نشریه علمی "پدافند الکترونیکی و سایبری"
سال هفتم، شماره ۲، تابستان ۱۳۹۸، ص ۵۱-۴۱

میزان تأثیرات تهدیدهای سایبری بر یکدیگر در پروژه‌های فناوری اطلاعات با رویکرد نقشه شناختی فازی

حمزه امین‌طهماسبی[1*]، مرتضی همتی آسیابرکی[2]

۱- استادیار، گروه مهندسی صنایع، دانشکده فنی و مهندسی شرق، دانشگاه گیلان

۲- دانشجوی کارشناسی ارشد، گروه مهندسی صنایع، دانشکده فنی فومن، دانشگاه تهران، فومن، ایران

(دریافت: ۹۷/۰۲/۱۱، پذیرش: ۹۷/۰۷/۲۱)

چکیده

عدم تطابق زمان و هزینه ازجمله مهم‌ترین دلایل شکست پروژه‌های فناوری اطلاعات، محسوب می‌شوند؛ اما باید در نظر داشت که غفلت از مباحث امنیتی مخصوصاً در پروژه‌هایی با ماهیت کار با داده و اطلاعات کامپیوتری می‌تواند خساراتی جبران‌ناپذیر به سازمان پروژه وارد نماید. در این میان، شناخت عواملی که می‌توانند یک پروژه فناوری اطلاعات را در فضای سایبری مورد تهدید قرار دهند و شناخت میزان اثرگذاری و اثرپذیری هر یک از این عوامل بر یکدیگر از اهمیت بالایی برخوردار است. درواقع مدیر پروژه با آگاهی از میزان تأثیرگذاری معیارها، می‌تواند در تصمیم‌گیری جهت پیشگیری از وقوع این تهدیدات به‌صورت کارآمدتر عمل نماید. در این پژوهش، با استفاده از مرور ادبیات، تجزیه‌وتحلیل نظرات و استفاده از نظر متخصصین، عوامل اصلی که می‌توانند یک پروژه فناوری اطلاعات را در فضای سایبری مورد تهدید قرار دهند، شناسایی می‌شود. در گام بعد تعدادی از این تهدیدات با استفاده از آزمون فریدمن حذف شده و ۶ تهدید مهم‌تر از دید خبرگان باقی می‌ماند. سپس با استفاده از روش تحلیل سلسله مراتبی (AHP) وزن آن‌ها به‌دست‌آمده و درنهایت تأثیرات هر یک از این عوامل بر یکدیگر با استفاده از روش نقشه شناختی فازی (FCM) مشخص می‌گردد. بر اساس نتایج به‌دست‌آمده، عدم استفاده از سامانه‌های رمزگذاری و احراز هویت مناسب، تأثیرگذارترین و جاسوسی سایبری تأثیرپذیرترین این عوامل می‌باشند.

کلیدواژه‌ها: پروژه‌های فناوری اطلاعات، فضای سایبری، نقشه شناختی فازی (FCM)، تهدیدات سایبری

۱- مقدمه

واضح است که هرجایی که زمینه‌ای برای خدمت‌رسانی به گروهی خاص و یا آحاد مردم فراهم شود مباحث مربوط به انجام پروژه‌ها و در رأس آن مدیریت پروژه وارد میدان خواهد شد. اکنون و با فراهم آمدن بستر وسیعی برای انجام کارها به‌صورت الکترونیکی، پروژه‌های فناوری اطلاعات[1] و شیوه مدیریت کارآمد آن‌ها و آشنایی با ریسک‌ها و سایر ویژگی‌های آن به دغدغه اصلی متخصصان این حوزه بدل شده است.

در کل، فناوری اطلاعات و ارتباطات مجموعه‌ای از سخت‌افزارها و نرم‌افزارها به همراه فکر است که گردش و بهره‌برداری از اطلاعات را امکان‌پذیر می‌سازد. این مفهوم از تعامل بخش‌های رایانه، اطلاعات و ارتباطات مخابراتی به‌وجود می‌آید. امروزه فناوری اطلاعات و ارتباطات رشد گسترده‌ای بین کشورهای مختلف داشته و مزایای فراوانی در بهبود کیفیت زندگی ایجاد کرده است. ازاین‌رو برای جذب منافع حاصل از فناوری اطلاعات و ارتباطات، باید این فناوری اجرا و به‌صورت کارآمد استفاده شود.

این امر بسیار مهم است که اگر کشورهای در حال رشد شکاف دیجیتالی موجود در کشور یا میان کشورهای دیگر را به‌خوبی شناسایی نکرده و یا به آن بی‌توجهی کنند به‌راحتی با عقب‌ماندگی روبه‌رو خواهند شد. این موضوع جایگاه فناوری اطلاعات و ارتباطات را در رشد و پیشرفت کشورها نشان می‌دهد و ضرورت دسترسی و استفاده از فناوری اطلاعات و ارتباطات را به‌خوبی مشخص می‌سازد.

در سال‌های اخیر درخواست استفاده از فناوری‌ها و راه‌کارهای مرتبط با فناوری اطلاعات و ارتباطات در کشورهای درحال‌توسعه، قابلیت‌ها و امکانات زیادی را برای ایجاد تحول به‌وجود آورده است. دستیابی به فرصت‌های فراوان برای مردم جامعه، عبور از شکاف دیجیتالی و دسترسی به منافع اطلاعاتی و فراهم‌سازی خدمات به‌وسیله فناوری اطلاعات و ارتباطات، می‌تواند نخستین مرحله در این تحول باشد. البته ورود فنّاوری و ماهیت آن برای نخستین بار

*رایانامه نویسنده مسئول: amintahmasbi@guilan.ac.ir

1- Information Technology

همیشه با مقاومت در استفاده از آن مواجه شده حتی زمانی که منافع اقتصادی اثبات‌شده‌ای با خود به همراه داشته است. این امر دلیلی واضح بر وجود کمبود اطلاعات و ناآگاهی است. ازاین‌رو، منافع حاصل از انقلاب اطلاعاتی و ارتباطاتی تنها به شهروندان و اشخاص خاص محدود نشده بلکه در مفهوم کلان می‌تواند تأثیرات وسیعی بر اقتصاد ملی و جهانی داشته باشد.

توسعه فناوری اطلاعات و ارتباطات در هر جامعه‌ای درهای جدیدی برای استفاده از امکانات نامحدود بازکرده و با خود کاهش فقر را به همراه داشته است. دسترسی به فناوری اطلاعات و ارتباطات به جذب و نگهداری مشاغل و زنده ماندن اقتصادی کمک کرده و چشم‌انداز مثبتی از آینده در پیش رو ایجاد خواهد نمود.

برخلاف بسیاری از پروژه‌ها در صنایع دیگر، پروژه‌های فناوری اطلاعات بسیار متنوع می‌باشند. بعضی از پروژه‌ها شامل تعداد محدودی از افراد هستند که سخت‌افزارهای رایج و در دسترس و نرم‌افزارهای مربوط به آن‌ها را نصب می‌کنند و بعضی دیگر شامل صدها نفر هستند که فرآیندهای تجاری سازمان را تحلیل می‌کنند و سپس نرم‌افزارهای جدیدی را برای برآورده کردن نیازهای تجاری در یک همکاری مشترک با کاربران بهبود می‌دهند. ماهیت پروژه‌های نرم‌افزاری متنوع‌تر از پروژه‌های سخت‌افزار محور است. بهبود یک پروژه نرم‌افزاری ممکن است بسیار راحت همچون بهبود یک برنامه اکسل و اکسس مستقل و یا بسیار پیچیده مانند طراحی یک سامانه تجارت الکترونیک جهانی که از یک‌زبان برنامه‌نویسی پیشرفته و مدرن استفاده می‌کند باشد. به دلیل تنوع پروژه‌های فناوری اطلاعات و ناب و جدید بودن زمینه موردنظر، این مهم است که از بهترین و به‌روزترین تدابیر مدیریتی در پروژه‌های مختلف استفاده شود [۱].

مدیریت پروژه‌های فناوری اطلاعات با مدیریت سایر پروژه‌هایی که درگذشته با آن‌ها سروکار داشته‌ایم، کاملاً متفاوت است. چراکه در دنیای فناوری اطلاعات شاهد هجومی همه‌جانبه هستیم. نیازهای همیشه در حال تغییر، سازگاری سخت‌افزاری، اشکالات نرم‌افزاری، پهنای باند شبکه، مسائل امنیتی و فقدان مهارت‌های لازم در سطوح مختلف از طراحی گرفته تا پیاده‌سازی، صرفاً نمونه‌هایی اندک از چالش‌های پیش رو پروژه‌های فناوری اطلاعات و داده است. مسائل امنیتی و در رأس آن‌ها تهدیدات سایبری که می‌تواند سامانه‌های خاص و زیرسامانه‌های مربوطه را به‌طور هم‌زمان و از راه دور مورد هدف قرار دهد [۲] از مهم‌ترین چالش‌های موجود در پروژه‌های فناوری اطلاعات هست. در سال ۲۰۱۷ گزارشی توسط انجمن اقتصاد جهانی که نشست سالانه آن در ژنو برگزار می‌شود و به دنبال جلب‌توجه کسب کارها در سراسر جهان و رسیدن به اعتباری در عرصه پیش‌بینی در این زمینه می‌باشد منتشر شد که نشان می‌دهد تهدیدات سایبری افزایش خواهد یافت و در این مسیر حملاتی چون منع سرویس، نقض داده‌ها، حملات مربوط به ارائه‌دهندگان خدمات رایانش ابری و اخاذی ازجمله نگرانی‌های عمده برای سازمان‌های IT محور خواهد بود [۳]. درواقع تهدیدات سایبری در پروژه‌های فناوری اطلاعات یکی از انواع ریسک‌های امنیتی موجود در این نوع پروژه‌ها است. عدم آگاهی از این ریسک‌ها و تأثیراتشان نسبت به یکدیگر، منجر می‌شود که تمرکز و زمان و هزینه‌ای که در حوزه تهدیدات سایبری باید معطوف گردد به طیف وسیعی از تهدیدات پراکنده شود که این پراکندگی در موارد فوق منجر به کاهش کیفیت و کارایی سازمان در انجام این نوع از پروژه‌ها و یا حتی در مواردی غفلت از برخی از این تهدیدات می‌گردد که می‌تواند منجر به شکست آن‌ها شود. بدیهی است مؤثرترین تهدید خود می‌تواند زمینه‌ساز بروز سایر تهدیدات باشد و جلوگیری از آن می‌تواند مانع وقوع سایر تهدیدات گردد و علاوه بر زمان و با توجه به محدود بودن بودجه‌ای که برای دفاع و جلوگیری از حملات سایبری تخصیص می‌یابد [۴]، باعث می‌شود در هزینه‌های مصرفی نیز به‌شدت صرفه‌جویی شود. ازاین‌رو، هدف این پژوهش آشنایی با تهدیدات سایبری در این پروژه‌ها و تعیین تأثیرات آن‌ها بر سازمان و گروه پروژه است. در حقیقت نوآوری موضوعی این مقاله در خصوص تهدیدات سایبری در پروژه‌های فناوری اطلاعات با ماهیتی بسیار متفاوت از تهدیدات سایبری است که تاکنون انجام نشده است. در خصوص روش حل نیز، نوآوری مقاله در استفاده ترکیبی از دو رویکرد AHP_FCM می‌باشد؛ که رویکرد AHP آن برای مشخص کردن اهمیت و وزن هر یک تهدیدات مورد استفاده قرار گرفته است. سپس این اوزان به‌عنوان ورودی برای محاسبات و تحلیل‌های روش FCM استفاده می‌گردد. روش FCM نیز از روش‌های نوین در حوزه مباحث MCDM محور محسوب می‌شود که به‌مراتب از روش‌های DEMATEL و ANP و ... در بررسی روابط میان معیارها کامل‌تر و برتر است [۵]. درواقع با استفاده از روش FCM و تعیین مؤثرترین تهدید بر روی سایر تهدیدات، می‌توان تنها با تمرکز بر روی تهدید موردنظر، زمینه رشد و نمو سایر تهدیدات را تا حد بسیار زیادی از بین برد و عملاً با حذف مؤثرترین تهدید، سایر تهدیدات دیگر عامل اصلی ایجادکننده خود را نمی‌یابند؛ یعنی با تمرکز بر روی مؤثرترین تهدید و حذف آن، پنج تهدید دیگر نیز خودبه‌خود کاهش یافته و یا از بین خواهند رفت. ازاین‌رو این پژوهش علاوه بر داشتن یک رویکرد توسعه‌ای، یک رویکرد کاربردی برای سازمان‌های انجام دهنده پروژه‌های فناوری اطلاعات را داراست.

۲- مبانی نظری و پیشینه پژوهش

شناسایی ریسک‌های موجود در پروژه‌های فناوری اطلاعات می‌تواند به‌عنوان چالشی عمده برای مدیران تلقی گردد [۶]. جریان اول تحقیقات در این زمینه بر روی ریسک‌های مربوط به بهبود نرم‌افزار است [۱]. فهرست‌های متفاوتی از ریسک‌های موجود در پروژه‌های فناوری اطلاعات در پژوهش‌های پیشین ذکر شده است. به‌عنوان مثال بواهم [۷] تعداد ده ریسک عمده موجود بر سر راه بهبود نرم‌افزار که موفقیت پروژه‌ها را تهدید می‌کند، تدوین کرد. بارکی و همکاران [۸] ۳۵ مورد از متغیرهای ریسک را در پروژه‌های نرم‌افزار مشخص و آن‌ها را در پنج دسته اصلی طبقه‌بندی کرده است. در همین راستا، والاک و همکاران [۹] طرحی را با ۵۰۷ نفر از مدیران پروژه‌های نرم‌افزاری تهیه و نتیجه حاصله را در شش دسته یا بعد ریسکی قرار داده است. این دسته‌بندی بدین‌صورت است: گروه، محیط سازمان، نیازها، برنامه‌ریزی و کنترل، کاربر و پیچیدگی پروژه.

جریان دوم تحقیقات متمرکز بر روی ریسک‌های مربوط به سرمایه‌گذاری در پروژه‌های فناوری اطلاعات [۱] و مباحث برون‌سپاری این پروژه‌ها، از یک دیدگاه وسیع‌تر است. ریسک‌های موجود در این زمینه توسط ناکاتسو و لاکوو [۱۰] به‌صورت زیر دسته‌بندی شده است: قابلیت‌های مشتری، قابلیت‌های فروشنده، روابط بین مشتری و فروشنده، مدیریت قراردادها، ریسک‌های راهبردی، قوانین و مقررات، مباحث امنیتی، مباحث مالی، موضوعات جغرافیایی، شهرت شرکت یا روحیه کارمندان، ریسک‌های فنّاورانه.

با توجه به وجود ادبیات غنی درباره ریسک‌های موجود در این نوع پروژه‌ها و علی‌رغم تحقیقات و بررسی‌های صورت گرفته در مورد مباحث امنیتی خاص این پروژه‌ها، تاکنون و با بررسی ادبیات در این زمینه، درباره تهدیدات سایبری موجود در پروژه‌های IT تحقیقات کمتری صورت گرفته است. از ریسک‌های امنیتی موجود در پروژه‌های IT می‌توان به تهدیدات سایبری در این پروژه‌ها اشاره کرد. در جدول (۱) می‌توان زمینه‌های کارشده و همچنین شکاف تحقیقاتی موجود در حوزه تهدیدات سایبری در پروژه‌های فناوری اطلاعات را به‌وضوح مشاهده کرد.

تهدیدات سایبری ازجمله ریسک‌های امنیتی است که در صورتی بی‌توجهی و غفلت نسبت به آن پروژه‌های فناوری اطلاعات را با عواقب و پیامدهای سنگینی روبه‌رو خواهد کرد، به‌طوری‌که نه‌تنها باعث شکست پروژه و عدم توفیق در دست‌یابی به اهداف پروژه خواهد شد بلکه پیامدهای حقوقی و قضایی آن تا مدت‌ها می‌تواند گریبان‌گیر سازمان انجام دهنده پروژه باشد؛ بنابراین، تهدیدات سایبری از جمله عوامل تأثیرگذار و حیاتی در یک پروژه با ماهیت فناوری اطلاعات است که نیازمند توجه اساسی نه‌تنها مدیران پروژه بلکه گروه پروژه و حتی کاربران نهایی است.

جدول (۱): تحقیقات انجام‌شده در حوزه پروژه‌های فناوری اطلاعات

منبع	محدودیت‌های پروژه‌های IT	مدیریت ریسک	امنیت اطلاعات	تهدیدات سایبری
[۱]		✓		
[۷]	✓	✓	✓	
[۸]		✓		
[۹]		✓		
[۱۰]	✓	✓	✓	
[۱۶]			✓	
[۱۷]		✓		
[۱۸]			✓	
[۱۹]		✓		
[۲۰]	✓			
[۲۱]	✓			
[۲۲]	✓			
[۲۳]	✓			
[۲۴]	✓			
[۲۵]	✓	✓		
[۲۶]			✓	
[۲۷]			✓	
[۲۹]	✓	✓		
[۳۰]	✓	✓		
[۳۱]	✓	✓		
[۳۲]	✓	✓		
[۳۳]	✓	✓		
[۳۴]	✓	✓		
[۳۵]	✓	✓		
[۳۶]	✓	✓		
[۳۷]	✓	✓	✓	
[۳۸]	✓	✓	✓	
[۳۹]	✓	✓	✓	
[۴۰]	✓	✓	✓	
[۴۱]	✓	✓		
[۴۲]		✓		
[۴۳]			✓	

تهدیدات موجود در حوزه فناوری اطلاعات حاصل از مرور ادبیات و تجزیه و تحلیل نظرات متخصصان حوزه پروژه‌های فناوری اطلاعات در جدول (۲) خلاصه شده است.

جدول (۲): تهدیدات شناسایی‌شده در حوزه پروژه‌های فناوری اطلاعات

شماره	تهدید شناسایی‌شده	منابع
۱	تهدیدهای مرتبط با کاربران مجاز	[۴۳]
۲	عدم آگاهی کاربران	[۱۶]،[۱۸]
۳	ریسک کاربر	[۱]،[۹]،[۱۷]،[۲۵]
۴	عدم استفاده از سامانه‌های رمزگذاری و احراز هویت مناسب	[۲۲]
۵	تهدیدهای مرتبط با برنامه‌های کاربردی	[۴۳]
۶	تهدیدهای مرتبط با خدمات زیرساخت اطلاعاتی بحرانی	[۴۳]
۷	عدم وجود سیاست‌ها و فرآیندهای امنیتی	[۱۶]
۸	ریسک مرتبط با محیط سازمانی	[۱]،[۹]،[۱۷]
۹	تهدیدهای مربوط به دارایی اطلاعاتی	[۴۳]
۱۰	تهدیدهای موجود هنگام برون‌سپاری	[۱۶]
۱۱	ریسک مربوط به تیم	[۱]،[۹]،[۱۷]
۱۲	عدم آگاهی از فرهنگ و افراد سازمان	[۱۶]
۱۳	افراد و کارکنان سازمان	[۱۶]
۱۴	عدم درک این‌که فرآیند امنیت اطلاعات یک موضوع تجاری ست نه یک موضوع فنی	[۱۸]
۱۵	تهدیدهای سخت‌افزاری	[۴۳]
۱۶	تهدیدهای نرم‌افزاری	[۴۳]
۱۷	ریسک کنترل و برنامه‌ریزی	[۱]،[۹]،[۱۷]
۱۸	ریسک الزامات	[۱]،[۹]،[۱۷]،[۲۵]
۱۹	صنایع پیشرو در حوزه فناوری اطلاعات	[۱۶]
۲۰	ریسک پیچیدگی	[۱]،[۹]،[۱۷]

۳- روش‌شناسی

هدف از این پژوهش شناسایی تهدیدات سایبری موجود در پروژه‌های IT به‌صورت تحلیلی است که با رویکرد نقشه شناختی فـازی (FCM[1]) گـراف تأثیرات این تهدیدها نسبت به هم رسم و مؤثرترین تهدید نسبت به سایر تهدیدات مشخص شده است تا بااستفاده از آن بتوان در جهت جلوگیری از وقوع تهدید موردنظر اقدام و با انجام یک عمل پیشگیرانه از تبعات ناگوار ناشی از وقوع آن جلوگیری نمود. جهت شناسایی تهدیدات سایبری موجود در پروژه‌های فناوری اطلاعات ابتدا، ۲۴ تهدید موجود در حوزه فناوری اطلاعات به‌وسیله مرور ادبیات و تجزیه و تحلیل نظرات متخصصان حوزه پروژه‌های فناوری اطلاعات شناسایی و با تعیین مهم‌ترین تهدیدات از دیدگاه متخصصان و با استفاده از روش فریدمن، ۶ تهدید اساسی که در ساختار پروژه‌های IT بیشتر مشاهده می‌شود مشخص شدند. ساختار آزمون فریدمن بدین‌صورت است که معیارهای موجود در یک پژوهش را بر اساس میانگین‌های به‌دست‌آمده از نظر خبرگان رتبه‌بندی می‌نماید و معیار(هایی) که امتیازشان از میانگین کل به‌دست‌آمده کمتر باشند، حذف می‌گردند. در این راستا از پرسشنامه طیف ۵ حالته لیکرت استفاده شده است. عدد ۱ در تحلیل‌ها، به منزله ضعیف‌ترین تهدید و عدد ۵ به‌مثابه قوی‌ترین تهدید می‌باشد. با توجه به این‌که میانگین به‌دست‌آمده از کل تهدیدات ۳ است تمامی تهدیدها با میانگین زیر ۳ حذف می‌شوند. شش تهدید سایبری باقی‌مانده ورودی مرحله بعد را تشکیل می‌دهند. با توجه به موضوع خاص پژوهش لازم بود تا جامعه آماری خاصی به پرسشنامه پاسخ دهند، لذا جامعه آماری به‌صورت هدفمند و با شرایط ویژه‌ای انتخاب شدند. تحصیلات در رشته مهندسی کامپیوتر-نرم‌افزار، تسلط به زبان‌های برنامه‌نویسی، داشتن سابقه فعالیت به‌عنوان مدیر پروژه در شرکت‌های توسعه محصولات نرم‌افزاری ازجمله این شرایط بوده‌اند. نحوه انتخاب این افراد با خصوصیات فوق‌الذکر بسیار حائز اهمیت است. لذا بهترین وضعیت، استفاده از اعضاء سازمان نظام صنفی رایانه بود؛ با توجه به محدودیت دسترسی به متخصصان که تمامی شرایط فوق را داشته باشند، از هشت شرکت بزرگ در زمینه پروژه‌های فناوری اطلاعات در ایران تعداد ۱۰ خبره انتخاب و پرسشنامه‌ها توسط ایشان تکمیل گردید [۱۱]. لازم به ذکر است با توجه به اینکه پرسشنامه موردنظر یک پرسشنامه با ماهیت کاملاً تخصصی است، مدیران فنی و یا تحلیلگران سامانه این شرکت‌ها که معیارهای تجربه بالای ۱۵ سال در پروژه‌های فناوری اطلاعات و آشنایی با مفاهیم امنیتی موجود در این پروژه‌ها و همچنین دارای حداقل مدرک تحصیلی کارشناسی ارشد را داشته‌اند، به‌عنوان خبره انتخاب شدند. ورودی‌های مدل حاصل پاسخ متخصصین مربوطه به دو پرسشنامه AHP و FCM است؛ که در زیر به توضیح کامل این دو پرسشنامه پرداخته می‌شود.

1- Fuzzy Cognitive Mapping

۳-۱- پرسشنامه AHP

در روش AHP برای تهیه پرسشنامه از روش مقایسه زوجی استفاده می‌شود. در روش مقایسات زوجی از طیف ۹ درجه‌ای ساعتی استفاده می‌شود و تمامی معیارها به‌صورت دوبه‌دو باهم مقایسه می‌شوند. در مقایسه زوجی قاعده‌ای به نام شرط معکوسی وجود دارد. برای نمونه اگر ترجیح معیار A به معیار B ۵ باشد، آنگاه ترجیح B به A، ۱/۵ است. می‌توان خط‌کش مقیاس را در جدول (۳) مشاهده کرد.

جدول (۳): طیف ۹ درجه‌ای ساعتی

ارزش	وضعیت مقایسه i نسبت به j	توضیح
۱	ترجیح یکسان	عنصر i و j اهمیت برابری دارند.
۳	کمی مرجح	عنصر i و j کمی مهم‌تر است.
۵	خیلی مرجح	عنصر i از j مهم‌تر است.
۷	بسیار زیاد مرجح	عنصر i از j خیلی مهم‌تر است.
۹	کاملاً مرجح	عنصر i از j کاملاً مهم‌تر است.
۶-۸-۴-۲	بینابین	اهمیت‌های بینابین را نشان می‌دهد.

۳-۲- پرسشنامه FCM

این پرسشنامه جهت تعیین میزان تأثیرگذاری و یا تأثیرپذیری هر یک از تهدیدات نسبت به یکدیگر استفاده می‌شود. در این پرسشنامه سطر و ستون جدول مورد نظر را معیارهای تعریف‌شده برای مسئله که در این بررسی ۶ مورد است، تشکیل می‌دهند و بین این سطر و ستون مقادیر عددی که به‌صورت فازی نیز هستند درج شده است. در مجموع چهار نوع فازی‌ساز وجود دارند که عبارت‌اند از فازی‌ساز مثلثی، فازی ذوزنقه‌ای، فازی‌ساز منفرد، فازی‌ساز گوسی [۱۲] که در این پژوهش با توجه به ماهیت عدم قطعیت داده‌های مسئله اقدام به استفاده از فازی‌ساز مثلثی شده است. کاربرد عدد فازی مثلثی برای دست‌یابی به انعطاف و دقت بیشتر در قضاوت‌های کارشناسانه به‌ویژه در گزینه‌هایی که دارای معیارهای کیفی با پیچیدگی بیشتری هستند، ملموس‌تر است. هر یک از این اعداد فازی که به‌صورت یک عدد فازی مثلثی نوشته شده است، نمایانگر یک متغیر زبانی ست. به‌عنوان‌مثال مقدار (۰،۰،۰) یعنی معیار i هیچ تأثیری بر معیار j نمی‌گذارد و (۰،۱،۲) به‌منزله تأثیر بسیار کم و مقدار (۸،۹،۱۰) به‌منزله تأثیر بسیار زیاد معیار i بر j خواهد بود، (جدول (۴)).

نگاشت ادراکی فازی (**FCM**) اولین بار توسط کاسکو [۱۳] در سال ۱۹۸۶ معرفی گردید. بر مبنای تعریف وی FCM یک نمودار گرافیکی هدایت‌شده با هدف نمایش روابط علت و معلولی میان عوامل است که رابطه میان هر یک جفت عامل در این مدل در بازه‌ی [۱ و ۱-] مشخص می‌شود.

جدول (۴): اعداد فازی مورد استفاده برای متغیرهای زبانی

واژه زبانی	اعداد فازی
بسیار کم	(۰،۱،۲)
خیلی کم	(۱،۲،۳)
کم	(۲،۳،۴)
نسبتاً کم	(۳،۴،۵)
متوسط	(۴،۵،۶)
نسبتاً زیاد	(۵،۶،۷)
زیاد	(۶،۷،۸)
خیلی زیاد	(۷،۸،۹)
بسیار زیاد	(۸،۹،۱۰)

اجزاء اصلی این مدل، گره‌ها و روابط علت و معلولی میان مفاهیم (معیارها) در این رویکرد است.

نقشه شناختی فازی یک روش‌شناسی مدل‌سازی برای سامانه‌های پیچیده تصمیم‌گیری است. یک نقشه شناختی فازی رفتار یک سامانه را بر اساس معیارها و مفاهیم موجود در آن توصیف می‌کند که هرکدام از این مفاهیم نشان‌دهنده یک هویت، وضعیت، متغیر یا یک خصوصیت سامانه است.

در حقیقت FCM توسعه‌یافته نگاشت‌های ادراکی (CMs[1]) است که برای اولین بار توسط رابرت اکسلراد، دانشمند علوم سیاسی، در دهه ۱۹۷۰ پیشنهاد و به‌کار گرفته شد. اگر قواعد نگاشت‌های ادراکی، با هر عددی بین [۱ و ۰] و یا [۱ و ۱-] سنجیده شوند یا از کلمات وزنی، مانند «کمی»، «مقداری» یا «بیشتر یا کمتر» استفاده شود، نگاشت‌های ادراکی به نگاشت ادراکی فازی تبدیل می‌شود. نگاشت‌های ادراکی فازی یک روش محاسباتی نرم برای مدل کردن سامانه‌ها است که به‌صورت هم‌زمان تئوری‌های شبکه‌های عصبی و منطق فازی را ترکیب کرده و به‌کار برده است. در FCM، ساختارهای نموداری فازی برای نشان دادن استدلال عِلّی هستند و فازی بودن آن‌ها درجات مبهمی از علیت بین مفاهیم را نشان می‌دهد [۱۴].

یک نگاشت ادراکی فازی یا FCM، تصویری عِلّی رسم می‌کند. این نگاشت حقایق، اشیاء و فرآیندها را به ارزش‌ها، سیاست‌ها و اهداف ارتباط می‌دهد و به شما اجازه می‌دهد تا چگونگی اعمال متقابل و نحوه عملکرد حوادث پیچیده را پیش‌گویی کنید.

1- Cognitive Maps

نگاشت‌های ادراکی فازی به شما امکان تحلیل بر مبنای «چه می‌شود- اگر» را می‌دهند.

گره‌های موجود در این روش به‌وسیله کمان‌های وزن‌دار با یکدیگر ارتباط داخلی دارند. هر ارتباط داخلی میان دو گره i و j دارای وزنی معادل w_{ij} است که در حقیقت نشان‌دهنده رابطه‌ی علت و معلولی میان آن دو گره هست.

اگر بین دو متغیر یک رابطه مستقیم (مثبت) وجود داشته باشد، افزایش یا کاهش در متغیر علت موجب تغییری در همان جهت (افزایش یا کاهش) در متغیر معلول خواهد شد. اگر یک رابطه معکوس (منفی) وجود داشته باشد، تغییری که متغیر علت پیدا می‌کند در جهت عکس به متغیر معلول اعمال می‌شود. در FCM گره‌ها یا ملاحظات (معیارها) نیز فازی هستند.

با توجه به اینکه روش نقشه شناختی فازی بر اساس روابط علت و معلولی بنا شده است، استفاده از آن نیز مزایا و نتایجی را همراه خود خواهد داشت و سؤالات و ابهاماتی همچون موارد زیر را برطرف خواهد کرد:

۱. مشخص کردن راه‌های دستیابی به یک هدف
۲. تعیین اثر تغییر بر سازمان و یا جنبه‌های سازمانی (افزایش و یا کاهش در متغیرهای خاص)
۳. تعیین مؤثرترین و تأثیرپذیرترین معیار
۴. استفاده در شرایط عدم قطعیت و شبیه‌سازی شرایط واقعی حاکم بر جامعه هدف

با توجه به ویژگی‌های گفته‌شده در بالا، نقشه شناختی فازی در شبیه‌سازی، مدل‌سازی راهبردهای سازمانی، حمایت از تدوین مسائل راهبردی و تجزیه‌وتحلیل تصمیمات، ایجاد پایگاه‌های دانش، تشخیص مسائل مدیریتی، تجزیه‌وتحلیل حالات شکست، مشخصات و الزامات سامانه‌ها، پشتیبانی از طراحی شهری، مدیریت روابط در خدمات شرکت‌های هواپیمایی و تقویت بهره‌برداری از شبکه به‌کاربرده می‌شود. همچنین از FCM برای تشخیص خطا، تصمیم‌گیری، مدیریت کسب‌وکار، تجزیه و تحلیل صنعتی و سامانه‌های کنترل علوم اجتماعی و سیاسی، مهندسی فناوری اطلاعات، رباتیک، سامانه‌های خبره، پزشکی، آموزش و پروش، فرآیندهای پیش‌بینی، مباحث زیست‌محیطی و ... استفاده می‌شود.

برای انجام روش FCM باید گام‌های زیر به ترتیب انجام شود.

۱. مقایسه اهمیت عوامل برای استخراج وزن محلی[1] با استفاده از روش مقادیر ویژه. توضیح اینکه ازجمله روش‌های محاسبه وزن بدون داشتن ماتریس تصمیم، می‌توان روش مقادیر ویژه را نام برد. در این روش می‌توان با کمک ماتریس مقایسات زوجی که حاصل از پرسشنامه AHP است، وزن تمامی معیارها را به‌دست آورد. کافی است که ابتدا مقدار λ_{max} را با استفاده از دترمینان رابطه (۱) محاسبه شود.

$$(A - \lambda_{max} * I) \qquad (۱)$$

سپس حاصل را در ماتریس رابطه (۱) جاگذاری کرده و ماتریس به‌دست‌آمده را در بردار وزنی مربوط به معیارها (W) ضرب و برابر صفر قرار دهیم. رابطه (۲)

$$(A - \lambda_{max} * I) * W = 0 \qquad (۲)$$

۲. به دست آوردن ماتریس مجاورت[2] یا همبستگی و ترسیم نقشه شناختی فازی (FCM) برای نمایش وزن رابطه علت و معلولی میان معیارها و زیرمعیارها از نظر خبرگان.

ماتریس مجاورت حاصل نظر متخصصین و پاسخ‌های آنان به پرسشنامه FCM است، بنابراین با توجه به تعدد پاسخ‌های به‌دست‌آمده از پرسشنامه‌ها برای هر معیار، لازم است که از تمامی نظرات مربوط به پرسشنامه‌ها طبق رابطه (۳) میانگین حسابی گرفته شود (برای هر درایه) و حاصل آن در قالب یک عدد واحد و به‌عنوان درایه‌های ماتریس مجاورت نرمال‌شده قرار داده شود.

$$a_{ij} = \frac{1}{H}\sum_{K=1}^{H} x_{ij}^{k} \qquad (۳)$$

که در آن، H تعداد متخصصان یا خبره‌ها است.

۳. محاسبه ماتریس حالت پایدار (C^*) با استفاده از رابطه (۴).

$$A_i^{(t+1)} = f\left(A_i^t + \sum_{\substack{j=1 \\ j\neq i}}^{n} W_{ji}A_j^t\right) \qquad (۴)$$

باید توجه داشت که $A^0 = I_{n*n}$ یعنی مقدار اولیه ماتریس A برابر است با یک ماتریس همانی به ابعاد n*n که در این ماتریس n تعداد معیارهای به‌کار رفته در مسئله است. همچنین در این رابطه $f(x)$ را تابع آستانه گویند. با توجه به ماهیت مسئله از توابع آستانه مختلفی همچون تابع آستانه خطی دوگانه، تابع آستانه خطی سه‌گانه و تابع تانژانت هایپربولیک استفاده می‌شود [۱۳]. در این تحقیق از تابع آستانه لجستیکی استفاده می‌شود که رابطه آن به‌صورت زیر است:

$$f(x) = \frac{1}{(1+e^{-x})} \qquad (۵)$$

با قرار دادن ماتریس حالت اولیه در رابطه (۴) ماتریس A^1 (ماتریس حالت در سطح ۱) به‌دست خواهد آمد. این مقدار به‌عنوان ورودی دیگری برای این رابطه محسوب می‌شود و این روند به همین شکل ادامه خواهد داشت تا جایی که $A^{t+1} - A^t \leq 0.0001$ و یا مجموعه‌ای از ماتریس‌های حالت به‌صورت دوره‌ای تکرار شوند.

1- Local weight

2- Steady state matrix

محاسبه ماتریس حالت پایدار نرمال با استفاده از رابطه (۶) است. در این رابطه K بزرگ‌ترین مجموع سطر ماتریس حالت پایدار می‌باشد.

$$C_n^* = \frac{C^*}{K} \quad (۶)$$

با توجه به ماتریس حالت پایدار نرمال شده و همچنین وزن‌هایی که در مرحله نخست این روش برای هرکدام از تهدیدات به‌دست‌آمده می‌توان اقدام به محاسبه وزن نهایی نمود؛ بنابراین، در گام آخر با در اختیار داشتن وزن هرکدام از معیارها که به روش مقادیر ویژه به‌دست‌آمده است، تک‌تک معیارها، از تأثیرگذارترین معیار تا تأثیرپذیرترین معیار، به‌وسیله رابطه (۷) رتبه‌بندی خواهد شد. در این رابطه L_n وزن محلی نرمال شده است.

$$G = L_n + C_n^* * L_n \quad (۷)$$

۴- یافته‌ها

شش تهدید اساسی شناسایی‌شده بر اساس روش فریدمن عبارت‌اند از:

- نقض حق مالکیت (PR)
- جاسوسی سایبری (CE)
- عدم آگاهی ذی‌نفعان (SA)
- عدم تخصیص بودجه مناسب برای مقابله با تهدیدات سایبری (BA)
- عدم استفاده از سامانه‌های رمزگذاری و احراز هویت مناسب (AE)
- عدم درک این‌که فرآیند امنیت اطلاعات یک موضوع تجاری است؛ نه یک موضوع فنی (BP)

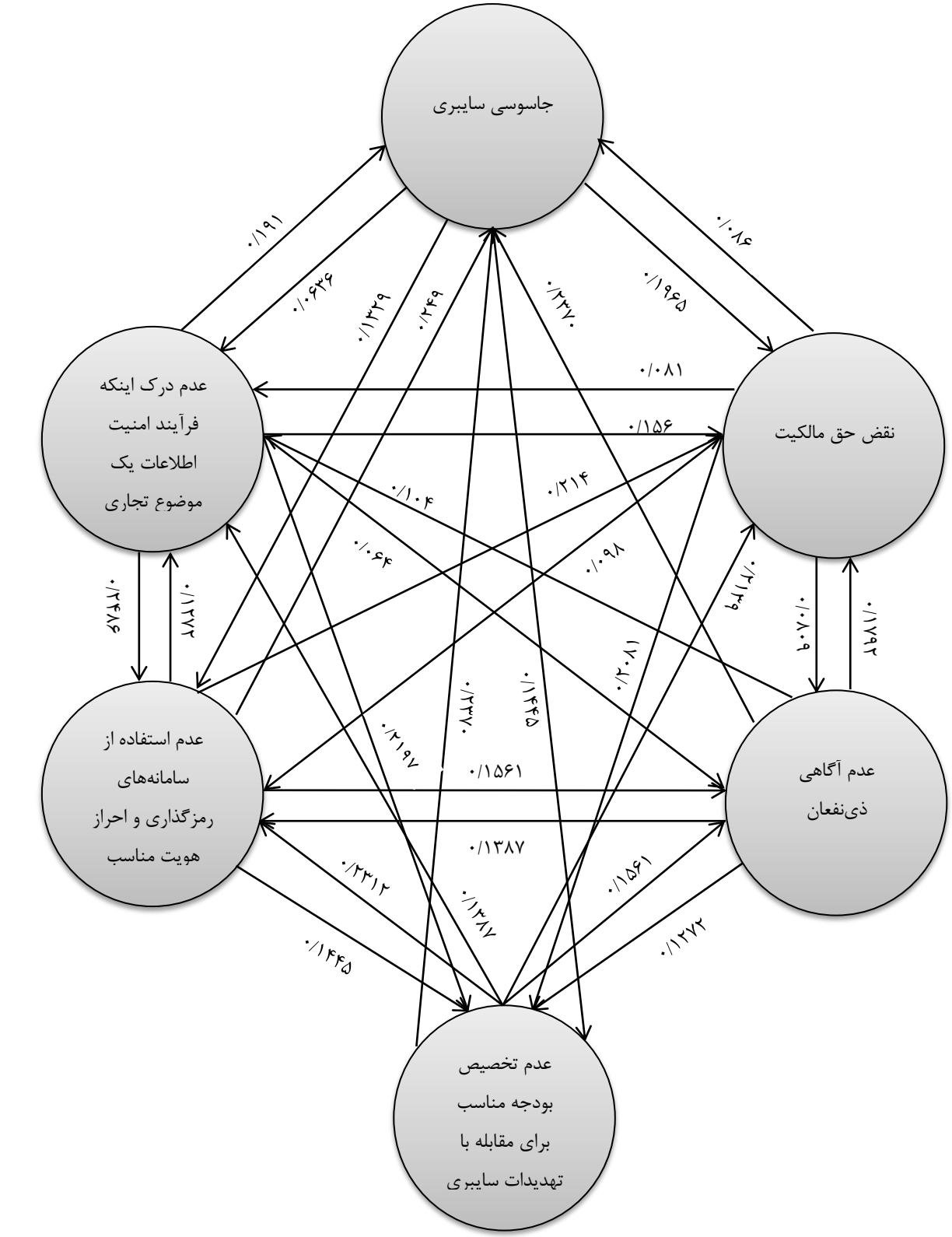
ماتریس مجاورت در جدول (۴) نمایش داده شده است. با در اختیار داشتن ماتریس مجاورت گراف علت و معلولی نقشه شناختی فازی مطابق شکل (۱) رسم می‌شود. در این شکل به هرکدام از کمان‌ها، کمان وزن‌دار و به عددی که در بالای آن درج شده است نیروی رابطه علت و معلولی بین دو گره می‌گویند که از نظر متخصصین حاصل شده است. در تحلیل میزان اثرگذاری و اثرپذیری معیارها می‌توان به‌عنوان نمونه تهدید نقض حق مالکیت را در نظر گرفت که همان‌طور که در شکل (۱) مشخص است از پنج تهدید دیگر پنج کمان به این تهدید وارد شده است که وزن هرکدام از این تهدیدات متفاوت است به‌عنوان‌مثال از تهدید جاسوسی سایبری کمانی با وزن ۰/۱۹۶۵ به این تهدید وارد می‌شود که این نشانه تأثیرگذاری جاسوسی سایبری بر نقض حق مالکیت به این میزان است که این وزن ناشی از میانگین حسابی گرفته‌شده از امتیازات فازی ۱۰ خبره مورد پرسش قرار گرفته است. این مقدار وزنی در سطر دوم ستون اول ماتریس مجاورت (جدول ۵) مشخص است. همچنین با داشتن ماتریس مجاورت، می‌توان اقدام به محاسبه ماتریس حالت پایدار (جدول ۶) نمود.

جدول (۵): ماتریس مجاورت

معیار i \ معیار j	PR	CE	SA	BA	AE	BP
PR	۰	۰/۰۸۶۷	۰/۰۸۰۹	۰/۰۶۹۴	۰/۰۹۸۳	۰/۰۸۰۹
CE	۰/۱۹۶۵	۰	۰	۰/۱۴۴۵	۰/۱۳۲۹	۰/۰۶۳۶
SA	۰/۱۷۹۲	۰/۲۳۷۰	۰	۰/۱۲۷۲	۰/۱۳۸۷	۰/۱۰۴۰
BA	۰/۲۰۸۱	۰/۲۳۷۰	۰/۱۵۶۱	۰	۰/۲۳۱۲	۰/۱۳۸۷
AE	۰/۲۱۳۹	۰/۲۴۸۶	۰/۱۵۶۱	۰/۱۴۴۵	۰	۰/۱۲۷۲
BP	۰/۱۵۶۱	۰/۱۹۰۸	۰/۰۶۳۶	۰/۲۴۸۶	۰/۲۱۹۷	۰

جدول (۶): ماتریس حالت پایدار

معیار i \ معیار j	PR	CE	SA	BA	AE	BP
PR	۰/۸۳۰۴	۰/۸۳۵۲	۰/۷۵۴۲	۰/۷۹۹۱	۰/۸۱۱۸	۰/۷۶۴۴
CE	۰/۸۳۰۴	۰/۸۳۵۲	۰/۷۵۴۲	۰/۷۹۹۱	۰/۸۱۱۸	۰/۷۶۴۴
SA	۰/۸۳۰۴	۰/۸۳۵۲	۰/۷۵۴۲	۰/۷۹۹۱	۰/۸۱۱۸	۰/۷۶۴۴
BA	۰/۸۳۰۴	۰/۸۳۵۲	۰/۷۵۴۲	۰/۷۹۹۱	۰/۸۱۱۸	۰/۷۶۴۴
AE	۰/۸۳۰۴	۰/۸۳۵۲	۰/۷۵۴۲	۰/۷۹۹۱	۰/۸۱۱۸	۰/۷۶۴۴
BP	۰/۸۳۰۴	۰/۸۳۵۲	۰/۷۵۴۲	۰/۷۹۹۱	۰/۸۱۱۸	۰/۷۶۴۴



شکل (۱): گراف علت و معلولی عوامل با استفاده از FCM

پس از به‌دست آوردن ماتریس حالت پایدار (C^*) که در این مسئله ماتریس حالت پایدار بعد از حدوداً هشت تکرار به‌دست آمده است، با استفاده از رابطه (۳) تبدیل به ماتریس حالت پایدار نرمال مطابق جدول (۷) می‌شود. همان‌طور که در بخش روش‌شناسی ذکر شد، در این تحقیق از تابع آستانه غیرخطی لجستیکی استفاده شده است. درواقع هنگامی از این تابع استفاده خواهد شد که ارزش و مقادیر به‌دست‌آمده در بازه [۱ و ۰] قرار داشته باشد.

جدول (۷): ماتریس حالت پایدار نرمال شده

معیار j / معیار i	PR	CE	SA	BA	AE	BP
PR	۰/۱۷۳۲	۰/۱۷۴۲	۰/۱۵۷۳	۰/۱۶۶۶	۰/۱۶۹۳	۰/۱۵۹۴
CE	۰/۱۷۳۲	۰/۱۷۴۲	۰/۱۵۷۳	۰/۱۶۶۶	۰/۱۶۹۳	۰/۱۵۹۴
SA	۰/۱۷۳۲	۰/۱۷۴۲	۰/۱۵۷۳	۰/۱۶۶۶	۰/۱۶۹۳	۰/۱۵۹۴
BA	۰/۱۷۳۲	۰/۱۷۴۲	۰/۱۵۷۳	۰/۱۶۶۶	۰/۱۶۹۳	۰/۱۵۹۴
AE	۰/۱۷۳۲	۰/۱۷۴۲	۰/۱۵۷۳	۰/۱۶۶۶	۰/۱۶۹۳	۰/۱۵۹۴
BP	۰/۱۷۳۲	۰/۱۷۴۲	۰/۱۵۷۳	۰/۱۶۶۶	۰/۱۶۹۳	۰/۱۵۹۴

وزن‌های به‌دست‌آمده به کمک پرسشنامه AHP و روش مقادیر ویژه به‌صورت زیر به‌دست آمده است:

$(W_1,W_2,W_3,W_4,W_5,W_6) =$

(۰/۲۰۵۱ و ۰/۲۹۹۴ و ۰/۱۶۷۴ و ۰/۱۸۷۸ و ۰/۰۵۷۴ و ۰/۰۸۳)

همچنین با توجه به رابطه (۵) مقادیر به‌دست‌آمده به‌صورت زیر خواهد بود:

$(G_1,G_2,G_3,G_4,G_5,G_6) =$

(۰/۳۷۰۳ و ۰/۴۶۴۶ و ۰/۳۳۲۶ و ۰/۳۵۲۹ و ۰/۲۲۲۵ و ۰/۲۴۸۲)

۵-نتیجه‌گیری

در این پژوهش ابتدا به‌وسیله سه رویکرد مرور ادبیات، پرسش از متخصصین حوزه پروژه‌های فناوری اطلاعات و تجزیه‌وتحلیل نظرات، شش تهدید مهم و تأثیرگذار در امنیت این پروژه‌ها شناسایی و مشخص شد. سپس به‌وسیله دو پرسشنامه AHP و FCM نظرات متخصصین در رابطه بااهمیت و تأثیرگذاری هر یک از این تهدیدات نسبت به یکدیگر استخراج گردید و نمودار روابط علت و معلولی این تهدیدات رسم شد. جهت تشخیص تأثیرگذارترین تهدید، میزان تأثیر هر یک از تهدیدها بر یکدیگر توسط ماتریس حالت پایدار مشخص گردید و در گام آخر با به‌دست آوردن وزن هر یک از این تأثیرات در قالب ماتریس G تمامی تهدیدات از تأثیرگذارترین تا تأثیرپذیرترین تهدید مشخص شدند.

بر اساس نتایج پژوهش، ترتیب تهدیدات سایبری در پروژه‌های فناوری اطلاعات جهت شناسایی تأثیرگذارترین تهدید و اقدام مدیران پروژه برای پیشگیری از وقوع آن به‌صورت زیر خواهد بود:

۱. عدم استفاده از سامانه‌های رمزگذاری و احراز هویت مناسب
۲. عدم درک این‌که فرآیند امنیت اطلاعات یک موضوع تجاری است نه یک موضوع فنی
۳. عدم آگاهی ذی‌نفعان
۴. عدم تخصیص بودجه مناسب برای مقابله با تهدیدات سایبری
۵. نقض حق مالکیت
۶. جاسوسی سایبری

معیارها به ترتیب تأثیرگذارترین تهدید (۱) تا تأثیرپذیرترین تهدید (۶) نوشته شده است.

در صورت توجه و برنامه‌ریزی صحیح، متناسب با معیارهای به‌دست‌آمده، مدیران پروژه می‌توانند پروژه‌های فناوری اطلاعات تحت اختیار خود را از گزند آسیب‌ها و تهدیدات سایبری حفظ نموده و امکان شکست پروژه خود را به حداقل رسانده و راه را برای رسیدن سازمان به اهداف و راهبردهایش هموار نمایند. این نتیجه بیانگر این مطلب است که عدم استفاده از سامانه‌های رمزگذاری و احراز هویت، مؤثرترین تهدید بین تهدیدات سایبری است و لذا رفع این تهدید می‌تواند تأثیر بسزایی در کاهش احتمال وقوع سایر تهدیدهای شناسایی‌شده داشته باشد. درنتیجه جهت مقابله با این تهدید، با توجه به این‌که در پروژه‌های فناوری اطلاعات حتی فرآیندهای آموزش و پشتیبانی از سامانه راه‌اندازی شده، پس از پایان مرحله پیاده‌سازی نیز درون فرآیند پروژه تعریف می‌شود، عدم رعایت مسائل امنیتی و عدم استفاده از سامانه‌های رمزگذاری توسط کاربر نهایی می‌تواند کارایی کل پروژه را زیر سؤال برده و عواقب آن گریبان‌گیر سازمان انجام‌دهنده پروژه

خواهد شد. در جهت رفع این مشکل می‌توان با تقویت آموزش کاربران در حفظ مسائل امنیتی و ارتقاء آگاهی آنان از طریق شناساندن خطرات موجود در این زمینه از وقوع خطرات احتمالی خودداری کرد. همچنین می‌توان با تعبیه سامانه‌های امنیتی قدرتمند و کارآمد احتمال وقوع حملات سایبری را به حداقل رساند.

نکته‌ای که در اینجا حائز اهمیت است و از مزایای مهم روش FCM نیز محسوب می‌شود این موضوع است که به تمامی معیارهای موجود در این مسئله در قالب یک سامانه نگاه می‌شود. بدین‌صورت که روابط این تهدیدات در این مسئله منحصراً متقابل و بدون در نظر گرفتن سایر تهدیدات در نظر گرفته نمی‌شود و با همین ویژگی مثبت این روش است که می‌توان به تهدیدی دست‌یافت که با تمرکز بر روی آن زمینه بروز و رشد سایر تهدیدات را کاملاً و یا تا حد زیادی از بین برد. در این پژوهش نیز تهدید "عدم استفاده از سامانه‌های رمزگذاری و احراز هویت مناسب" مؤثرترین تهدید در میان سایر تهدیدات سایبری در پروژه‌های فناوری اطلاعات شناخته شده است که بر این اساس اگر به‌عنوان نمونه بخواهد مورد تجزیه‌وتحلیل قرار گیرد می‌توان آن را با تهدید مؤثر دوم (عدم درک این‌که فرآیند امنیت اطلاعات یک موضوع تجاری ست نه یک موضوع فنی) مقایسه نمود که طبق نظر متخصصین بیش از دو برابر معیار مؤثر اول بر روی آن تأثیرگذار است (شکل ۱) اما اگر این روابط در حضور سایر تهدیدات مورد ارزیابی قرار گیرد، نتیجه متفاوت خواهد شد که این حاصل از همان دید جامعی ست که روش FCM در تحلیل سامانه‌ها به تحلیل‌گر می‌دهد.

برای تحقیقات آتی پیشنهاد می‌شود تمامی اقدامات عملی مقابله با این ریسک‌ها و راه‌کارهایی که در این حوزه می‌تواند یاری‌دهنده مدیران پروژه باشد را شناسایی و به کمک روش‌های تصمیم‌گیری چندمعیاره بهترین راهکارها را جهت اجرا انتخاب کرد. در این راستا می‌توان با مشخص کردن معیارهایی برای تعیین بهترین راه‌کار همچون تخصیص کمترین بودجه ممکن، قابلیت اجرایی، منحصربه‌فرد بودن، قابلیت اطمینان و ...، با استفاده از روش‌هایی همچون Fuzzy Topsis این راه‌کارها را رتبه‌بندی نمود. همچنین می‌توان با استفاده از مبانی تصمیم‌گیری چندهدفه، مدلی را با اهداف سطح سامانه امنیتی و هزینه‌های مربوط به پیاده‌سازی و اجرا آن تعریف کرد که هم‌زمان و با ارتقاء سطح سامانه‌های امنیتی و احراز هویت در یک واحد انجام‌دهنده پروژه‌های فناوری اطلاعات، هزینه‌های مربوط به ارتقاء سامانه‌های امنیتی کاهش یابد.

۶- منابع

[1] T. Chen, J. Zhang, and K.-K. Lai, "An integrated real options evaluating model for information technology projects under multiple risks," International Journal of Project Management, vol. 27, no. 8, pp. 776-786, 2009.

[2] M. Rahmani, F. Faghihi, and B. Mozafari, "Control Strategy to Maintain Stability of Micro-grids, During Occurring Cyber Attacks on the Power Grid," Journal of Electronical & Cyber Defence, vol. 5, no. 2, pp. 47-58, 2017.

[3] L. Kirichenko, T. Radivilova, and Anders Carlsson, "Detecting cyber threats through social network analysis: short survey," Socio Economic Challenges, vol. 1, no. 1, pp. 1-15, 2017.

[4] N. Fardad, S. Soleymani, and F. Faghihi, "Evaluation of Attack and Defense Budget for Cyber Security of High Voltage Substations Based on Application Classification Via Fuzzy AHP Method," Journal of Electronical & Cyber Defence, vol. 6, no. 1, pp. 95-108, 2017.

[5] A. Baykasoglu and Z. D. U. Durmusoglu, "A hybrid MCDM for private primary school assessment using DEMATEL based on ANP and fuzzy cognitive map," International Journal of Computational Intelligence Systems, pp. 615-635, 2014.

[6] D. Baccarini, G. Salm, and P. E. D. Love, "Management of risks in information technology projects," Industrial Management & Data Systems, vol. 104, no. 4, pp. 286-295, 2004.

[7] B W. Boehm, "Software risk management: principles and practices," IEEE Software, vol. 8, no. 1, pp. 32-41, 1991.

[8] H. Barki, S. Rivard, and J. Talbot, "Toward an Assessment of Software Development Risk," Journal of Management Information Systems, vol. 10, no. 2, pp. 203-225, 2015.

[9] L. Wallace, M. Keil, and A. Rai, "Understanding software project risk: a cluster analysis," Information & Management, vol. 42, no. 1, pp. 115-125, 2004.

[10] R. T. Nakatsu and C. L. Iacovou, "A comparative study of important risk factors involved in offshore and domestic outsourcing of software development projects: A two-panel Delphi study," Information & Management, vol. 46, no. 1, pp. 57-68, 2009.

[11] C. R. Boddy, "Sample size for qualitative research," Qualitative Market Research: An international journal, pp. 426-432, 2016.

[12] A. Ghasemzadeh and M. Gayoori Sales, "Model of Fuzzy Evaluation of the Effectiveness of the Distributed Denial of Service Attacks, Based on Open Source," Journal of Electronical & Cyber Defence, vol. 5, no. 1, pp. 85-98, 2017.

[13] B. Kosko, "Fuzzy cognitive maps," International Journal of Man-Machine Studies, vol. 24, no. 1, pp. 65-75, 1986.

[14] E. I. Papageorgiou, C. Stylios, and P. P. Groumpos, "Active Hebbian learning algorithm to train fuzzy cognitive maps," International Journal of Approximate Reasoning, vol. 37, no. 3, pp. 219-249, 2004.

[15] K. Schwalbe, "Information Technology Project Management," 6th ed. Boston, United States: Course Technology Press, 2010.

[16] A. M. Khalfan, "Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors," International Journal of Information Management, vol. 24, no. 1, pp. 29-42, 2004.

[17] S. Liu and L. Wang, "Understanding the impact of risks on performance in internal and outsourced information technology projects: The role of strategic importance," International Journal of Project Management, vol. 32, no. 8, pp. 1494-1510, 2014.

[18] B. Von Solms and R. Von Solms, "The 10 deadly sins of information security management," Computers & Security, vol. 23, no. 5, pp. 371-376, 2004.

[19] E. Kutsch and M. Hall, "The rational choice of not applying project risk management in information technology projects," Project Management Journal, vol. 40, no. 3, pp. 72-81, 2009.

[20] F. Okumus, A. Bilgihan, A.t B. Ozturk, and X. (Roy) Zhao, "Identifying and overcoming barriers to deployment of information technology projects in hotels," Journal of Organizational Change Management, vol. 30, no. 5, pp. 744-766, 2017.

[21] D. V. Chulkov and M. S. Desai, "Information technology project failures: Applying the bandit problem to evaluate managerial decision making," Information Management & Computer Security, vol. 13, no. 2, pp. 135-143, 2005.

[22] M. Pruitt, "Security Best Practices for IT Project Managers," SANS Institute, pp. 1-28, 2013.

[23] A. Alami, "Why Do Information Technology Projects Fail?," Procedia Computer Science, vol. 100, pp. 62-71, 2016.

[24] M. A. Terlizzi, F. de Souza Meirelles, and H. R. Oliveira Cesar de Moraes, "Barriers to the use of an IT Project Management Methodology in a large financial institution," International Journal of Project Management, vol. 34, no. 3, pp. 467-479, 2016.

[25] M. Keil, A. Rai, and S. Liu, "How user risk and requirements risk moderate," European Journal of Information Systems, vol. 22, no. 6, pp. 650-672, 2013.

[26] M. Meingast, T. Roosta, and S. Sastry, "Security and Privacy Issues with Health Care Information Technology," in Engineering in Medicine and Biology Society, New York, pp. 5453-5458, 2006.

[27] M. E. Whitman and H. J. Mattord, "Principles of Information Security," 4th ed. Kennesaw: Course Technology, 2012.

[28] S. Sakthivel, "Managing risk in offshore systems development," Communications of the ACM, vol. 50, no. 4, pp. 69-75, 2007.

[29] P. Kumar Dey and J. Kinch, "Risk management in information technology projects," International Journal of Risk Assessment and Management, vol. 9, no. 3, pp. 311-329, 2008.

[30] B. Javani, P. Mutajwaa, and D. Rwelamila, "Risk management in IT projects – a case of the South African public sector," International Journal of Managing Projects in Business, vol. 9, no. 2, pp. 389-413, 2016.

[31] M. H. A. Tafti, "Risks factors associated with offshore IT outsourcing," Industrial Management & Data Systems, vol. 105, no. 5, pp. 549-560, 2005.

[32] H. Taylor, "Critical risks in outsourced IT projects: the intractable and the unforeseen," Communications of the ACM - Entertainment networking, vol. 49, no. 11, pp. 74-79, 2006.

[33] F. Freitas Silveira, R. de F. S. Macri Russo, I. G. Júnior, and R. Sbragia, "Systematic review of risks in domestic and global IT projects," Journal of Global Information Management, vol. 26, no. 1, pp. 20-40, 2018.

[34] H. Samadi, S. Nazari-Shirkouhi, and A. Keramati, "Identifying and Analyzing Risks and Responses for Risk Management in Information Technology Outsourcing Projects Under Fuzzy Environment," International Journal of Information Technology & Decision Making, vol. 13, no. 6, pp. 1283-1323, 2014.

[35] A. Rodriguez, F. Ortega, and R. Concepcion, "A method for the evaluation of risk in IT projects," Expert Systems with Applications, vol. 45, pp. 273-285, 2016.

[36] R. Aron, E. K. Clemons, and S. Reddi, "Just Right Outsourcing: Understanding and Managing Risk," Journal of Management Information Systems, vol. 22, no. 2, pp. 37-55, 2005.

[37] R. Gonzalez, J. Gasco, and J. Llopis, "Information systems outsourcing risks: a study of large firms," Industrial Management & Data Systems, vol. 105, no. 1, pp. 45-62, 2005.

[38] G. Ahn, M. Kwon, C. Kang, and S. Hur, "Probabilistic Graphical Framework for Predicting Software Project Risk," Industrial Engineering and Management Systems, vol. 17, no. 1, pp. 120-127, 2018.

[39] S. Yuwei, "Today's Solution and Tomorrow's Problem: The Business Process Outsourcing Risk Management Puzzle," California Management Review, vol. 60, no. 1, pp. 27-44, 2007.

[40] S. Dhar and B. Balakrishnan, "Risks, benefits, and challenges in global IT outsourcing:Perspectives and Practices," Journal of Global Information Management, vol. 14, no. 3, pp. 39-69, 2006.

[41] C. Kahraman and S. Cevik Onar, "Intelligent Techniques in Engineering Management," 1st ed. Cengiz Kahraman and Sezi Cevik Onar, Eds. Cham Switzerland: Springer International Publishing, 2015.

[42] A. Rodríguez, F. Ortega, and R. Concepción, "An intuitionistic method for the selection of a risk management approach to information technology projects," Information Sciences, vol. 375, pp. 202-218, 2017.

[43] E. Luiijf, "Understanding Cyber Threats and Vulnerabilities," in Introduction to Critical Information Infrastructure Protection, Javier Lopez, Roberto Setola, and Stephen D. Wolthusen, Eds. Berlin, Heidelberg: Springer, ch. 4, pp. 52-67, 2012.

Journal of Electronical & Cyber Defence
Vol. 7, No. 2, 2019, Serial No. 26

Effects of Cyber Threats in IT Projects Using the Fuzzy Cognitive Mapping Approach

H. Amin-Tahmasbi*, M. Hemmati Asiabaraki

*Department of Industrial Engineering, Faculty of Technology and Engineering, East of Guilan, University of Guilan

(Received: 01/05/2018, Accepted: 13/10/2018)

ABSTRACT

Mismatches in time and cost are among the most important reasons for the failure of information technology projects. But it should be borne in mind that neglecting security issues, especially in projects with the nature of working with data and information, can cause irreparable damage to the project organization. Meanwhile, recognizing the factors that can threaten an IT project in cyberspace, and the impact of each of these factors on the other has great importance. In fact, the project manager can be more effective in preventing these threats by knowing the impact of the criteria. In this research, the main factors that could threaten an IT project in cyberspace are identified. At the next step, some of these threats are eliminated by Friedman test and the 6 threats which remain are more important than others, in expert's opinion. Then their weights are calculated by Analytic Hierarchy Process (AHP) approach and eventually their effects on each other are determined by using the Fuzzy Cognitive Mapping (FCM) method. The results show that, lack of appropriate encryption and authentication systems is the most effective, and cyber espionage is the most influenced of these threats.

Keywords: Information Technology Project, Cyber Space, Fuzzy Cognitive Map, Cyber Threats

* Corresponding Author Email: amintahmasbi@guilan.ac.ir