Archive of SID

بهبود رتبه‌بندی مخاطرات امنیت اطّلاعات با استفاده از مدل‌های تصمیم‌گیری چندشاخصه

حسین قرایی[1] و مهسا آقا محی‌الدین[2]
[1]مرکز تحقیقات مخابرات، تهران، ایران
[2]دانشگاه تهران، پردیس بین الملل کیش، کیش، ایران

چکیده

یکی از مهم‌ترین قابلیت‌های سامانهٔ مدیریت امنیت اطلاعات که در هر سازمانی به فراخور نیاز باید انجام شود، مدیریت مخاطرات امنیت اطلاعات است. اهمیت به‌کارگیری مدیریت مخاطرات امنیت اطلاعات تا جایی است که می‌توان آن را قلب سامانهٔ مدیریت امنیت اطلاعات نامید و رتبه‌بندی مخاطرات امنیت اطلاعات، قسمت مهم و کلیدی مرحلهٔ ارزیابی مخاطرات در فرایند این مدیریت به شمار می‌رود. در این مقاله روشی کاربردی براساس تلفیق دو روش تصمیم‌گیری چندشاخصهٔ فرایند تحلیل سلسله‌مراتبی و تاپسیس، در محیط فازی، برای بهبود رتبه‌بندی مخاطرات امنیت اطلاعات ارائه شده است. نتایج حاصل از پیاده‌سازی مدل تلفیقی فرایند تحلیل سلسله‌مراتبی فازی-تاپسیس (FAHP-TOPSIS) در مقایسه با مدل فرایند تحلیل سلسله‌مراتبی فازی (FAHP) نشان می‌دهد که وزن‌های حاصل از مدل پیشنهادی FAHP-TOPSIS دارای ضریب تغییرات کمتر و میانگین بیشتر نسبت به مدل FAHP است و درنتیجه نتایج دقیق تر و با درصد خطای کمتری را جهت رتبه‌بندی مخاطرات ارائه می‌دهد.

واژگان کلیدی: مدیریت مخاطرات، امنیت اطلاعات، روش‌های تصمیم‌گیری چندشاخصه، روش فرایند تحلیل سلسله‌مراتبی، روش تاپسیس.

۱-مقدّمه

امروزه سازمان‌ها و دارایی‌های آنها در محیطی پر از چالش و تحول قرار گرفته‌اند. در میان دارایی‌های سازمانی، اطلاعات به‌عنوان یک دارایی مهم و با ارزش برای هر سازمان به حساب می‌آیند؛ لذا جهت حفظ اطلاعات و مدیریت آنها و جلوگیری از هرگونه سوء استفاده باید براساس آخرین دستاوردهای روز دنیا و استانداردهای مربوطه اقدام کرد. سامانهٔ مدیریت امنیت اطلاعات به مدیران این امکان را می‌دهد تا بتوانند امنیت سامانه‌ها و اطلاعات خود را با به حداقل رساندن مخاطرات امنیتی و تجاری کنترل کنند. یکی از مهم‌ترین قابلیت‌های سامانهٔ مدیریت امنیت اطلاعات که در هر سازمانی به فراخور نیاز باید انجام شود، مدیریت مخاطرات است (Almunawa, 2011). مدیریت مخاطرات، فرآیند تشخیص و ارزیابی احتمال تاثیر مخاطرات تبیین شده می باشد (Talabis, 2013) و رتبه بندی مخاطرات، قسمت مهم و کلیدی از فاز ارزیابی مخاطرات در فرایند این مدیریت است. در خصوص مدیریت مخاطرات امنیت اطلاعات در حال حاضر استاندارد ها و متدلوژی هایی در دنیا وجود دارد، من جمله OCTAVE, COBRA, ISO27005 و .... که تنها به بیان قوائد کلی و راهنمایی‌هایی[1] جهت ارزیابی مخاطرات امنیت اطلاعات می پردازند و در خصوص جزئیات پیاده سازی، اطلاعاتی را مطرح نمی نمایند (Shamely, 2010).

همچنین در رتبه‌بندی و ارزیابی مخاطرات، توجه به این نکته ضروری است که مخاطرات را نمی‌توان تنها با توجه به یک بعد خاص از ابعاد، آثار و علل مخاطرات تجزیه و تحلیل کرد؛ بلکه مخاطرات دارای ابعاد و اثرات مختلفی، با

[1] Guidelines

www.SID.ir

Archive of SID

قابلیت رخداد در سطوح مختلف هستند و اقدامات پیش‌گیرانهٔ خاص خود را در هر سطح می‌طلبند؛ لذا در این مقاله، روشی کاربردی و کمی، براساس مدل‌های تصمیم‌گیری چندشاخصه برای رتبه‌بندی مخاطرات امنیت اطلاعات ارائه شده است.

علاوه‌بر این، برای رفع مشکلات مربوط به عدم قطعیت همراه با قضاوت‌های خبرگان که در ذات تصمیمات انسانی نهفته است، روش‌های تحلیلی مورد نظر، براساس منطق فازی و در ترکیب با این منطق ارایه شده است.

در این مقاله، ابتدا مخاطرات امنیت اطاعات شناسایی‌شده در یک سازمان، به کمک روش تصمیم‌گیری چندشاخصه فرایند تحلیل سلسله‌مراتبی فازی[1] رتبه‌بندی شده‌اند و پس از آن به‌منظور ایجاد بهبود در رتبه‌بندی انجام شده و به‌دست آوردن نتایج دقیق‌تر، از روش تاپسیس در ترکیب با روش فرایند تحلیل سلسله‌مراتبی فازی استفاده شده است.

این مقاله مشتمل‌بر شش بخش است. ابتدا تحقیقات مشابه انجام‌گرفته برای ارزیابی و رتبه‌بندی مخاطرات امنیت اطلاعات در بخش دوم بیان می‌شوند. در بخش سوم نحوهٔ پیاده‌سازی روش فرایند تحلیل سلسله‌مراتبی فازی و تاپسیس ارائه می‌شود. مدل پیشنهادی در بخش چهارم و نتایج حاصل از آن به‌همراه نتایج حاصل از پیاده‌سازی روش فرایند تحلیل سلسله‌مراتبی فازی و مقایسهٔ نتایج دو روش در بخش پنجم و درنهایت نتیجه‌گیری کلی در بخش ششم بیان می‌شود.

۲- تحقیقات مشابه انجام گرفته

تحقیقات مشابه انجام‌گرفته را می‌توان در سه بخش ارزیابی مخاطرات امنیت اطلاعات، ارزیابی مخاطرات با استفاده از مدل‌های تصمیم‌گیری چندشاخصه و ارزیابی مخاطرات امنیت اطلاعات با استفاده از مدل‌های تصمیم‌گیری چندشاخصه دسته‌بندی کرد.

۲-۱- ارزیابی مخاطرات امنیت اطلاعات

ژیوی و *ژونگیوان* در سال ۲۰۱۲ مدلی را جهت بهبود ارزیابی مخاطرات امنیت سامانه‌های اطلاعاتی براساس رویکردی فرآیندی ارائه کردند (Zhiwe,2012).

هانگوی و یانلینگ در سال ۲۰۱۰ از ترکیب تئوری RBF شبکه عصبی و روش ارزیابی فازی بهینه سازی ازدحام ذرات برای ارزیابی مخاطرات امنیت اطلاعات استفاده کردند (Honghui,2010).

اکلهارت و همکاران در سال ۲۰۰۹ شیوه ای برای مدیریت مخاطرات امنیت اطلاعات ارائه کرده‌اند که استاندارد NIST SP800-30 را به طور کامل پوشش می‌دهد. (Ekelhaet, 2009).

بوجانک و بلاژیک در سال ۲۰۰۸ از طریق مدل سازی اقتصادی به تحلیل و رتبه بندی مخاطرات امنیت اطلاعات پرداختند (Bojank, 2008).

۲-۲- ارزیابی مخاطرات با استفاده از مدل‌های تصمیم‌گیری چندشاخصه

ستوده گوهر و همکاران در سال ۲۰۱۱ به ارزیابی مخاطرات پروژه‌های ساختمانی بر اساس مدل فازی سلسله مراتبی پرداخته‌اند (Sotoude, 2011).

وانگ و الاگ در سال ۲۰۰۶ روش تاپسیس را برای ارزیابی مخاطرات در پل‌ها به کار گرفته اند(Wang, 2006).

جوزی و *صفاریان* در سال ۱۳۹۰ به اولویت‌بندی مخاطرات و آثار ناشی از آن در نیروگاه گازی آبادان به کمک روش تاپسیس پرداختند (جوزی و صفاریان، ۱۳۹۰).

جبل‌عاملی و همکاران در سال ۱۳۸۶ پژوهشی را به‌عنوان رتبه‌بندی مخاطرات پروژه با استفاده از فرآیند تصمیم‌گیری چندشاخصه تاپسیس انجام دادند (جبل‌عاملی و همکاران، ۱۳۸۶).

۲-۳- ارزیابی مخاطرات امنیت اطلاعات با استفاده از مدل‌های تصمیم‌گیری چندشاخصه

چنگ هانگ و *چن* در سال ۲۰۰۹ با استفاده از روش تاپسیس و تئوری فازی به سنجش و رتبه بندی مخاطرات امنیت اطلاعات پرداخته اند(Hung, 2009).

سموجور در سال ۲۰۱۱ مدلی برای انتخاب بهینه روش مدیریت مخاطرات امنیت اطلاعات بر اساس فرآیند تحلیل سلسله مراتبی ارائه داد (Smojver,2011).

وانگ و زنگ در سال ۲۰۱۰ نتایج تحقیقات فرایند تحلیل سلسله مراتبی، ریاضیات فازی و روش شبکه عصبی مصنوعی را برای ارزیابی مخاطرات امنیت اطلاعات ادغام نمودند (Wang & Zeng, 2010).

[1]Fuzzy Analytic Hierarchy Process (FAHP)

www.SID.ir

Archive of SID

شاملی سندی و همکاران در سال ۲۰۱۰ به ارزیابی مخاطرات امنیت اطلاعات با استفاده از ترکیب استاندارد ایزو ۲۷۰۰۱، روش‌های تاپسیس فازی و سیستم‌های خبره پرداخته‌اند (Shamely, 2010) و در سال ۲۰۱۲ مدلی عملی برای کسب ارزیابی مخاطرات امنیت اطلاعات بر اساس مدل‌های تاپسیس و روش جمع وزنی ساده[1] و با استفاده از منطق فازی ارائه نمودند (Shamely, 2012).

۳- مدل‌های تصمیم‌گیری چندشاخصه[2]

مدل های تصمیم گیری چند شاخصه یک سری از تکنیک‌هاست که اجازه می دهد طیفی از شاخصهای وابسته به یک مبحث، امتیازدهی و وزن‌دهی شده و سپس رتبه‌بندی شوند (Meer, 2012). روش تصمیم‌گیری چند شاخصه، چارچوبی برای ارزیابی مسائل چند بعدی، متناقض و ناسازگار است (Jolai) و پتانسیل زیادی را به منظور کاهش دادن هزینه و زمان و بالا بردن دقت در تصمیم‌گیری ها دارا می باشد و می تواند چارچوب مناسبی را برای بهبود مدیریت مخاطرات امنیت اطلاعات فراهم آورد (Meer, 2012). دو دسته کلی از روش‌های مختلف برای حل مسائل تصمیم‌گیری چند شاخصه عبارتند از:

- روش‌های منشعب از مدل غیرجبرانی[3]
- روش‌های منشعب از مدل جبرانی[4]

مدل غیر جبرانی شامل روش‌هایی است که در آنها مبادلهٔ بین شاخص‌ها مجاز نیست؛ یعنی نقطه‌ضعف موجود در یک شاخص توسط مزیت موجود از شاخص دیگر، جبران نمی شود. مزیت روش‌های متعلق به این مدل نیز سادگی آنهاست که با رفتار تصمیم‌گیرنده و محدودبودن اطلاعات او مطابقت دارد. در برخی از این روش‌ها ممکن است حتی نیازی به کسب اطلاعات از تصمیم‌گیرنده نباشد.

در مقابل، مدل جبرانی مشتمل بر روش‌هایی است که اجازهٔ مبادله در بین شاخص‌ها در آنها مجاز است. یعنی به‌طور مثال تغییری (حتی کوچک) در یک شاخص می‌تواند توسط تغییری مخالف در شاخص (یا شاخص‌های) دیگر جبران شود.

براساس تعاریف بالا نمی‌توان از روش‌های غیرجبرانی برای مسأله رتبه‌بندی مخاطرات استفاده کرد. زیرا همان‌طور که اشاره شد در این روش‌ها نباید مبادله‌ای بین شاخص‌ها وجود داشته باشد، درحالی‌که در مسأله رتبه‌بندی مخاطرات، شاخص‌های مختلف از قبیل احتمال وقوع و تأثیر بر یکدیگر تأثیر داشته و ضعف یک شاخص می‌تواند توسط مزیت شاخص دیگر جبران شود. بنابراین از روش‌های غیر جبرانی در مسألهٔ رتبه‌بندی مخاطرات استفاده نشده است. از مهم‌ترین روش‌های جبرانی می‌توان به موارد زیر اشاره کرد:

- **روش مجموع وزین ساده[5]**

در این روش با مفروض‌بودن بردار W (وزن شاخص‌ها) مناسب ترین گزینه (A^*) محاسبه می شود. با توجه به این‌که در مسأله رتبه‌بندی مخاطرات به دنبال بهترین گزینه نیستیم و هدف اولویت‌بندی گزینه‌هاست، این روش نمی‌تواند روش مفیدی باشد.

- **روش ویکور[6]**

تکنیک ویکور یکی از تکنیک های تصمیم‌گیری چندشاخصه است که به‌منظور یافتن بهترین گزینه براساس میزان سازش میان فاصلهٔ گزینه‌ها نسبت به بهترین گزینه استفاده می شود. بنابراین درصورتی‌که هدف مسأله، یافتن گزینهٔ بهینه باشد، می‌توان از روش ویکور استفاده کرد.

- **روش الکتر[7]**

در این روش به‌جای رتبه بندی گزینه ها از مفهوم جدیدی معروف به مفهوم «غیر رتبه‌ای» استفاده می‌شود. بدین صورت که به‌عنوان مثال $A_k \rightarrow A_l$ بیان‌گر آن است که اگر چه گزینه های k و l هیچ ارجحیتی از نظر ریاضی به یکدیگر ندارند، اما تصمیم گیرنده و تحلیل گر، مخاطرهٔ بهتربودن A_k را بر A_l می‌پذیرند. در این روش کلیهٔ گزینه‌ها با استفاده از مقایسات غیر رتبه‌ای مورد ارزیابی قرار گرفته و بدان طریق گزینه‌های غیر مؤثر حذف می‌شوند. این روش تنها به یافتن بهترین گزینه می‌پردازد.

- **روش مجموع وزین و رده‌بندی‌شده[8]**

این روش در مسائلی کاربرد دارد که عوامل و زیرفاکتورهای مؤثر در تصمیم‌گیری به‌صورت رده‌ای و در سطوح مختلف نشان داده شده‌اند؛ به‌طوری‌که هر سطح شامل زیرفاکتورهای

[1] SAW
[2] Multi Criteria Decision Making (MCDM)
[3] Non-compensatory Model
[4] Compensatory Model
[5] Simple- Additive- weighting method (SAW)
[6] VIKOR
[7] Elimination et choice Translating reality (ELECTRE)
[8] Hierarchical additive weighting method

www.SID.ir

Archive of SID

متأثر از متغیر یا متغیرهای موجود در سطح بلافاصله ماقبل است. ارزش هر سطح نیز باید برابر ارزش متغیرهای سطح بلافاصله پایین آن باشد. از این رو، روش مجموع وزین و رده‌بندی‌شده نیز قابل استفاده در مسألهٔ رتبه‌بندی مخاطرات نیست؛ زیرا در مورد مخاطرات به‌عنوان گزینه‌های مسأله نمی‌توان شاخص‌ها را به‌صورت لایه‌ای درنظر گرفت.

- **روش مجموع ساده وزین با تعامل متقابل**[1]

این روش برای برآورد w_j های مناسب از رتبه‌بندی گزینه‌ها به شرط وجود یک تابع مطلوبیت خطی (اما نامشخص) استفاده می‌کند. الگوریتم حل این روش از سایر روش‌ها پیچیده‌تر بوده و از طرفی مشخص نیست که آیا تابع مطلوبیت در مسألهٔ رتبه‌بندی مخاطرات خطی است یا نه! بنابراین از این روش نیز برای حل مسألهٔ مورد نظر استفاده نشده است.

- **روش لین مپ**[2]

در این روش m گزینه و n شاخص از یک مسألهٔ مفروض به‌صورت m نقطه در یک فضای nبعدی درنظر گرفته شده و سپس نقطهٔ ایدآل تشخیص داده شده و گزینه‌ای که دارای کمترین فاصله از ایدآل باشد، انتخاب می شود. در این روش هیچ فرض محدودکننده‌ای که به‌واسطهٔ آن نتوان از این روش در مسألهٔ رتبه‌بندی مخاطرات استفاده کرد، وجود ندارد؛ ولی شاید لزوم انجام مقایسات زوجی بین گزینه‌ها (مخاطرات) استفاده از این روش را در مسألهٔ مورد نظر با مشکل مواجه سازد. اعتبار راه حل به‌دست آمده با داشتن تعداد مقایسات زوجی بیشتر، بالا خواهد رفت.

- **روش فرایند تحلیل سلسله‌مراتبی فازی**[3]

یکی از پرکاربردترین و در عین حال مناسب‌ترین روش‌های تصمیم‌گیری چندشاخصه، روش فرآیند تحلیل سلسله‌مراتبی است. به زبان ساده اگر ساختار مسأله شامل سطوح مختلفی از شاخص‌های ارزیابی و به شکل سلسله‌مراتبی باشد و بخواهیم اهمیت تجمیعی و نهایی گزینه‌ها را با توجه به هر شاخص یا زیرشاخص بسنجیم و به اولویت‌بندی آنها بپردازیم، روش فرآیند تحلیل سلسله‌مراتبی مناسب‌ترین روش تحلیل مسأله است.

- **روش تاپسیس**[4]

در استفاده از این روش توجه به نکات زیر ضروری است:

- مطلوب‌بودن هر شاخص باید به‌طور یکنواخت افزایشی (یا کاهشی) باشد (هرچه r_{ij} بیشتر، مطلوبیت بیشتر و یا برعکس). یعنی بهترین ارزش موجود از یک شاخص نشان‌دهندهٔ ایده‌آل مثبت آن بوده و بدترین ارزش موجود از آن، مشخص‌کننده ایده آل منفی برای آن خواهد بود.

- فاصله یک گزینه از ایده‌آل مثبت (یا از ایده‌آل منفی) ممکن است به‌صورت فاصلهٔ اقلیدسی (از توان دوم) و یا به‌صورت مجموع قدر مطلق از فواصل خطی (معروف به فواصل بلوکی) محاسبه شود، که این امر بستگی به نرخ تبادل و جایگزینی در بین شاخص‌ها دارد.

با توجه به اینکه در مسألهٔ رتبه‌بندی مخاطرات، دو فرضیهٔ بالا در روش تاپسیس نقض نمی‌شوند و همچنین به علت سادگی استفاده از این روش و روش فرایند تحلیل سلسله‌مراتبی فازی و اعتبار و دقت داده‌های حاصل از این روش‌ها، الگوریتم استفاده از آنها در ادامه ارائه شده و روش پیشنهاد شده در این مقاله براساس دو مدل فرآیند تحلیل سلسله‌مراتبی فازی و تاپسیس است.

۳-۱- تکنیک فرآیند تحلیل سلسله‌مراتبی فازی

قدم های لازم برای انجام رتبه بندی مخاطرات امنیت اطلاعات بر اساس روش تحلیل سلسله مراتبی فازی در ادامه آمده است. مهم ترین قابلیت مجموعه های فازی توانایی آنها در نشان دادن داده‌های مبهم و نا مشخص است (Hangjun, 2011).

گام اول: به‌دست‌آوردن ساختار سلسله‌مراتبی از شاخص‌ها و زیرشاخص‌های مؤثر در مسأله.

گام دوم: جمع‌آوری نظرات خبرگان در قالب اعداد فازی و تشکیل جداول مقایسه زوجی فازی. مقیاس مورد استفاده این مقاله، مقیاس فازی مثلثی[5] نه‌تایی است که توسط *تسفاماریام* و *صدیق* در سال ۲۰۰۶ براساس مقیاس ساعتی پیشنهاد شده است است (Tesfamariam, 2006).

هر عددی فازی مثلثی دارای تابع عضویتی مطابق آنچه در رابطه (۱) آمده است می باشد(Tesfamariam, 20

[1] Interactive simple average weighting method
[2] Linear Programing for Multidimensional analysis of preferences
[3] Fazzy Analytical Hierarchy Process (FAHP)
[4] Technique for Order Performance by Similarity to Ideal Solution (TOPSIS)
[5] Triangular Fuzzy Number

www.SID.ir

Archive of SID

$$U(x)=\begin{cases}\frac{x-l}{m-l} & ;l\le x\le m\\ 1 & \\ \frac{u-x}{u-m} & ;m\le x\le u\\ 1 & \\ 0 & ;Otherwise\end{cases} \qquad (۱)$$

جدول ۱-۳ اعداد فازی متناظر با متغیرهای زبانی(Tesfamariam, 2006)

متغیر زبانی	عدد فازی	مقیاس عددی مربوطه
یکسان	$\tilde{1}$	(۱،۱،۱)
بینابین	$\tilde{2}$	(۱،۲،۳)
اندکی مهم‌تر	$\tilde{3}$	(۲،۴،۳)
بینابین	$\tilde{4}$	(۳،۵،۴)
مهم‌تر	$\tilde{5}$	(۶،۵،۴)
بینابین	$\tilde{6}$	(۷،۶،۵)
بسیار مهم‌تر	$\tilde{7}$	(۸،۷،۶)
بینابین	$\tilde{8}$	(۷،۹،۳)
اکیدا مهم‌تر	$\tilde{9}$	(۹،۹،۸)

گام سوم: محاسبهٔ ماتریس تجمیع نظرات خبرگان. در این مقاله از روش محاسبه میانگین هندسی نظرات افراد مطابق با رابطهٔ (۲) برای به‌دست‌آوردن ترکیب نظرات افراد و به‌دست آوردن جداول نهایی مقایسه‌های زوجی استفاده شده است.

$$a^*_{ij}=\sqrt[k]{\left(a^{*1}_{ij}\times a^{*2}_{ij}\times\ldots\times a^{*k}_{ij}\right)} \qquad (۲)$$

گام چهارم: محاسبه و بررسی نرخ سازگاری[1] . چنانچه $C.R$ به‌دست آمده با استفاده از فرمول‌های (۳) و (۴) کمتر از ۰/۱ به‌دست آید، جداول مقایسات زوجی سازگار هستند (Wang, 2006; Kordi, 2008).

$$C.I=(\lambda_{max}-n)/(n-1) \qquad (۳)$$

$$C.R=(C.I)/(R.I) \qquad (۴)$$

جدول ۲-۳ مقادیر شاخص تصادفی $R.I$ به ازای ابعاد ماتریس تصمیم گیری(n)(Kordi, 2008)

n	۳	۴	۵	۶	۷	۸	۹
$R.I$	۰/۵۸	۰/۹۰	۱/۱۲	۱/۲۴	۱/۳۲	۱/۴۱	۱/۴۵

n	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵
$R.I$	۱/۴۹	۱/۵۱	۱/۴۸	۱/۵۶	۱/۵۷	۱/۵۹

[1]Consistency Rate

گام پنجم: محاسبه ماتریس قطعی تجمیع نظرات خبرگان با استفاده از روش CFCS. اگر $\tilde{A}_{ij}^{\,k}=(l_{ij}^k,m_{ij}^k,u_{ij}^k)$ ماتریس مقایسه زوجی kامین فرد خبره از مقایسه زوجی بین معیار i و معیار j باشد در این‌صورت گام‌های روش CFCS به شکل زیر است (Opricovic, 2003)

۱ – محاسبهٔ ماتریس نرمال‌شده

$$xl_{ij}^k=\left(l_{ij}^k-\min l_{ij}^k\right)/\Delta_{min}^{max} \qquad (۵)$$

$$xm_{ij}^k=\left(m_{ij}^k-\min l_{ij}^k\right)/\Delta_{min}^{max} \qquad (۶)$$

$$xu_{ij}^k=\left(u_{ij}^k-\min l_{ij}^k\right)/\Delta_{min}^{max} \qquad (۷)$$

$$\Delta_{min}^{max}=\max u_{ij}^k-\min l_{ij}^k \qquad (۸)$$

۲- محاسبهٔ مقادیر نرمال‌شدهٔ چپ (ls) وراست (us)

$$xls_{ij}^k=xm_{ij}^k/\left(1+xm_{ij}^k-xl_{ij}^k\right) \qquad (۹)$$

$$xus_{ij}^k=xu_{ij}^k/\left(1+xu_{ij}^k-xm_{ij}^k\right) \qquad (۱۰)$$

۳- محاسبهٔ مقدار قطعی نهایی نرمال‌شدهٔ

$$x_{ij}^k=\frac{\left[xls_{ij}^k\left(1-xls_{ij}^k\right)+xus_{ij}^k\right]}{\left[1-xls_{ij}^k+xus_{ij}^k\right]} \qquad (۱۱)$$

۴- محاسبهٔ مقادیر قطعی

$$a^{*k}_{ij}=\min l_{ij}^k+x_{ij}^k\Delta_{min}^{max} \qquad (۱۲)$$

گام ششم: محاسبهٔ اوزان نهایی. درنهایت برای به‌دست‌آوردن اوزان، از روش میانگین‌گیری هندسی بردار سطری ماتریس تصمیم‌گیری قطعی ترکیب نظرات افراد، که توسط ساعتی (۱۹۸۰) معرفی شده است، مطابق رابطهٔ (۱۳) استفاده می‌شود (Saaty, 2000) .

$$W_i=\frac{\left(\prod_{j=1}^{n}a^*_{ij}\right)^{1/n}}{\sum_{i=1}^{n}\left(\prod_{j=1}^{n}a^*_{ij}\right)^{1/n}} \qquad i,j=1,2,\ldots,n \qquad (۱۳)$$

۳-۲- تکنیک تاپسیس

روش تاپسیس، اولین بار توسط هوانگ و یون[2] در سال ۱۹۸۱ ارائه شد (Wang, 2006 ; Lin, 2005). در این روش بهترین گزینه، گزینه ایست که نزدیکترین فاصله را به حل ایده آل مثبت و در عین حال دورترین فاصله را از حل ایده ال منفی داشته باشد (Hosseinzadeh Lotfi, 2006). ورودی‌ها و داده‌های این روش همانند روش فرایند تحلیل سلسله‌مراتبی فازی، براساس نظر خبرگان است. در این روش خبرگان ابتدا اهمیت نسبی شاخص‌ها یا زیرشاخص‌ها را

[2]Hwang and Yoon

www.SID.ir

Archive of SID

مشخص کرده و سپس عملکرد هر گزینه را نیز نسبت به هر شاخص می‌سنجند. روش تاپسیس، ماتریس تصمیمی را ارزیابی می‌کند که شامل m آلترناتیو و n مشخصه است. الگوریتم استفاده از روش تاپسیس براساس مراحل زیر است:

گام اول: تبدیل ماتریس تصمیم‌گیری موجود به یک ماتریس بدون مقیاس. هر درآیه r_{ij} از ماتریس تصمیم نرمالیزشده از رابطهٔ زیر محاسبه می‌شود (Hosseinzadeh Lotfi, 2006):

$$r_{ij}=\frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \qquad \begin{matrix} i=1,2,\dots,m; \\ j=1,2,\dots,n \end{matrix} \qquad (۱۴)$$

گام دوم: ایجاد ماتریس تصمیم نرمالیزشده وزندار V با مفروض‌بودن بردار W به‌عنوان ورودی الگوریتم (Zakarevicius, 2006).

$$W=(w_1,w_2,\dots,w_n)$$

$$v_{ij}=w_j\times r_{ij} \qquad \begin{matrix} i=1,2,\dots,m; \\ j=1,2,\dots,n \end{matrix} \qquad (۱۵)$$

گام سوم: تعیین راه حل ایده‌آل مثبت و راه ایده‌آل منفی. دو آلترناتیو مجازی A^+ و A^- را به‌صورت زیر تعریف می کنیم (Zakarevicius, 2006):

آلترناتیو ایده‌آل مثبت (۱۶)

$$A^+ = \left\{\left(\max_i v_{ij} \middle| j\in J\right), \left(\min_i v_{ij} \middle| j\in J'\right) \middle| i=1,2,\dots,m\right\} = \left\{v_1^+, v_2^+, \dots, v_j^+, \dots, v_n^+\right\}$$

آلترناتیو ایده‌آل منفی (۱۷)

$$A^- = \left\{\left(\min_i v_{ij} \middle| j\in J\right), \left(\max_i v_{ij} \middle| j\in J'\right) \middle| i=1,2,\dots,m\right\} = \left\{v_1^-, v_2^-, \dots, v_j^-, \dots, v_n^-\right\}$$

$$J=\{j=1,2,\dots,n\} \middle| j\in \text{Benefit}$$
$$J'=\{j=1,2,\dots,n\} \middle| j\in \text{Cost}$$

دو آلترناتیو مجازی ایجادشده به‌ترتیب برترین آلترناتیو و کم‌اثرترین آلترناتیو (حل ایده‌آل منفی) هستند.

گام چهارم: محاسبهٔ اندازهٔ فاصله (جدایی). فاصلهٔ آلترناتیو iام از ایده آل مثبت با فرمول زیر به‌دست می آید (Haghighirad, 2009):

$$s_i^+ = \sqrt{\sum_{j=1}^{n}(v_{ij}-v_j^+)^2} \qquad (۱۸)$$

$$;\ i=1,2,\dots,m$$

به‌طور مشابه فاصله آلترناتیو iام از حل ایده‌آل منفی به‌صورت زیر محاسبه می‌شود:

$$s_i^- = \sqrt{\sum_{j=1}^{n}(v_{ij}-v_j^-)^2} \qquad (۱۹)$$
$$;\ i=1,2,\dots,m$$

گام پنجم : محاسبهٔ ضرایب نزدیکی (نزدیکی A_i نسبت به A^+). این نزدیکی به‌صورت زیر تعریف می‌شود (Zakarevicius, 2006):

$$C_i^+ = \frac{s_i^-}{s_i^+ + s_i^-} \qquad ;\ i=1,2,\dots,m \qquad (۲۰)$$

$$;\ 0<C_i^+<1$$

ملاحظه می‌شود که اگر $A_i=A^+$ آنگاه $C_i^+=1$ و اگر $A_i=A^-$ آنگاه $C_i^+=0$ خواهد شد. بنابراین هر اندازه فاصلهٔ آلترناتیو A_i از حل ایده‌آل A^+ نزدیکتر باشد C_i^+ به واحد نزدیک‌تر خواهد بود.

گام ششم: رتبه‌بندی گزینه‌ها. براساس ترتیب نزولی C_i^+ها می‌توان گزینه‌های موجود از مسأله را به‌صورت کاهشی رتبه‌بندی کنیم (Zakarevicius, 2006).

۴- مدل پیشنهادی

همان‌طور که پیش‌تر ذکر شد، هدف از این مقاله، ارائهٔ راه‌کاری جهت بهبود رتبه‌بندی مخاطرات امنیت اطلاعات با استفاده از مدل‌های تصمیم‌گیری چندشاخصهٔ فرایند تحلیل سلسله‌مراتبی فازی و تاپسیس است؛ به‌گونه‌ای که با ترکیب این دو مدل و رفع معایب و قوت‌بخشیدن به مزایای آنها، روشی کاربردی و بهینه ارائه شود.

استفاده از مدل فرایند تحلیل سلسله‌مراتبی در کنار تمام مزایایی که نسبت به سایر مدل‌های تصمیم‌گیری چندشاخصه دارد، چالش‌های خاص خود را نیز دارد که در ذات انجام مقایسات زوجی نهفته است. بدین معنی که با زیادشدن تعداد شاخص‌ها و زیرشاخص‌ها، درعمل انجام مقایسات زوجی به‌شدت دشوار می‌شود و نمی‌توان به نتایج مطلوب و دقیق رسید (Wang & Zeng, 2010). برای حل این مشکل، در مدل پیشنهادی به دنبال ارائهٔ راه‌حلی جهت به‌حداقل‌رساندن انجام مقایسات زوجی و درنتیجه حصول

www.SID.ir

Archive of SID

نتایج مطلوب‌تر و دقیق‌تر و درنهایت بهبود رتبه‌بندی مخاطرات امنیت اطلاعات می‌باشیم. روش پیشنهاد شده در این مقاله برای کاهش انجام مقایسات زوجی، استفاده از مدل فرایند تحلیل سلسله‌مراتبی فازی در ترکیب با روش تاپسیس است.

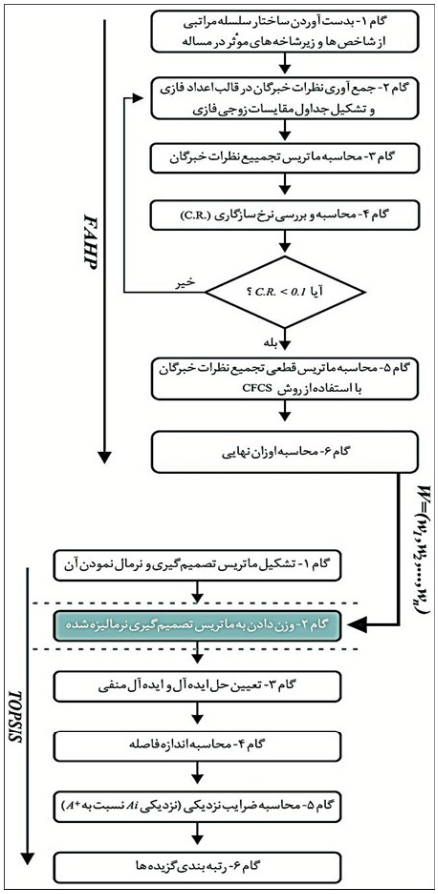
ساختار سلسله‌مراتبی در مدل پیشنهادی در سه سطح مخاطرات (سطح اول)، اثر مخاطرات (سطح دوم) و علل بروز مخاطرات (سطح سوم) درنظر گرفته شده است و روش کار به این صورت که در ابتدا وزن شاخص‌ها و زیرشاخص‌ها تا سطح دوم سلسله‌مراتب، یعنی وزن مخاطرات و اثر مخاطرات، با استفاده از روش فرایند تحلیل سلسله‌مراتبی فازی محاسبه می‌شود و پس از آن برای محاسبه وزن زیرشاخص، زیرشاخص‌ها در سطح سوم سلسله‌مراتب یعنی علل بروز مخاطرات، به جای ادامه کار با روش فرایند تحلیل سلسله‌مراتبی فازی از روش تاپسیس استفاده می‌شود.

در روش تاپسیس، ورودی‌ها به دو دسته تقسیم می‌شوند. دستهٔ اول، وزن یا اهمیت شاخص‌های ارزیابی گزینه‌ها (W) و دسته دوم، اطلاعات عملکرد گزینه ها با توجه به هر شاخص (r_{ij}) (Haghighirad, 2009). در روش پیشنهادی، وزن یا اهمیت شاخص‌های ارزیابی گزینه‌ها یعنی همان وزن‌های سطح دوم ساختار سلسله‌مراتب، از خروجی فرایند تحلیل سلسله‌مراتبی فازی و اطلاعات عملکرد هر گزینه، بر اساس نظر خبرگان و به کمک نتایج به‌دست آمده از پرسش‌نامهٔ طراحی‌شده براساس مدل تاپسیس به‌دست می‌آید.

نحوهٔ استفاده از این داده‌ها در روش تاپسیس به این صورت است که در گام اول برای به‌دست آوردن اطلاعات عملکرد هر گزینه و تشکیل ماتریس تصمیم‌گیری نرمالیزشده از داده‌های به‌دست آمده از نظر خبرگان به کمک پرسش‌نامهٔ طراحی‌شده براساس مدل تاپسیس استفاده می‌شود و در گام دوم یعنی در گام وزن‌دادن به ماتریس تصمیم‌گیری نرمالیزه‌شده، مجموعه وزن‌های $W=(w_1,w_2,...,w_n)$ که در آن $\sum_{j=1}^{n} w_j = 1$ است، از محاسبات فرایند تحلیل سلسله‌مراتبی فازی به‌دست می‌آید و به این ترتیب در این گام از روش تاپسیس، با ضرب ستون jام ماتریس تصمیم‌گیری نرمالیزشده در وزن مربوطه W_j حاصل از فرایند تحلیل سلسله‌مراتبی فازی، ماتریس تصمیم نرمالیزشده وزن‌دار V حاصل می‌شود. این اوزان نرمال‌شده v_{ij} از رابطه (۱۵) محاسبه می‌شود:

$$W = (w_1, w_2, \dots, w_n)$$
$$v_{ij} = w_j \times r_{ij} \quad \begin{matrix} i=1,2,\dots,m; \\ j=1,2,\dots,n \end{matrix} \qquad (۱۵)$$

$$v = \begin{array}{c} \\ A_1 \\ \vdots \\ A_i \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{matrix} X_1 & \dots & X_j & \dots & X_n \end{matrix} \\ \begin{bmatrix} v_{11} & \dots & v_{1j} & \dots & v_{1n} \\ \vdots & & \vdots & & \vdots \\ v_{i1} & \dots & v_{ij} & \dots & v_{in} \\ \vdots & & \vdots & & \vdots \\ v_{m1} & \dots & v_{mj} & \dots & v_{mn} \end{bmatrix} \end{array}$$



شکل۱-۴: گام‌های پیاده‌سازی روش‌های پیشنهادی

و پس از آن گام‌های بعدی پیاده‌سازی روش تاپسیس تا رسیدن به اوزان نهایی سطوح سوم (علل بروز مخاطرات) انجام می‌شود. گام‌های انجام کار در مدل پیشنهادی در شکل ۱-۴ نشان داده شده است.

www.SID.ir

Archive of SID

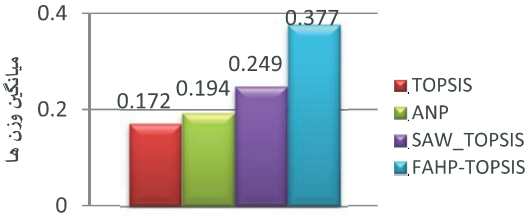
۵-نتایج پیاده‌سازی مدل پیشنهادی

در این تحقیق شاخص‌ها و زیرشاخص‌های مؤثر بر مسأله علل بروز مخاطرات امنیت اطلاعات در سه سطح سلسله‌مراتب و در قالب ۱۰ شاخص اصلی (مخاطرات)، ۳۴ زیرشاخص (اثرات مخاطرات و بعضاً مشترک) و ۵۸ زیرشاخص زیر شاخص‌ها (علل بروز مخاطرات و بعضاً مشترک) از نظرات خبرگان آگاه در این مسأله به‌دست آمده است (جدول ۱-۵).

نتایج محاسبهٔ اوزان علل مخاطرات شناسایی‌شده با استفاده از روش فرایند تحلیل سلسله‌مراتبی فازی (FAHP) و مدل پیشنهادی (FAHP-TOPSIS) جهت رتبه‌بندی، در جدول ۲-۵ به صورت خلاصه آورده شده است.

براساس نتایج تحلیلی آزمون تی نمونه‌های مستقل جهت بررسی تفاوت بین دو روش FAHP و FAHP-TOPSIS، با توجه به مقدار سطح معنی‌داری، که از مقدار ۰/۰۵ کمتر است (جدول ۳-۵)، نتیجه‌گیری می‌شود که اختلاف معنی‌داری بین دو روش فرایند تحلیل سلسله‌مراتبی فازی و مدل پیشنهادی FAHP-TOPSIS وجود دارد. از آنجا که میانگین اوزان به‌دست آمده با روش پیشنهادی FAHP-TOPSIS، ۹۲٪ بیشتر از میانگین اوزان به‌دست آمده با روش فرایند تحلیل سلسله‌مراتبی فازی است، می‌توان نتیجه گرفت که روش پیشنهادی FAHP-TOPSIS نتایج دقیق‌تر و قابل قبول‌تری نسبت به روش فرایند تحلیل سلسله‌مراتبی فازی برای رتبه‌بندی مخاطرات ارائه می‌دهد. همچنین نتایج توصیفی آزمون تی نمونه‌های مستقل، جهت مقایسه و بررسی تفاوت بین دو روش فرایند تحلیل سلسله‌مراتبی فازی و مدل پیشنهادی FAHP-TOPSIS، نشان می‌دهد که مدل پیشنهادی دارای ضریب تغییرات کمتری نسبت به مدل فرایند تحلیل سلسله‌مراتبی فازی است. مقدار کمتر ضریب تغییرات در روش پیشنهادی FAHP-TOPSIS به‌معنای درصد خطای کمتر این روش است. نتایج توصیفی آزمون تی نمونه‌های مستقل در جدول ۴-۵ ارائه شده است.

میانگین وزن‌های حاصل از پیاده‌سازی مدل پیشنهادی در مقایسه با وزن‌های حاصل از مدل‌های ارائه‌شده در سایر مقالات در نمودار ۱-۵ نشان داده شده است. (Shameli, 2012 ; Yu-Ping, 2013). در مقالات مختف به‌منظور بهبود مدل‌هایی مانند تاپسیس، AHP،ANP و ...، استفاده از این مدل‌ها در ترکیب با مدل‌های دیگر پیشنهاد شده است. مانند ترکیب مدل تاپسیس با مدل SAW و یا ANP با دیمتل. در این مقاله همان‌طور که پیش‌تر ذکر شد، استفاده از AHP در ترکیب با تئوری فازی و تاپسیس پیشنهاد شده است. همان‌طور که در نمودار ۱-۵ مشاهده می‌شود، مدل پیشنهادی دارای بیش‌ترین میانگین وزن نسبت به مدل های ارائه شده در سایر مقالات است که این امر منجر به بهبود رتبه‌بندی مخاطرات خواهد شد.



نمودار ۱-۵ : نمودار میله‌ای مقایسه نتایج حاصل از مدل پیشنهادی و نتایج مدل‌های ارائه‌شده در سایر مقالات

۶- نتیجه‌گیری

در این مقاله سعی شده است تا راه‌کار جدیدی جهت بهبود رتبه‌بندی مخاطرات امنیت اطلاعات ارائه شود. در این راستا و به‌منظور ارائه مدل مناسب، در این مقاله توجه به این نکته حائز اهمیت بوده است که مخاطرات را نمی‌توان تنها با توجه به یک بعد خاص از ابعاد، آثار و علل مخاطرات تجزیه و تحلیل کرد؛ بلکه مخاطرات دارای ابعاد و اثرات مختلفی، با قابلیت رخداد در سطوح مختلف هستند و اقدامات پیشگیرانهٔ خاص خود را در هر سطح می‌طلبند. لذا در این مقاله، روشی کاربردی، براساس تلفیق دو روش تصمیم‌گیری چندشاخصه فرایند تحلیل سلسله‌مراتبی فازی و تاپسیس، برای رتبه‌بندی مخاطرات امنیت اطلاعات ارائه شده است و علل بروز هر مخاطره با درنظر گرفتن وزن آن مخاطره و اثر آن مخاطره رتبه‌بندی شده‌اند. مقایسه نتایج حاصل از پیاده‌سازی مدل پیشنهادی فرایند تحلیل سلسله‌مراتبی فازی- تاپسیس و مدل فرایند تحلیل سلسله‌مراتبی فازی نشان می‌دهد که مدل پیشنهادی فرایند تحلیل سلسله‌مراتبی فازی- تاپسیس، نتایج دقیق‌تر و با درصد خطای کمتری را ارائه می‌دهد. مزیت‌های مدل پیشنهادی را می‌توان به‌صورت زیر خلاصه کرد:

- وزن نهایی مخاطرات در مدل پیشنهادی شامل وزن هر سه سطح اول، دوم و سوم است.
- با افزایش وزن مخاطرات در مدل پیشنهادی، جواب دقیق‌تری درخصوص اولویت‌بندی حاصل می‌شود.

www.SID.ir

Archive of SID

- یک روش تصمیم‌گیری قوی و تکنیکی برای اولویت‌بندی براساس نزدیکی به جواب ایده‌آل است.
- نتایج عینی‌تر در تجزیه و تحلیل و رتبه‌بندی مخاطرات ارائه می‌کند.
- از عوامل بیشتر و اهمیت متفاوت بین عوامل اثرگذار بهره‌مند است.
- عوامل کمی و کیفی را در تجزیه و تحلیل‌ها شامل می‌شود.
- استفاده از ابزارهایی برای افزایش دقت و کیفیت اولویت‌بندی مخاطرات ارائه می‌کند.
- روش پیشنهادی ساده و انعطاف‌پذیر است و هر تعداد معیار می‌تواند در حل یک مسأله به‌کار گرفته شود. اگر چه لازم به ذکر است با افزایش تعداد معیارها، تصمیم‌گیران ممکن است با دشواری‌هایی در وزن‌دادن به این معیارها روبه‌رو شوند.

جدول۱-۵: سه سطح سلسله‌مراتب مسألهٔ رتبه‌بندی علل بروز مخاطرات

سطح اول (مخاطرات)	سطح دوم (اثر مخاطرات)	سطح سوم (علل بروز مخاطرات)
آتش‌سوزی (C1)	از بین رفتن اطلاعات (C11)	• نبود سامانهٔ اطفای حریق (C45) • نبود سامانهٔ تهویه مناسب (C46) • عدم رعایت اصول امنیت نواحی امن (C47) • عدم استقرار مناسب و حفاظت تجهیزات (C48) • حصار امنیت فیزیکی (C459) • عدم وجود امکانات پشتیبانی (C50)
خرابکاری و دستکاری (C2)	• از بین رفتن اطلاعات (C12) • دزدی اطلاعات (C13) • قطع دسترسی اطلاعات (C14) • از بین بردن یکپارچگی اطلاعات (C15) • متوقف کردن عملیات کاری (C16) • از بین بردن اعتبار شرکت (C17)	• نداشتن توافق‌نامه‌های محرمانگی (C51) • نداشتن توافق‌نامه‌های عدم افشاء (C52) • عدم وجود کنترل و حذف حقوق دسترسی (C53) • عدم رعایت خروج دارایی اطلاعاتی (C54) • عدم سیستم مانیتورینگ و کنترل‌های شبکه (C55) • عدم کنترل‌های رمزنگاری (C56)
زلزله (C3)	از بین رفتن اطلاعات (C18)	• حصار امنیت فیزیکی (C57) • عدم رعایت اصول امنیت نواحی امن (C58) • عدم کار در مناطق امن (C59) • عدم استقرار مناسب و حفاظت تجهیزات (C60) • عدم وجود امکانات پشتیبانی (C61)
سیل (C4)	از بین رفتن اطلاعات (C19)	• حصار امنیت فیزیکی (C62) • عدم رعایت اصول امنیت نواحی امن (C63) • عدم کار در مناطق امن (C64) • عدم استقرار مناسب و حفاظت تجهیزات (C65) • عدم وجود امکانات پشتیبانی (C66)

جدول۱-۵: سه سطح سلسله‌مراتب مسألهٔ رتبه‌بندی علل بروز مخاطرات – ادامه

سطح اول (مخاطرات)	سطح دوم (اثر مخاطرات)	سطح سوم (علل بروز مخاطرات)
تغییرات (C5)	• از بین رفتن اطلاعات (C20) • قطع دسترسی اطلاعات (C21) • متوقف شدن عملیات کاری (C22)	• عدم داشتن روال مناسب (C67) • عدم وجود روش های اجرایی کنترل تغییر (C68) • منعطف‌نبودن سامانه (C69) • عدم بازنگری مستقل امنیت اطلاعات (C70) • عدم وجود فرآیند نظم و انضباط (C71) • عدم نگهداری مناسب تجهیزات (C72) • عدم مدیریت تغییر (C73) • عدم مدیریت ظرفیت اطلاعات (C74) • عدم مدیریت پذیرش اطلاعات در سامانه (C75)
نفوذ به سیستم (C6)	• از بین رفتن اطلاعات (C23) • دزدی اطلاعات (C24) • قطع دسترسی اطلاعات (C25) • از بین بردن یکپارچگی اطلاعات (C26) • متوقف نمودن عملیات کاری (C27) • از بین بردن اعتبار شرکت (C28)	• عدم وجود کنترل و حذف حقوق دسترسی (C76) • عدم سامانهٔ مانیتورینگ و کنترل های شبکه (C77) • عدم کنترل‌های رمزنگاری (C78)
حمله سایبری (C7)	• از بین رفتن اطلاعات (C29) • دزدی اطلاعات (C30) • قطع دسترسی اطلاعات (C31) • از بین بردن یکپارچگی اطلاعات (C32) • متوقف نمودن عملیات کاری (C33) • از بین بردن اعتبار شرکت (C34)	• عدم محافظت در برابر تهدیدهای خارجی و محیطی (C79) • عدم وجود کنترل‌ها در برابر کدهای مخرب (C80) • عدم وجود کنترل‌ها در برابر کدهای سیار (C81) • عدم سامانه محاسبه و ارتباطات سیار (C82) • نداشتن خط مشی طبقه‌بندی اطلاعات (C83) • عدم سامانهٔ مانیتورینگ و کنترل های شبکه (C84) • عدم کنترل‌های رمزنگاری (C85)

www.SID.ir

Archive of SID

جدول۱-۵: سه سطح سلسله‌مراتب مسأله رتبه‌بندی علل بروز مخاطرات – ادامه

سطح اول (مخاطرات)	سطح دوم (اثر مخاطرات)	سطح سوم (علل بروز مخاطرات)
دسترسی غیر مجاز (C8)	• از بین رفتن اطلاعات (C35) • دزدی اطلاعات (C36) • قطع دسترسی اطلاعات (C37) • از بین بردن یکپارچگی اطلاعات (C38) • متوقف کردن عملیات کاری (C39) • از بین بردن اعتبار شرکت (C40)	• نبود سیاهه مالکیت دارایی ها (C86) • عدم حذف حقوق دسترسی (C87) • حصار امنیت فیزیکی (C88) • عدم کنترل های ورودی های فیزیکی (C89) • عم ایمن سازی دفاتر،اتاق ها و تجهیزات (C90) • عدم وجود سامانهٔ کنترل دسترسی (C91) • صحت هویت کاربران برای اتصالات خارجی (C92) • نداشتن خط مشی طبقه‌بندی اطلاعات (C93) • عدم سامانهٔ مانیتورینگ و کنترل های شبکه (C94)
الزامات قانونی (C9)	• از بین رفتن اطلاعات (C41) • قطع دسترسی اطلاعات (C42) • متوقف‌شدن عملیات کاری (C43)	• عدم تحلیل و تعیین الزامات امنیتی (C95) • شناسایی قوانین قابل اجرا (C96) • قوانین کنترل های رمز نگاری (C97)
آگاهی و دانش نیروی انسانی (C10)	اشتباهات امنیتی (C44)	• عدم استفاده قابل قبول از دارایی ها (C98) • مشخص‌نبودن نقش ها و مسئولیت‌ها (C99) • نبود آگاهی ،تحصیل و آموزش امنیت اطلاعات (C100) • استفاده نکردن از کلمه عبور-رمز عبور (C101) • عدم رعایت میز پاک و صفحه پاک (C102)

جدول ۲-۵: خلاصه نتایج محاسبات وزن‌های علل بروز مخاطرات براساس FAHP و FAHP-TOPSIS

علل بروز مخاطرات	وزن نهایی علل بروز مخاطرات FAHP	وزن نهایی علل بروز مخاطرات FAHP – TOPSIS
C45	0.012	0.009
C46	0.010	0.012
C47	0.011	0.010
C48	0.011	0.009
C49	0.010	0.011
C50	0.011	0.010
C51	0.030	0.928
C52	0.028	0.62
C53	0.033	0.045
C54	0.030	0.658
C55	0.030	0.487
C56	0.033	0.584
C57	0.006	0.007
C58	0.008	0.007
C59	0.008	0.007
C60	0.008	0.009
C61	0.009	0.007
C62	0.008	0.008
C63	0.009	0.0095
C64	0.009	0.007
C65	0.009	0.010
C66	0.010	0.008
C67	0.037	0.936
C68	0.036	0.494
C69	0.036	0.141
C70	0.036	0.305
C71	0.035	0.629
C72	0.038	0.648
C73	0.040	0.835
C74	0.038	0.153
C75	0.038	0.731
C76	0.054	0.417
C77	0.056	0.710
C78	0.056	0.133
C79	0.023	0.478
C80	0.024	0.831
C81	0.024	0.500
C82	0.022	0.403
C83	0.024	0.465
C84	0.025	0.560
C85	0.025	0.132
C86	0.017	0.467
C87	0.018	0.463
C88	0.017	0.579
C89	0.018	0.876
C90	0.018	0.196
C91	0.019	0.307
C92	0.020	0.344
C93	0.019	0.621
C94	0.020	0.637
C95	0.113	0.648
C96	0.106	0.147
C97	0.115	0.790
C98	0.011	0.0118
C99	0.012	0.0095
C100	0.013	0.0118
C101	0.013	0.013
C102	0.011	0.0127
C94	0.020	0.637
C95	0.113	0.648
C96	0.106	0.147
C97	0.115	0.790
C98	0.011	0.0118
C99	0.012	0.0095
C100	0.013	0.0118
C101	0.013	0.013
C102	0.011	0.0127

www.SID.ir

Archive of SID

جدول۳-۵: نتایج تحلیلی آزمون تی نمونه‌های مستقل جهت بررسی تفاوت بین دو روش FAHP و FAHP-TOPSIS

t	درجه آزادی	سطح معنی داری	اختلاف میانگین ها	اختلاف خطای معیار	فاصله اطمینان	
					حد پایین	حد بالا
-7.172	80	0.000	-0.347	0.048	-0.443	-0.250

جدول۴-۵ نتایج توصیفی آزمون تی نمونه‌های مستقل جهت بررسی تفاوت بین دو روش FAHP و FAHP-TOPSIS

روش	میانگین	ضریب تغییرات
FAHP	0.029	0.856
FAHP-TOPSIS	0.377	0.819

۷- منابع

جبل‌عاملی س، رضائی‌فر الف، چائی‌بخش لنگرودی ع.، "رتبه‌بندی ریسک‌های پروژه با استفاده از مدل‌های تصمیم‌گیری چندشاخصه،" دومین کنفرانس بین‌المللی مدیریت پروژه، نشریه دانشکدهٔ فنی، اسفند ۱۳۸۶، جلد ۴۱، شماره ۷، صص. ۸۶۳-۸۷۱.

جوزی ع.، صفاریان ش.، "تجزیه و تحلیل ریسک‌های محیط زیستی نیروگاه گازی آبادان با استفاده از روش تاپسیس،" محیط‌شناسی، تابستان ۱۳۹۰، سال سی و هفتم، شماره ۵۸، صص.۵۳-۶۶.

Almunawar Mohammad Nabil, Susanto Heru, Tuan Yong Chee, "Information Security Management System Standards:A Comparative Study of the Big Five," Inter-national Journal of Electrical & Computer Sciences IJECS-IJENS, 2011, vol. 11, PP. 23-27.

Bojanc Rok, Jerman-Blazic Borka, "An economic modelling approach to information security risk management," International Journal of Information management, 2008, vol. 28, no. 5, pp. 413–422.

Ekelhart Andreas, Fenz Stefan, Neubauer Thomas, "AURUM: A Framework for Information Security Risk Management," 42nd Hawaii International Conference on System Sciences - 2009, 2009.

Elhag Taha M.S., Wang Ying-Ming, "Fuzzy TOPSIS method based on alpha level sets with an application to bridge risk assessment," Expert Systems with Applications,2006, vol. 31, no. 2, pp. 309–319.

Haghighirad F., Makui A., Ashtiani B., "Extension of fuzzy TOPSIS method based on interval-valued fuzzy sets," Journal Applied Soft Computing, vol. 9, no. 2, pp. 457-461, March 2009.

Hosseinzadeh Lotfi F., Izadikhah M., Jahanshahloo G.R., "Extension of the TOPSIS method for decision-making problems with fuzzy data," International Journal of Mathematics and Computation, 2006, vol. 181, pp. 1544–155.

Hung Chia-Chang, Chen Liang-Hsuan, "A Fuzzy TOPSIS Decision Making Model with Entropy Weight under Intuitionistic Fuzzy Environment," in International Multi Conference of Engineers and Computer Scientists (IMECS), Hong Kong, 2009, vol. 1.

Jolai Fariborz, Tavakkoli-Moghaddam Reza, Mousavi S. Meysam, "A Fuzzy Stochastic Multi-Attribute Group Decision-Making Approach for Selec-tion Problems," Group Decision and Negtiation Conference, March 2013, vol. 22, no. 2, pp. 207-233.

Kordi Maryam, "Comparison of fuzzy and crisp analytic hierarchy process (AHP) methods for spatial multi criteria decision analysis in GIS," Master's Thesis Dep. OF Technologhy and Built enviroment, University of GAVLE, September 2008.

Lin Cheng-Wei, Opricovic Serafim, Tzenga Gwo-Hshiung, "Multi-criteria analysis of alternative-fuel buses for public transportation," International Journal of Energy Policy, vol. 33, pp. 1373–1383, 2005.

Meer Jeroen van der, "Multi-criteria decision model inference and application in information security risk classification," Master Thesis, Dept. of Compu-tational Economics, Erasmus University Rotterdam, Aug 2012.

Opricovic Serafim, Tzeng Gwo-Hshiung, "Defu-zzification within a Multi Criteria Decision Model," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems , October 2003, vol. 11, no. 5.

Shameli-Sendi A., Shajari M., Hassanabadi M., Jabbarifar M., Dagenais M., "Fuzzy Multi-Criteria Decision-Making for Information Security Risk Assessment," The Open Cybernetics & Systemics Journal, 2012, vol. 6, pp. 26-37.

Shameli-Sendi Alireza, Jabbarifar Masoume, Shajari Mehdi and Dagenais Michel, "FEMRA: Fuzzy Expert Model for Risk Assessment," The Fifth International Conference on Internet Monitoring and Protection,2010.

Smojver Slave, "Selection of Information Security Risk Management Method Using Analytic Hierarchy Process (AHP)," in 22nd Central European Conference on Information and Intelligent Systems, September 2011.

www.SID.ir

Archive of SID

Sotoudeh Gohar A., Khanzadi M., Parchami Jalal M., "A Fuzzy MCDM for Evaluating Risk of Construction Projects," Australian Journal of Basic and Applied Sciences, 2011, vol. 5, no. 12, pp. 162-171.

Talabis Mark Rayan, Martin Jason, "Information Security Risk Assessment Toolkit," 1st ed.: Syngress, 2013.

Tesfamariam S., Sadiq R., "Risk-based environmental decision-making using fuzzy analytic hierarchy process (F-AHP)," Stochastic Environmental Research and Risk Assessment, 2006, vol. 2, no. 1.

T.L. Saaty, "The Analytic Hierarchy Process," 2000.

Wang Jing-Hong, Ma Jian-feng, Zhao Dong-Mei, "Fuzzy Risk Assessment of the Network Security," Proceedings of the Fifth International Conferenceon Machine Learning and Cybernetics, August 2006.

Wang Zhihu, Zeng Haiwen, "Study on the Risk Assessment Quantitative Method of Information Security," 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), 2010, pp. V6-529-V6-533.

Yanling Shang, Honghui Niu, "Research on risk assessment model of information security based on particle swarm algorithm -RBF neural network," Second Pacific-Asia Conference on Circuits, Communications and System (PACCS), 2010.

Zakarevicius Algimantas, Antucheviciene Jurgita, Zavadskas Edmundas Kazimieras, "Evaluation of Ranking Accuracy in Multi-Criteria Decisions," International Journal of Mathematics and Informatics, Vilnius, 2006, vol. 17, no. 4, pp. 601–618.

Zhiwei Yu, Zhongyuan Ji, "A Survey on the Evolution of Risk Evaluation for Information Systems Security," International Conference on Future Electrical Power and Energy System, 2012, vol. 17, pp. 1288–1294.

Zhiwei Yu, Zhongyuan Ji, "A Survey on the Evolution of Risk Evaluation for Information Systems Security," International Conference on Future Electrical Power and Energy System, 2012, vol. 17, pp. 1288–1294.

Zhou Hangjun, Fu Sha, "The information security risk assessment based on AHP and fuzzy comprehensive evaluation," Communication Software and Networks (ICCSN), in IEEE 3rd International Conference on, 2011, pp. 124 -128.

Yu-Ping Ou Yang, How-Ming Shieh, Gwo-Hshiung Tzeng, "A VIKOR technique based on DEMATEL and ANP for information security risk control assessment," Information Sciences Journal, 2013, vol. 232, pp. 482-500.

مهسا آقا محی‌الدین دورهٔ کارشناسی خود را در دانشگاه کیش (صنعتی شریف پردیس کیش) در رشتهٔ مهندسی نرم‌افزار پشت سر گذاشت و مدرک کارشناسی ارشد خود در رشته فناوری اطلاعات گرایش امنیت اطلاعات را در سال ۹۲ از دانشگاه تهران پردیس کیش دریافت کرد. زمینه‌های مورد علاقهٔ ایشان سامانه‌های مدیریت امنیت اطلاعات، مدیریت ریسک امنیت اطلاعات و روش‌های مختلف تصمیم‌گیری چندشاخصه در زمینه این مدیریت‌هاست.

نشانی رایانامهٔ ایشان عبارت است از:

mahmoh@ymail.com

حسین قرایی تحصیلات خود را در مقطع کارشناسی مهندسی برق- الکترونیک در دانشکده مهندسی برق دانشگاه خواجه نصیرالدین طوسی در سال ۱۳۷۷ به اتمام رساند. مقاطع کارشناسی ارشد و دکتری مهندسی برق - الکترونیک در دانشکده مهندسی برق دانشگاه تربیت مدرس را به‌ترتیب در سال‌های ۱۳۷۹ و ۱۳۸۸ تکمیل کرد. از سال ۱۳۸۱ تاکنون عضو هیئت علمی مرکز تحقیقات مخابرات است و زمینه‌های تحقیقاتی مورد علاقهٔ ایشان طراحی مدارات VLSI دیجیتال، آنالوگ و سیگنال مختلط، پردازش سیگنال‌های دیجیتال، سامانه‌های تشخیص و پیش‌گیری از نفوذ و مرکز عملیات امنیت و اجزای آن هستند.

نشانی رایانامهٔ ایشان عبارت است از:

gharaee@itrc.ac.ir

www.SID.ir