمان و پژهشگران که امتیاز محسوب شده کمی کمتر است.
- در شناسهٔ جواز نیز، برای اکثر رده‌های اطلاعاتی حداکثر امتیاز در نظر گرفته شده است. در اطلاعات مشتریان سازمان امتیاز متوسط و ارتباط با سازمان‌های خارجی، حداقل امتیاز در نظر گرفته شده است.
- در شناسهٔ ممیزی، برای اطلاعات مشتریان سازمان و نحوهٔ نگهداری از نرم‌افزارها و سخت‌افزارها امتیاز متوسطی در نظر گرفته شده است. اطلاعات ارتباط با سازمان‌های خارجی، حداقل امتیاز را کسب نموده است. بقیهٔ موارد حداکثر امتیاز را کسب کرده‌اند.
- در شناسهٔ کنترل دسترسی، اطلاعات مشتریان سازمان، ارتباط با سازمان‌های خارجی و نحوهٔ نگهداری از نرم‌افزارها و سخت‌افزارها، حداقل امتیاز لحاظ شده است.سایر موارد حداکثر امتیاز را کسب کرده‌اند.

چه تهدیدهایی با چه ضریب تأثیری بر مدیریت حقوق دیجیتالی در سامانهٔ مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوری اطلاعات ایران وجود دارند؟

در این بخش از پژوهش، سیاهه‌ای از تهدیدها (جدول ۲) ارائه شده است. در واقع، برای بررسی لزوم استفاده از فناوری‌های مدیریت حقوق دیجیتالی و امنیت مورد نیاز در رده‌های اطلاعاتی پژوهشگاه علوم و فناوری اطلاعات ایرن، نیازمند تهیه فهرستی از تهدیدها است که لزوم تهیه فناوری‌ها و سایر تدابیر امنیتی را با سطوح ضریب تأثیر در مأموریت سازمان، مشخص سازد. همچنین عواقب ناشی از نقص یا عدم وجود هر یک نیز با توجه به مستندات و شواهد موجود تشریح شده است.

- در این جدول بیشترین نوع تهدیدها مربوط به دسترسی غیرمجاز است، که مربوط به عواملی مانند عدم وجود رمزنگاری، نقض در احراز هویت، عدم حفاظت نسخه‌برداری و فقدان مجوزها می‌باشد.

جدول ۲. تهدیدها به همراه ضریب تأثیر آن‌ها.

	نام آسیب‌پذیری	ضریب تاثیر	نوع تهدید	عواقب
۱	عدم وجود رمزنگاری	بالا	دسترسی غیرمجاز	از محتوای دیجیتالی حفاظت نشده و نفوذگر می‌تواند بدون داشتن مجوز به محتوای منابع دسترسی داشته باشد.
۲	نقص در احراز هویت *(Authentication)*	بالا	دسترسی غیرمجاز	عدم شناسایی کاربران، سبب پایین آمدن امنیت در دسترسی به اطلاعات می‌گردد و نفوذگران قادر خواهند بود به‌راحتی به منابع اطلاعاتی دسترسی داشته و از آن استفاده نامطلوب نمایند.
۳	نقص در احراز مجوز *(Authorization)*	بالا	عدم دسترسی مناسب	باعث دسترسی بدون مجوز افراد به اطلاعات می‌گردد و نفوذگر می‌تواند به بالاترین سطح دسترسی (*Admin*) به سرویس‌دهنده دسترسی پیدا کند.
۴	عدم حفاظت نسخه‌برداری	بالا	دسترسی غیرمجاز	کاربر می‌تواند از محتوای دیجیتالی نسخ متعدد به‌صورت غیرمجاز تهیه نماید.
۵	عدم تعبیه واترمارک و انگشت‌نگاری	بالا	عدم امکان پیگرد	در صورت نسخه‌برداری غیرمجاز، تغییر یا تحریف و ... قابل ردیابی نمی‌باشد.
۶	عدم استفاده از امضای دیجیتالی	بالا	پایین آمدن انکار ناپذیری و صحت اطلاعات	باعث اطمینان کمتر به درستی اطلاعات دریافتی همچنین ارسال کننده اطلاعات می‌گردد.
۷	فقدان مجوزها *(License)*	بالا	دسترسی غیرمجاز	نفوذگر قادر خواهد بود از محتوا استفاده غیرمجاز نماید.
۸	عدم استفاده از شناساگرها و توصیف‌کننده‌های استاندارد محتوا	بالا	اشکال مدیریتی	سبب پایین آمدن امکان جستجوی و بازیابی دقیق و قابلیت تعامل‌پذیری با سایر فناوری‌های موجود در شبکه می‌گردد.
۹	عدم بهره‌برداری از پروتکل لایه سوکت امن *(SSL)*	بالا	پایین آمدن امنیت	سطح اطمینان در محیط شبکه یا وب پایین می‌آید.
۱۰	نقص در آنتی‌ویروس	بالا	ویروس	وجود نقص یا عدم وجود آنتی‌ویروس بر روی ماشین‌ها باعث خواهد شد که ویروس‌ها به سادگی بتوانند ماشین را آلوده کرده و آن را از کار انداخته یا داده‌ها را تغییر بدهند.
۱۱	آموزش ناکافی پرسنل	بالا	اشکال مدیریتی	آموزش ناکافی عامل بسیاری از اختلالات سهوی و از دست رفتن کنترل سیستم‌های کاربری و سرویس‌دهنده‌های شبکه است و جزو خطرات جدی به شمار می‌رود.
۱۲	عدم ثبت فایل سوابق (*Log*)	متوسط	عدم امکان پیگرد	هرگاه هر سرویس‌دهنده سیاستی دقیق و اصولی برای ذخیره‌سازی تمام تعاملات کاربران اتخاذ نکرده باشد آنگاه این امکان برای نفوذگر وجود دارد که از مصونیت در عدم پیگرد برخودار باشد. بدین ترتیب احتمال حمله علیه منابع اطلاعاتی به مراتب افزایش می‌یابد.
۱۳	عدم انقضای به موقع حساب کاربری	متوسط	دسترسی غیرمجاز	عدم انقضای کلمات عبور و دایمی بودن حساب‌های کاربری بر خلاف سیاست‌های رایج امنیتی است زیرا از دست رفتن کلمه عبور مسئولین شبکه و سرویس‌دهنده‌ها می‌تواند ضربات شدیدی به امنیت سازمان بزند.
۱۴	نقص در سیاست‌های صیانت از داده‌ها	متوسط	تغییر در داده‌ها	هرگاه برای حفظ اصالت و سلامت داده‌ها (*Integrity*) سیاست‌های درستی اتخاذ نشده باشد احتمال آنکه کسی بتواند در منابع اطلاعاتی تغییری ایجاد کند، وجود دارد.
۱۵	عدم وجود سیاست درست ومستند در خصوص هشدارهای امنیتی	پایین	اشکال مدیریتی	کاربران حتی در صورت آگاهی از خطرات امنیتی، انگیزه کافی در خصوص رعایت سیاست‌های امنیتی نخواهند داشت و هرکس سیاستهای امنیتی را به‌طور سلیقه‌ای دنبال خواهد کرد. صدور هشدار و وضع قوانین داخلی در خصوص رعایت نکات مرتبط با امنیت اطلاعات این مشکل را رفع خواهد کرد.
۱۶	عدم وجود سیاست خروج از بحران	متوسط	اشکال مدیریتی	هرگاه به شبکه حمله‌ای انجام شود و راه درستی برای بازگرداندن شبکه و منابع اطلاعاتی به وضع قبلی پیش‌بینی نشده باشد، طبعاً زمان قابل توجهی از دست خواهد رفت.

برای آسیب‌پذیری عدم وجود سیاست درست و مستند در خصوص هشدارهای امنیتی، ضریب تأثیر در نظر گرفته شده پایین می‌باشد و نوع تهدید اشکال مدیریتی است.

• آسیب‌پذیری‌های ایجاد شده بر اثر تهدید اشکال مدیریتی، عبارتند از عدم استفاده از شناساگرها و توصیف‌کننده‌های محتوا استاندارد، آموزش ناکافی پرسنل، عدم وجود سیاست درست و مستند در خصوص هشدارهای امنیتی و سیاست خروج از بحران.

• برای آسیب‌پذیری‌هایی مانند آموزش ناکافی پرسنل، ثبت فایل سوابق، عدم انقضای به موقع حساب کاربری، نقض در سیاست‌های صیانت از داده‌ها و عدم وجود سیاست خروج از بحران، ضریب تأثیر در حد متوسط در نظر گرفته شده است.

• در میان ۱۶ آسیب‌پذیری مطرح شده، برای ۱۰ مورد آن ضریب تأثیر بالایی در نظر گرفته شده است. یک مورد ضریب تأثیر پایین و بقیهٔ موارد در حد متوسط هستند.

بحث و نتیجه‌گیری

امروزه برای تبادل و نشر کالاهای اطلاعاتی، نیازمند استفاده از شبکه‌های اطلاعاتی و ارتباطی هستیم. پژوهشگاه علوم و فناوری اطلاعات ایران نیز از این امر مستثنی نمی‌باشد. همانطورکه یافته‌های حاصل از پژوهش نشان می‌دهد، از اهداف پژوهشگاه علوم و فناوری اطلاعات ایران، فراهم نمودن امکان دسترسی به منابع اطلاعاتی، از طریق شبکهٔ اینترنت برای دانشگاه‌ها و سایر مراکز تحقیقاتی ایران است لذا چاره‌ای جز مواجه با خطرات ناشی از این فناوری‌های مدرن را نخواهد داشت. نقض حقوق مالکیت فکری در فضای مجازی از مهمترین چالش‌ها است.

بررسی‌های حاصل از پژوهش حاضر نشان داد، در اهداف پژوهشگاه علوم و فناوری اطلاعات ایران، حمایت از حق مؤلف گنجانده نشده است. به همین سبب سطح امنیت ایجاد شده نسبت به وظایف و مأموریت سازمان پایین می‌باشد. در واقع، اشاعهٔ اطلاعات بدون در نظر داشتن حق مؤلف صدمات جبران ناپذیری را در عرصهٔ اقتصاد و توسعه کشور به‌همراه خواهد داشت. در پژوهشی که کیوکوئیو (۲۰۱۱) انجام داده نیز این مسئله به‌وضوح بیان شده است. هدف وی از این پژوهش نشان دادن وضعیت کشور رمانی به لحاظ گسترش حفاظت از مالکیت فکری، رشد اقتصادی و نوآوری در بافت اقتصاد دیجیتالی بوده است. نتایج حاصل از این پژوهش نشان می‌دهد، حمایت از حقوق مالکیت فکری مشوقی برای نوآوری در کشورهای با درآمد بالا و تبادل فناوری در کشورهای کم درآمد است. با توجه به ماهیت منابع اطلاعاتی پژوهشگاه علوم و فناوری اطلاعات ایران، که حاصل تحقیق و پژوهش افراد بوده است توجه به حقوق آن‌ها امری بدیهی و واجب به‌نظر می‌رسد.

تحلیل حاصل از بررسی و ارزیابی میزان امنیت موجود در شبکه و محتواهای اطلاعاتی پژوهشگاه علوم و فناوری اطلاعات نشان می‌دهد، استفاده از سیستم عامل لینوکس، دیواره آتش، کانال ارتباطی امن VPN و امکان تعریف سطوح دسترسی در برنامه کاربردی این سازمان، امنیتی نسبی را فراهم می‌آورد، اما برای اهداف و مأموریت سازمان کافی نیست. چراکه هریک از فناوری‌های نامبرده می‌توانند امنیت را در محدوده‌ای خاص ایجاد نمایند و دارای نقاط نفوذپذیر هستند. مثلاً: سیستم عامل لینوکس علی‌رغم طراحی در محیط وب و امنیت بالا، دارای نقاط نفوذپذیر است. یکی از نقاط ضعفی که به‌تازگی در آن کشف شده، ضعف نرم‌افزاری است که به آن GHOST می‌گویند. یا VPN کانال ارتباطی امنی را برای دسترسی‌های خارج از سازمان به منابع اطلاعاتی فراهم می‌کند اما کار احراز هویت یا احراز مجوز را انجام نمی‌دهد و دارای نقاط نفوذپذیر نیز می‌باشد. استفاده از دیواره آتش نیز از ملزومات اساسی در معماری شبکه سازمان است و میزان امنیت در شبکه سازمان افزایش می‌دهد اما بارها دیده شده نفوذگران توانسته‌اند به‌راحتی از این فناوری‌ها عبور کرده و صدماتی را به منابع اطلاعاتی سازمان‌ها وارد نمایند.

به این ترتیب، می‌توان نتیجه گرفت اگرچه برخی از تدابیر امنیتی به‌کار گرفته شده در پژوهشگاه علوم و فناوری اطلاعات ایران لازم است اما کافی نیست و امنیت مورد نیاز سازمان را تأمین نمی‌کند. لذا نیازمند استفاده از سایر فناوری امنیتی نظیر مدیریت حقوق دیجیتالی هستیم. چنانچه زنگ، پارکین و مورسل[23]، (۲۰۱۰) نیز در پژوهشی با عنوان «مدیریت حقوق دیجیتال» به نتایج مشابهی رسیده‌اند. آن‌ها به بررسی راه‌حل‌های حفاظت از منابع دیجیتالی در سازمان‌ها پرداخته‌اند و راه‌حل‌های مختلف را به لحاظ حمایت نرم‌افزاری، انگیزه تولید، مدل‌های مدیریتی، قابلیت کنترل کاربران، عملکرد رمزگذاری و احراز هویت برای تعیین سطح دسترسی و دسترسی به داده‌ها به‌صورت ناپیوسته مورد بررسی قرار داده‌اند. نتایج حاصل از این پژوهش نشان داد محصولات مدیریت حقوق دیجیتال بیش از دیگر محصولات، مورد رضایت بوده و نیاز سازمان‌ها را برآورده می‌سازند. همچنین تحقیقات انجام شده در جهت توسعهٔ سیستم‌های مدیریت حقوق دیجیتالی، مانند پژوهش‌های ولف، استینبچ و داینر (۲۰۰۶) و کالندر و برسترم (۲۰۰۳) و دیگران نیز گواه این مطلب می‌باشد. چنانچه براید[24] (۲۰۰۴) در پژوهش خود با عنوان «استفاده از سیستم مدیریت حقوق دیجیتالی در خدمات تحویل مدرک» سعی در استفاده از فناوری‌های حقوق دیجیتال در راستای اهداف کتابخانه بریتانیا (اشاعهٔ اطلاعات با رعایت حقوق مالکیت فکری و حقوق مرتبط) داشته است و با کمک شرکت «الزویر» سیستمی مناسب را پیاده‌سازی نموده است.

از دیگر مواردی که از بررسی یافته‌های این پژوهش به‌دست آمده است، فقدان امکان لازم در پژوهشگاه علوم و فناوری اطلاعات ایران برای تراکنش‌های مالی در محیط مجازی است. لذا کاربران در صورت نیاز به منبع اطلاعاتی مجبور هستند به‌صورت حضوری به بانک مراجعه نموده و شمارهٔ

23 Zeng, Parkin & Moorsel
25 Braid

فیش و مبلغ واریزی را به پژوهشگاه علوم و فناوری اطلاعات ایران اعلام نمایند. بنابراین کاربران برای به‌دست آوردن مطلبی هرچند کم، نیازمند صرف زمان زیادی هستند. این مسئله سبب دلسردی و حتی عدم استفاده از منابع موجود در سازمان خواهد شد. همچنین برای رعایت حقوق مالکیت فکری و فراهم نمودن راه‌حلی امن برای تراکنش‌های مالی در محیط شبکه، ناگزیر از استفادهٔ فناوری‌هایی مانند لایهٔ سوکت امن و نظایر آن، برای تراکنش‌های مالی هستیم تا بتوانیم اعتماد کاربران و مالکان محتوا را جلب نماییم. بنابراین پیاده‌سازی این امکان، از رسالت‌های مهم پژوهشگاه علوم و فناوری اطلاعات ایران می‌باشد. در پژوهشی که زهانگ و دیگران (۲۰۰۹) با عنوان «امنیت و اعتماد در سیستم مدیریت حقوق دیجیتال: یک تحقیق» انجام داده‌اند به این مسئله در سطحی وسیع‌تر پرداخته‌اند. آن‌ها چهار جزء اصلی زنجیرهٔ ارزشی در مدیریت حقوق دیجیتالی را پدیدآور، توزیع‌کننده، کاربر و اعتبار دهنده معرفی کرده‌اند و به این نتیجه رسیده‌اند یک تعامل موفقیت آمیز محتوای دیجیتالی، ابتداً به خط مشی‌های امنیتی، روابط مطمئن و تعادل مناسب در میان شرکای گوناگون در نظام زنجیرهٔ ارزشی مدیریت حقوق دیجیتالی بستگی دارد و بدون آن صنعت محتوا مورد مخاطره قرار خواهد گرفت.

همچنین تحلیل یافته‌های جدول فهرست تهدیدات نشان می‌دهد، بیشترین نوع تهدید برای پژوهشگاه علوم و فناوری اطلاعات، دسترسی غیرمجاز است که بر اثر عدم وجود رمزنگاری، نقص در احراز هویت, عدم حفاظت نسخه‌برداری، فقدان مجوزها و عدم انقضای به‌موقع حساب کاربری حادث می‌شود. در جدول ماتریس نیز رده‌های اطلاعاتی که در شناسهٔ تأثیر محرمانگی حداکثر امتیاز را کسب نموده‌اند شامل اطلاعات پایان‌نامه‌ها (متن کامل)، اطلاعات شبکه و سرویس‌دهنده‌ها، اطلاعات حساب‌های کاربری (مجوزها)، اطلاعات نحوهٔ نگهداری از نرم‌افزارها و سخت‌افزارها و اطلاعات مالی و حسابداری است. حداکثر امتیاز برحسب شناسهٔ تأثیر محرمانگی به این معنا است که افشای ردهٔ اطلاعاتی مورد نظر و دسترسی عوامل غیرمجاز به آن‌ها لطمهٔ شدیدی به مأموریت سازمان وارد خواهد ساخت. بنابراین نتیجه می‌گیریم، پژوهشگاه علوم و فناوری اطلاعات ایران در درجهٔ اول نیازمند فناوری‌هایی است که از دسترسی غیرمجاز ممانعت نمایند. فناوری‌هایی مانند: رمزنگاری، احراز هویت، سیستم حفاظت نسخه‌برداری، مجوزها و انقضای به‌موقع حساب کاربری. باید توجه داشته باشیم تمامی فناوری‌های نامبرده از اجزای سیستم‌های مدیریت حقوق دیجیتال محسوب می‌شوند. در پژوهشی که کیم[25] (۲۰۱۰) با عنوان «سیستم مدیریت حقوق دیجیتالی غیرقابل انعطاف و انعطاف‌پذیر برای شبکه‌های خانگی» انجام داده است به نتایج مشابهی رسیده است. وی بیان می‌کند، از زمان پیدایش رایانه‌های شخصی و ابزارهای اشتراک فایل‌های اینترنتی، تولید و توزیع نامحدود نسخه‌برداری از محتوای دیجیتال بدون کوچک‌ترین نقصان در کیفیت، بسیار آسان شده است. سپس به این نتیجه رسیده است، برای جلوگیری از استفادهٔ غیرقانونی و تکثیر محتوا برای مقاصد تجاری و حمایت از منافع تهیه‌کنندگان محتوای دیجیتالی استفاده از سیستم‌های مدیریت حقوق دیجیتالی غیرقابل انعطاف ضروری است.

از دیگر تهدیداتی که پژوهشگاه علوم و فناوری اطلاعات ایران با آن مواجه است، اشکال مدیریتی است. این تهدید بر اثر عواملی مانند آموزش ناکافی کارکنان سازمان، عدم وجود سیاست درست مستند در خصوص هشدارهای امنیتی، عدم وجود سیاست خروج از بحران و عدم استفاده از شناساگرها و توصیف‌کننده‌های محتوای استاندارد رخ خواهد داد. طبق بررسی‌های انجام شده هیچ یک از موارد مطرح شده در پژوهشگاه علوم و فناوری اطلاعات ایران مد نظر قرار نگرفته است لذا امکان از دست رفتن سهوی یا عمدی منابع اطلاعاتی سازمان، کنترل سیستم‌های کاربری و سرویس‌دهنده‌های شبکه در سازمان وجود دارد و به علت عدم وجود سیاست خروج از بحران، از آنجاکه راه درستی برای بازگرداندن شبکه و منابع اطلاعاتی به وضع قبلی پیش‌بینی نشده، ترمیم آسیب وارد شده بسیار سخت و زمان‌بر خواهد بود. همچنین عدم تعامل با برنامه‌های کاربردی دیگر، از نقاط ضعف برنامهٔ کاربردی طراحی شده در پژوهشگاه علوم و فناوری اطلاعات است. همین‌طور عدم امکان پیگرد از دیگر تهدیداتی است که پژوهشگاه علوم و فناوری اطلاعات ایران با آن مواجه خواهد بود چون در محتواهای اطلاعاتی سازمان از فناوری‌هایی نظیر واترمارکینگ استفاده نشده است و درصورت نسخه‌برادری غیرمجاز، تغییر، تحریف و ... قادر به ردیابی نخواهد بود. ریاضی احمدسرایی (۱۳۸۸) و نمازی (۱۳۹۰) نیز در پژوهش خود در ارتباط با واترمارکینگ دیجیتالی به نتایج مشابهی رسیده‌اند. از نتایج تمام موارد مذکور، لطمات جبران‌ناپذیر به اعتبار سازمان خواهد بود.

با بررسی شناسه‌های تأثیر مطرح شده در جدول ماتریس، برای هر یک از رده‌های اطلاعاتی سازمان و میزان تأثیر

25 Kim

آن‌ها در مأموریت سازمان می‌توان نتیجه گرفت، پژوهشگاه علوم و فناوری اطلاعات ایران، نیازمند بهره‌مندی از سیستم‌هایی است که شرایط ذیل را تأمین نماید:

- از دسترسی‌های غیرمجاز به محتواهای دیجیتالی سازمان جلوگیری نماید.
- دسترسی دائم و بی‌وقفهٔ اطلاعات برای کاربران تأمین گردد.
- دسترسی کاربران به هر منبع اطلاعاتی در سطوح مختلف، الزاماً بر اساس جواز صادر شده باشد.
- تغییرات عمدی و سهوی در اطلاعات غیرممکن باشد.
- هر منبع اطلاعاتی بایستی براساس مکانیزم‌های حساب شده و دقیق، قابل حسابرسی و پیگرد باشد.
- هر تعامل انجام شده توسط کاربران طبق مکانیزمی ثبت شود که غیرقابل انکار باشد.
- رده‌های متفاوتی از کنترل دسترسی اعمال گردد. این مورد از حراست‌های فیزیکی آغاز شده و به مکانیزم‌های پیچیده‌ای مثل نصب و راه‌اندازی سرویس‌دهندهٔ کربروس[۲۶] ختم می‌شود. مکانیزم‌های حراست از کلمات عبور نیز در این بخش گنجانده شده است.

در انتخاب فناوری‌های مورد نیاز نیز باید در نظر داشته باشیم فناوری‌های مورد استفاده مطابق با تحولات فناوری‌های اطلاعاتی و ارتباطی، قابلیت انطباق‌پذیری و گسترش داشته باشند. تاکنون پژوهش‌های زیادی در این زمینه انجام شده است از جمله در پژوهشی که لیو، لیو و شائو (۲۰۱۴) با عنوان «سیستم مدیریت حقوق یجیتال و کنترل دسترسی در شبکه‌های اجتماعی» انجام داده‌اند این مسئله مشهود است و در پژوهش پاتریکیو و دیگران (۲۰۱۱)، با عنوان «یک ساختار معماری عموی برای سیستم‌های مدیریت حقوق دیجیتال» انجام داده‌اند به نتایج مشابهی رسیده‌اند. آن‌ها بیان می‌کند توزیع کالای دیجیتال به‌صورت پیوسته، ما را به سمت سیستم‌هایی برای حفاظت از مالکیت فکری سوق می‌دهد. وی هدف خود را، تشکیل یک ساختار معماری عمومی سیستم مدیریت حقوق دیجیتال بیان نموده است تا بتواند در سیستم‌های ارسال کالای پیوسته از انواع گوناگون به‌کار رود.

بنابراین با شناسایی وضعیت بهره‌گیری از فناوری مدیریت حقوق دیجیتالی در سامانهٔ مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوری اطلاعات ایران، آن‌چه از تحلیل یافته‌های پژوهش حاضر استنباط می‌گردد، گریزناپذیری استفاده از فناوری‌های مدیریت حقوق دیجیتال، مناسب با اهداف پژوهشگاه علوم و فناوری اطلاعات ایران باید باشد.

پیشنهادها

با شناسایی وضعیت بهره‌گیری از فناوری مدیریت حقوق دیجیتالی در سامانهٔ مدیریت پایان‌نامه‌های پژوهشگاه علوم و فناوری اطلاعات ایران، آن‌چه از تحلیل یافته‌های پژوهش حاضر استنباط می‌گردد، گریزناپذیری استفاده از فناوری‌های مدیریت حقوق دیجیتال است، همانطورکه زنگ، پارکین و مورسل (۲۰۱۰) نیز در پژوهش خود به این نتیجه رسیده‌اند. بنابراین با توجه به مأموریت پژوهشگاه علوم و فناوری اطلاعات ایران پیشنهادی به شرح ذیل ارائه شده است که می‌تواند پاسخگوی سئوال چهارم پژوهش نیز باشد.

برای بهبود وضعیت موجود از نظر مدیریت حقوق دیجیتالی پژوهشگاه علوم و فناوری اطلاعات ایران چه اقداماتی می‌توانند در سامانهٔ مدیریت پایان‌نامه‌ها ایجاد نمایند؟

با توجه به تحلیل انجام گرفته بر اساس سیاهه وارسی، الگوی مناسب سیستم مدیریت حقوق دیجیتالی برای پژوهشگاه علوم و فناوری اطلاعات ایران به شرح ذیل می‌باشد:

ابتدا، لازمهٔ استفاده از فناوری مدیریت حقوق دیجیتالی، تعیین هدف و مأموریت سازمان در جهت دسترس‌پذیری منابع اطلاعاتی پژوهشگاه علوم و فناوری اطلاعات ایران، برای تمامی پژوهشگران کشور با توجه به رعایت حقوق مالکیت فکری پدیدآورندگان محتوا است. از آنجاکه فناوری‌های امنیتی مختلف کارکردهای متفاوتی دارند، نیازمند بهره‌گیری از فناوری‌های متفاوتی هستیم.

برای ارائه الگویی مناسب از سیستم مدیریت حقوق دیجیتالی برای پژوهشگاه علوم و فناوری اطلاعات ایران، نیازمند تعیین موجودیت‌ها هستیم. تقریباً موجودیت‌های تعریف شده برای تمامی سیستم‌های مدیریت حقوق دیجیتالی مشابه است. موجودیت‌هایی که در سامانهٔ مدیریت پژوهشگاه علوم و فناوری اطلاعات ایران، باید مد نظر داشت عبارتند از: الف) مالکان محتوا (پژوهشگران، مؤلفان و ...) تهیه‌کننده محتوا (در اینجا پژوهشگاه علوم و فناوری اطلاعات ایران تهیه‌کننده محتوا محسوب می‌گردد یعنی منابع اطلاعاتی سازمان را به‌صورت دیجیتالی تهیه وظیفه اشاعهٔ آن‌را بر عهده دارد. ج) کاربران (شامل شخصیت‌های حقیقی و حقوقی نظیر دانشگاه‌ها، سازمان‌ها، پژوهشگران و ... است. د)

26 Kerberos

توزیع‌کنندهٔ مجوزها: پژوهشگاه علوم و فناوری اطلاعات ایران، نیازمند راه‌اندازی سرویس‌دهنده‌ای است که مجوزها در آن نگهداری و پس از احراز هویت، به کاربران توزیع گردد. همچنین تراکنش‌های مالی نیز در این سرویس‌دهنده انجام و کنترل می‌شود.

با توجه به محدودیت‌های پژوهشگاه علوم و فناوری اطلاعات ایران، الگویی با حداقل تدابیر امنیتی در پنج بخش به شرح ذیل پیشنهاد می‌گردد:

• زیرساخت‌های امنیتی

۱. استفاده از رمزنگاری داخلی (غیر استاندارد): مانند MD5 یا SH1 جهت جایگزینی رمزنگاری نامتقارن (در مدیریت حقوق دیجیتالی از رمزگذاری‌های متقارن و نامتقارن استفاده می‌شود. لذا توصیه می‌شود اولویت نخست استفاده از رمزنگاری‌های استاندارد باشد).

۲. دریافت گواهینامه دیجیتالی جهت تأیید هویت پژوهشگاه علوم و فناوری اطلاعات ایران الزامی است.

۳. بهره‌برداری از سرویس امنیتی لایهٔ سوکت امن، در پژوهشگاه علوم و فناوری اطلاعات ایران الزامی است. اما پیش‌نیاز آن راه اندازی، موارد ۱ و ۲ (رمزنگاری و گواهینامه دیجیتال) می‌باشد.

• صدور مجوزها

۱. الزامی است پژوهشگاه علوم و فناوری اطلاعات ایران دو سرویس‌دهنده تهیه نماید:

الف) یک سرویس‌دهنده جهت قرارگیری برنامهٔ کاربردی تحت وب سازمان

ب) یک سرویس‌دهنده جهت قرارگیری پایگاه داده و فایل‌های پایان‌نامه

۲. الزامی است پایگاه داده مجزا جهت ایجاد جداول مالکان محتوا، توزیع‌کنندهٔ مجوزها و کاربران محتوا ایجاد گردد.

۳. الزامی است برخی اطلاعات ثبت شده در مورد شمارهٔ ۲ (پایگاه داده حاوی جداول مالکان محتوا، توزیع‌کنندهٔ مجوزها و کاربران محتوا) رمزنگاری گردد. از جمله کلمهٔ عبور، سطح دسترسی و نظایر آن.

• پیگردها:

۱. ضروری است پژوهشگاه علوم و فناوری اطلاعات ایران، فناوری واترمارکینگ را در محتواهای دیجیتالی تعبیه نماید. همچنین پیشنهاد می‌شود واترمارک ایجاد شده همراه با اطلاعات کنترل نسخه‌برداری باشد.

۲. در پژوهشگاه علوم و فناوری اطلاعات ایران برای پیگرد رویدادها، ثبت لاگهای[27] سیستمی ضروری می‌باشد.

۳. الزامی است کلیه تراکنش‌های مالی و کدهای پیگیری آن ثبت گردد.

• پشتیبانی و نگهداری

۱. پژوهشگاه علوم و فناوری اطلاعات ایران لازم است کلیه اقدامات لازم جهت ریدبندی[28] سرویس‌دهندهٔ اشاره شده در بخش صدور مجوزها (مورد ۱: بند ب) را اعمال نماید.

۲. پژوهشگاه علوم و فناری اطلاعات ایران لازم است از کلیهٔ پایگاه داده‌ها و فایل‌های موجود بر روی سرویس‌دهنده، نسخهٔ پشتیبان به‌صورت روزانه و ماهیانه تهیه و در مکان امنی نگهداری نماید.

• ارتباط با سازمان‌های خارجی

الزامی است سازمان جهت انجام تراکنش‌های مالی زیرساخت‌های ارتباطی را با بانک‌های مورد نظر برقرار نماید.

References

Braid, A (2004). The use of digital rights management system in a document supply service. Interlending & Document Supply, 32(3): 189-191.

Burstrom, A; Callander, J (2003). Digital Rights Management: Evaluation of existing systems. Thesis project done at Information Theory. Linkoping University.

Ciocoiu, CN (2011). Consideration about Intellectual Property Rights, Innovation and Economic Growth in the Digital Economy. Economia. Seria Management, 14(2): 310-323.

Deyhimi, S (2012). Foundations and Legal Effects Distribution Rights in Intellectual Property Rights. M.A Thesis on Law. Tarbiat Modares University. (Persian)

Falahati Marvast, F(2010). Intellectual Property Law with an Emphasis on Copyright. M. A Thesis on Law. Tehran Payame Noor University. (Persian)

Gaber, T (2012). Support Consumer's s Mights in DRM: A Secure and Fair Solution to Digital License Reselling over the Internet. The Degree of Doctor of Philosophy in the faculty of Engineering and Physical Sciences. The University of Manchester.

Iranian Research Institute for Information Science and Technology. About Research Institute Goals, Tasks and Powers (2014). Retrieved March 13, 2014, from: http://www.irandoc.ac.ir/about-us/mission.html (Persian)

[27] Logs
[28] Raid

Karandish, N (2006). Failure to Investigate the Intellectual Property Rights Laws in Order to Use Them in Digital Libraries Country. M. A Thesis on Librarianship and Information. Faculty of Psychology and Educational Sciences. Tehran University. (Persian)

Kim, H; Lee, Y; Park, Y(2010). A robust and flexible digital rights management system for home networks. The Journal of systems and Software, (83): 2431-2440.

Liu, E; Liu, Z; Shao, F(2014). Genetic and Evolutionary Computing: Proceedings of the Seventh International Conference on Gene tic and Evolutionary Computing, ICGEC 2013, August 25-27. Switzerland: Springer International Publishing. 257-266.

Matlabi, D (2008). Copyright in the Digital World. Keta`b-e Ma`h-e Kolliya`t. Information, Communication and Knowledgology. 11(16): 47-62. (Persian)

Namazi, F (2011). Digital Watermarking According to the Human Visual System. M. A Thesis on Electrical Engineering. Babol Noshirvani University of Technology. (Persian)

Onsorynezhad, S (2014). Civil Liability in Information and Communication Technology Law (Electronic Communications).M. A. Thesis On Private Law, Kharazmi University.(Persian)

Patriciu, VV (2011). A Generalized DRM Architectural Framework. Advances in Electrical and Computer Engineering, 11(1): 43-48.

Reyazi A; Saraei, V (2009). Digital Watermarking in Wavelet transform. M.A Thesis on Electrical Engineering. Department of Electrical and Computer, Shiraz University. (Persian)

Tabataba`i, SH (2010). Legal Requirements for E-commerce Security with an Emphasis on Iran and Rules of International Law. MA Thesis on International Business Law, Tabataba`i University. (Persian)

Tajabadi, R; Ranjbari, S(2010). Application of Copyright and its Rules and Regulations in the Electronic Environment. Information Seeking & Information Science Monthly. (135): 32-41. (Persian)

Tassel, JV (2006). Digital Rights Management. Amesterdam: Elsevier.

Wolf, Patrick; Steinebach, Martin and Diener, Konstantin. (2006). Complementing DRM with digital watermarking: mark, search, retrieve. Online Information Review, 31 (1): 10-21.

Zeng, W; Parkin, S; Van Moorsel, A (2010). Digital Rights Management. University of Newcastle upon Tyne: Computing Science, (CS -TR- 1223): 3-48.

Zhang, Z. (2009). Security and Trust in Digital Rights Management: A Survey. International Journal of Network Security, 9(3): 247-263.

[DOR: 20.1001.1.24237418.1395.3.1.5.9]

Human Information Interaction. Vol. 3, No. 1
http://hii.khu.ac.ir
Original Article

Using Digital Right Management technology in IRANDOC ETD System

Parichehr Agha SeyyedJavadi: MA Student, field of Information Science and Knowledge, Islamic Azad University Sciense and Research Brach, Tehran. p.seyedjavadi@gmail.com
Mehdi Alipour-Hafezi: PhD, Knowledge and Information Science, Assistant Professor, Department of Knowledge and Information Science, Faculty of Psychology and Education Sciences, Allameh Tabataba'i University (ATU), Tehran, Iran.

Abstract

Background and Aim: Easing the probability of violation of intellectual property rights and unauthorized access of digital resources is one of the most important consequences of information and communication technologies like the internet. The purpose of this research is to identify the state of Using Digital Right Management technology in IRANDOC ETD system.
Method: Research method is a case study, applied research. Instrument was a checklist, that was principally prepared by NSA INFOSEC IAM.
Findings: Results were signified in three sections: Section one; is related to needed information for security assessment of electronic theses and dissertation (ETD) system in IRANDOC. Data was collected by structured interview and observation. Section two; covered data that collected by OICM matrix. In fact, information categories in organization flowchart and value of each one in organization goals were identified. Section three; is related to identifying the threats and their effects that organization may come across.
Conclusion: Results demonstrate that, as a matter of security infrastructures, IRANDOC is located in an unfavorable condition. Consequently factors such as unauthorized access, forms of management, and lack of prosecution would threaten their services. Therefore, they should incorporate techniques such as DRM for collecting, managing, maintenance and dissemination.

Keywords: Digital Rights Management, Copy right, Information and Communication Technology, Security technique, Digital resource, Electronic Theses and Dissertation (ETD), Unauthorized access.

[DOR: 20.1001.1.24237418.1395.3.1.5.9]