

ارزیابی ریسک‌های نرم افزاری امنیت اطلاعات سامانه اطلاعاتی تحقیقاتی با استفاده از روش ترکیبی تجزیه تحلیل حالات بالقوه خرابی فازی و تصمیم‌گیری با معیارهای چندگانه فازی

مهرداد فروزنده

دانشجوی کارشناسی ارشد، گروه مهندسی صنایع دانشگاه آزاد اسلامی نجف آباد؛ forouzandeh05@gmail.com

محمد جواد ارشادی

عضو هیئت علمی پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)*

مهدی کرباسیان

عضو هیئت علمی، دانشگاه صنعتی مالک اشتر؛ mkarbasi@mut-es.ac.ir

چکیده امروزه با گسترده تر شدن استفاده از رایانه در سیستم‌های اطلاعاتی، تنوع ریسک‌های امنیت اطلاعات افزایش یافته و مدیریت اینگونه ریسک‌ها بیش از پیش مورد توجه قرار گرفته است. با توجه به اهمیت امنیت اطلاعات در سامانه‌های اطلاعاتی تحقیقاتی برخط بعنوان منابع اصلی تحقیقات و پژوهش‌های آتی، این مطالعه با بکارگیری مدل ترکیبی از منطق فازی، ابزار FMEA و روش‌های تصمیم‌گیری AHP و TOPSIS، سعی در ارزیابی و اولویت‌بندی بهینه ریسک‌های امنیت اطلاعات یک سامانه اطلاعاتی تحقیقاتی برخط در ایران را دارد. با استفاده از منطق فازی در روش FMEA سنتی، امتیازات شفاف‌تر و دقیق‌تر ارزیابی شده و با بکارگیری روش‌های AHP و TOPSIS فازی ابتدا وزن معیارهای روش FMEA اندازه‌گیری و سپس با محاسبه ضریب نزدیکی، ریسک‌های بالقوه شناسایی شده، اولویت‌بندی گردیده است. نتایج حاصل از این مقاله در بررسی کاربرد این مدل در شناسایی، ارزیابی و اولویت‌بندی ریسک‌های بالقوه سامانه مورد مطالعه در سه حوزه اصلی: محرمانگی، دردسترس بودن و یکپارچگی اطلاعات نشان می‌دهد، ریسک‌های مربوط به دسترسی غیرمجاز به اطلاعات و درست و یکپارچه نبودن اطلاعات از نظر کارشناسان این سامانه در اولویت بالاتری قرار دارد.

کلمات کلیدی سامانه اطلاعاتی تحقیقاتی، مدیریت ریسک، امنیت اطلاعات، تجزیه و تحلیل حالات خرابی و آثار آن.

۱- مقدمه

ارزش بیش از یک هزار میلیارد دلار در عرض یک سال منجر می‌شود [۲].

مدیریت امنیت اطلاعات وظیفه پیاده‌سازی و کنترل عملکرد سیستم امنیت سازمان را بر عهده داشته و در نهایت باید تلاش کند سیستم را همیشه روز آمد نگه دارد [۳]. هدف مدیریت امنیت اطلاعات در سازمان، حفظ سرمایه‌های سازمان در برابر هرگونه

امروزه فناوری اطلاعات به سرعت توسعه یافته و سیستم‌های اطلاعاتی نقشی تعیین کننده و فراگیر در کسب و کارهای سازمانی دارند [۱]. از این رو عالی ترین سطح مدیریت پاسخگوی سازمان، مسئولیت حفاظت از اطلاعات سازمان را بر عهده دارد. اگر چه امنیت اطلاعات اغلب منافع بسیاری را برای سازمان به ارمغان می آورد اما پیاده‌سازی آن، گاه با مشکل مواجه می شود. در پژوهشی که توسط شرکت امنیتی مک آفی در سال ۲۰۰۸ انجام شده نشان داده که نقض امنیت اطلاعات در شرکت‌های جهانی به زبانی به

* (Corresponding author) ershadi@irandoc.ac.ir

این سامانه علی‌رغم کارایی و اثر بخشی در ثبت و اشاعه اطلاعات علمی به کاربران، با معایب و اشکالاتی مواجه است و نیاز به بهینه‌سازی بخصوص در حوزه مدیریت امنیت اطلاعات دارد تا اهداف راهبردی بهتر محقق شوند.

پیش‌نیاز برنامه‌ریزی موفق جهت کاهش ریسک‌ها، شناسایی و ارزیابی مناسب و در ادامه ارائه طرح‌های اصلاحی و پیشگیرانه کم‌هزینه و موثر می‌باشد. در این زمینه روش تجزیه و تحلیل حالات شکست و آثار آنها (FMEA¹) به عنوان ابزاری کارآمد می‌تواند بهترین گزینه باشد. اگرچه روش FMEA سنتی بطور گسترده در منابع تحقیقاتی استفاده شده است اما نقاط ضعف و محدودیت‌هایی نیز دارد که از جمله اینها عبارتند از:

- در نظر نگرفتن درجه اهمیت معیارها نسبت به یکدیگر
 - گاهی ممکن است امتیازات چند ریسک یکسان شده و تصمیم‌گیری را سخت نمایند
 - معیارها دارای ماهیت ذهنی و امتیازها نادقیق و مبهم هستند
 - سوال برانگیز بودن فرمول محاسبه امتیاز ریسک‌ها
- برای حل مشکلات فوق از روش FMEA سنتی همراه با تئوری فازی و ترکیب روش‌های امتیازدهی و روش‌های تصمیم‌گیری چندگانه استفاده می‌شود [6].

در این پژوهش تلاش می‌شود با هدف صرفه‌جویی در هزینه‌های مدیریت امنیت اطلاعات و جلوگیری از به خطر افتادن اعتبار سامانه اطلاعاتی تحقیقاتی برخط مورد مطالعه، ریسک‌های حوزه نرم‌افزاری امنیت اطلاعات این سامانه با استفاده از جلسات طوفان فکری خبرگان این سازمان و با بهره‌گیری از روش FMEA فازی شناسایی و ارزیابی و با بکارگیری مدل ترکیبی روش‌های تصمیم‌گیری فازی فرایند تحلیل سلسله‌مراتبی² (AHP) و روش تصمیم‌گیری ترجیح براساس مشابهت به راه حل ایده‌آل³ (TOPSIS) رتبه‌بندی شده تا برنامه‌ریزی و مدیریت آنها در برنامه آتی سازمان قرار گیرد.

تهدید است و برای رسیدن به این هدف به برنامه جامع و یکپارچه‌ای نیاز دارد.

بهترین راه مدیریت، اطلاع از وضعیت موجود و اتخاذ تصمیمات صحیح جهت بهبود آن می‌باشد. ارزیابی ریسک مهم‌ترین بخش ارزیابی و شناسایی وضعیت موجود می‌باشد [4]. مدیریت ریسک از چهار فاز شناسایی، ارزیابی، برنامه‌ریزی یا مدیریت و ردیابی رخدادهای ریسکی تشکیل می‌گردد.

در چارچوب مدیریت ریسک امنیت اطلاعات دو بعد ساختاری و دو بعد رویه‌ای تعریف شده که حوزه و معیارهای ارزیابی، ابعاد ساختاری و روند و ابزار ارزیابی، ابعاد رویه‌ای می‌باشند. این چارچوب دیدی جامع، دربرگیرنده استراتژی، فناوری، سازمان، مردم و محیط برای دامنه این مدیریت دارا می‌باشد. در این چارچوب جهت تعیین معیارهای ارزیابی می‌توان از استانداردهای گوناگون و جهت ابعاد رویه‌ای نیز می‌توان از چرخه شش سیگما (تعریف، اندازه‌گیری، تجزیه و تحلیل، بهبود و کنترل) و ابزارهای دیگر استفاده نمود [5]. در سامانه‌های تحقیقاتی برخط بعنوان پایگاه‌های جمع‌آوری، سازمان‌دهی، ذخیره، حفظ، بازیابی، تحلیل و اشاعه اطلاعات پشتیبان آنها در سطح بین‌المللی، امنیت اطلاعات و مدیریت ریسک از اهمیت بسزایی برخوردار می‌باشد. در اینگونه سامانه‌ها عوامل شکست می‌توانند سطوح دسترسی به اطلاعات، درستی و یکپارچه بودن اطلاعات و محرمانه بودن اطلاعات را تهدید نموده و در نهایت اعتبار سامانه و مطالعات تحقیقاتی ارجاع شده به این مراکز را زیر سوال ببرند.

پژوهشگاه علوم و فناوری اطلاعات ایران (ایراندک) که سابقاً مرکز اطلاعات و مدارک علمی ایران نامیده می‌شد، از سال ۱۳۴۷ عهده دار شناسایی، گردآوری، سازماندهی و اشاعه اطلاعات مربوط به مدارک علمی متعددی در ایران بوده است. این مرکز از سال ۱۳۶۹ با استفاده از نرم‌افزار CDS/ISIS شروع به تولید پایگاه اطلاعات علمی نمود و از سال ۱۳۷۲، عرضه و روزآمدی پایگاه‌های اطلاعات متنوعی در این محیط را آغاز نمود و به مدت چندین سال به انتشار نسخه‌های چاپی این اطلاعات، ادامه داده است. در سالهای اخیر با توجه به گسترش برنامه‌های رایانه‌ای در بستر وب، این پایگاه اطلاعات با نام گنج و در محیط MySQL ارائه شده است. سامانه گنج، گنجینه‌ای با ارزش از اطلاعات علمی و فراداده‌های اساتید، دانشجویان و محققان ایرانی است.

3 Technique for Order Preference by Similarity to Ideal Solution (TOPSIS)

¹ Failure Mode and Effects Analysis (FMEA)

² Analytical Hierarchy Process (AHP)

۲- پیشینه پژوهش

ترکیبی از روش بهینه‌سازی چندمعیاره و حل‌سازی (VIKOR)^۲، روش تصمیم‌گیری قضاوتی و ارزیابی آزمایشی (DEMATEL)^۴ و روش فرآیند تحلیل شبکه^۵ (ANP) برای حل مساله معیارهای متناقض است که وابستگی و بازخورد آنها را نشان می‌دهد. علاوه بر این، یک مطالعه موردی نیز برای ارزیابی مدل ارائه شده و نشان دادن اثربخشی آن، انجام گرفته است [۱۰].

در ارزیابی ریسک‌های امنیت اطلاعات یک گروه پژوهشی در دانشگاه، از روش FMEA فازی استفاده شده است. در این روش ۵ بعد از امنیت اطلاعات شامل: دسترسی به اطلاعات و سیستم‌ها، ارتباطات، زیرساخت‌ها، مدیریت امنیت، توسعه سیستم‌های امنیت اطلاعات توسط روش FMEA فازی آنالیز و ریسک‌های مربوطه اولویت‌بندی شده است [۱۱].

با استفاده از شبکه‌های بیزین، ریسک‌های امنیت اطلاعات در یک شرکت خدمات مالی شناسایی و سپس بوسیله الگوریتم کلونی مورچگان بر اساس مسیر انتشار با بالاترین احتمال و بزرگی امتیاز ریسک برآوردی رتبه‌بندی شده که در این تحقیق ریسک شبکه و حالات شکست مربوط به احراز هویت برای کاربر در اتصالات خارجی در اولویت قرار گرفته است [۱۲].

با ترکیب روش FMEA و تئوری خاکستری مدلی جهت شناسایی و ارزیابی ریسک‌های امنیت داده‌های بزرگ ارائه شده که در این مدل از روش FMEA جهت شناسایی و ارزیابی ریسک‌های امنیت اطلاعات در چهار حوزه اصلی شناسایی و مدیریت دسترسی، ثبت نام دستگاه و برنامه، مدیریت زیرساخت، مدیریت اطلاعات و از تئوری خاکستری جهت رتبه‌بندی ریسک‌ها استفاده شده است [۱۳].

در پژوهشی با ارائه مدلی ترکیبی از درخت رویداد و تئوری تصمیم‌گیری فازی به شناسایی و ارزیابی ریسک‌های امنیت اطلاعات پرداخته و در این مدل رویدادها و خطرات شناسایی و با استفاده از نظرات خبرگان و ابزار تصمیم‌گیری فازی و بر اساس احتمال وقوع و زیان‌های مالی، ریسک‌ها اولویت‌بندی می‌شوند [۱۴].

برای ارزیابی حالات شکست رایانش‌های ابری از مدلی با استفاده از منطق فازی و اعداد فازی ذوزنقه‌ای استفاده شده که

موضوع امنیت اطلاعات از زمانی در کانون توجه قرار گرفت که مبحث امنیت فیزیکی مطرح شد و این دو موضوع با پشتیبانی از یکدیگر، به استخوان‌بندی امنیت شرکت‌ها می‌پردازند. با پیدایش اولین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵، نگرش نظام‌مند به مقوله ایمن‌سازی فضای تبادل اطلاعات شکل گرفت [۶]. بر اساس این نگرش، امنیت اطلاعات سازمان‌ها، با تکرار تأمین نمی‌شود، بلکه باید این کار بصورت مداوم طی چرخه ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح، بر اساس روش‌شناسی مشخص و برنامه‌ریزی شده‌ای در سازمان انجام گیرد [۷].

پژوهش‌های زیادی در زمینه مدیریت ریسک امنیت اطلاعات بوسیله ابزارهای و مدل‌های گوناگون در سازمان‌های مختلف انجام گردیده و با توجه به زمینه‌های کاری، اهداف و استراتژی‌های آنها نتایج متنوعی در ارزیابی اینگونه ریسک‌ها حاصل گردیده است.

با توجه به اهمیت مدیریت ریسک امنیت اطلاعات در بیمارستان‌ها، در پژوهشی با استفاده از گروه‌های خبره و سوابق گذشته تهدیدات امنیت اطلاعات در بیمارستان‌ها را بررسی شده است. یافته‌های این پژوهش حاکی از آن است که عوامل مختلفی مثل عدم آموزش کارکنان، دستورالعمل‌های مبهم در مورد امنیت اطلاعات، چالش‌های بهره‌وری، کاربرد نامناسب اطلاعات و زیرساخت‌های امنیتی منسوخ شده، می‌توانند امنیت و محرمانگی اطلاعات را در معرض خطر قرار دهند [۸].

جهت ارزیابی ریسک‌های امنیت اطلاعات دولت الکترونیک از ادغام نتایج تحقیقات فرایند تحلیل سلسله‌مراتبی فازی^۱ (FAHP) و روش شبکه عصبی مصنوعی^۲ (ANN) استفاده شده است. در این تحقیق عدم حفاظت از سیستم‌ها و داده‌های مدیریت، نقص‌ها و عیوب فنی و کیفیت خطوط انتقال داده اطلاعات از جمله ارجح‌ترین این ریسک‌ها بیان شده است [۹].

در مقاله‌ای مدلی جهت ارزیابی و کنترل ریسک امنیت اطلاعات پیشنهاد می‌دهند که می‌تواند امنیت اطلاعات را برای شرکت‌ها و سازمان‌ها ارتقا دهد. این مدل یک مدل تصمیم‌گیری چند معیاره

⁴ Decision Making Trial and Evaluation Laboratory (DEMATEL)

⁵ Analytical Network Process (ANP)

¹ Fuzzy Analytical Hierarchy Process (FAHP)

² Artificial Neural Network (ANN)

³ Vlse Kriterijumska Optimizacija I Kompromisno Resenje (VIKOR)

در این پژوهش ریسک‌ها با در نظر گرفتن شدت اثر و احتمال وقوع آنها رتبه‌بندی می‌شوند [۱۵].

از آنجا که ارزیابی ریسک در امنیت اطلاعات تاریخچه جدیدی دارد، مطالعات، استانداردها و متدولوژی‌ها در زمینه مدیریت ریسک امنیت اطلاعات روز به روز در حال افزایش می‌باشد.

با ترکیب روش FMEA سنتی بعنوان یک ابزار کارآمد در مدیریت ریسک با ابزارهای دیگر سعی شده محدودیت‌های این روش را کاهش و اعتماد به نتایج را افزایش داد. از جمله این روش‌های ترکیبی، در مطالعه‌ای از ابزار FMEA و منطق فازی جهت اصلاح ضعف‌های FMEA سنتی و شناسایی، ارزیابی و اولویت‌بندی دقیق‌تر ریسک‌های اورژانس یک بیمارستان بهره برده است [۱۶].

مدلی دیگر ترکیب AHP و روش FMEA فازی می‌باشد؛ در این روش بوسیله FMEA حالات شکست بالقوه شناسایی و ارزیابی شده، سپس با بکارگیری روش AHP معیارها وزن‌دهی شده و در نهایت ریسک‌ها اولویت بندی می‌شوند [۱۷]. در تجزیه تحلیل حالات خطای کارخانه صنایع فولاد کرمان با بهره‌گیری از FMEA فازی، حالات خطا شناسایی و ارزیابی و جهت اولویت‌بندی دقیق‌تر از روش‌های AHP و MULTIMOORA فازی جهت وزن‌دهی معیارهای ابزار FMEA و حالات خطا استفاده شده است [۱۸].

برای تعیین اولویت‌های تعمیر و نگهداری در برنامه‌ریزی نت شرکت بین المللی مواد غذایی ترکیب FMEA فازی و روش تصمیم‌گیری TOPSIS بکارگیری شده است [۱۹]. یکی از مدل‌های پر کاربرد دیگر، استفاده از ترکیب منطق فازی، روش‌های تصمیم‌گیری AHP و TOPSIS با ابزار FMEA جهت بهبود ارزیابی و اولویت بندی ریسک می‌باشد. در این روش نیز بوسیله FMEA فازی عدم انطباق‌ها شناسایی و ارزیابی و سپس با AHP فازی معیارها وزن‌دهی و با روش TOPSIS ریسک‌ها اولویت‌بندی شده‌اند [۲۰]. همچنین در پژوهشی دیگر از ترکیب روش‌های DEMATEL و TOPSIS در مرحله تصمیم‌گیری روش FMEA استفاده شده است [۲۱].

در ادامه سوابق فوق با توجه به نبود پیشینه در حوزه امنیت اطلاعات سازمان‌ها و سامانه‌های علمی تحقیقاتی و ارزیابی ریسک‌های آنها، سعی می‌شود برای نخستین بار، با استفاده از روش بهبود یافته FMEA فازی تهدیدات و عدم انطباق‌های حوزه نرم افزاری امنیت اطلاعات سامانه اطلاعاتی تحقیقاتی برخط مورد مطالعه، شناسایی و ارزیابی و پس از وزن‌دهی معیارهای روش

FMEA از نظر کارشناسان بوسیله روش تصمیم‌گیری مقایسات زوجی AHP فازی، با استفاده از روش تصمیم‌گیری چندگانه TOPSIS فازی ضریب نزدیکی هر کدام از ریسک‌ها محاسبه و اولویت‌بندی شوند.

۳- روش پژوهش

مدل استفاده شده در این پژوهش و مراحل شناسایی و ارزیابی حالات خطا امنیت اطلاعات با محوریت ابزار FMEA نشان داده شده است. در این مدل پس از شناسایی و بررسی فرایندها و دارایی‌های حوزه نرم‌افزار سامانه علمی تحقیقاتی مورد مطالعه، حالات خطا و عدم انطباق‌های احتمالی با استفاده از نظرات کارشناسان خبره این سامانه و ابزار FMEA شناسایی و ارزیابی می‌گردد؛ سپس با بکارگیری روش تصمیم‌گیری AHP فازی و نظرسنجی از خبرگان سامانه وزن‌های سه معیار ابزار FMEA، شدت اثر، احتمال وقوع و احتمال شناسایی، محاسبه و در نظرات اعمال می‌گردد. در نهایت با بهره‌گیری از روش تصمیم‌گیری TOPSIS فازی ضریب‌نزدیکی هر یک از ریسک‌های شناسایی و پیش‌بینی شده محاسبه و با توجه به نزدیکی آنها به عدد یک، ریسک‌ها رتبه بندی و اولویت‌بندی می‌گردند.

در ادامه ابزارها و روش‌های مورد استفاده در مدل ترکیبی FMEA فازی و روش‌های تصمیم‌گیری فازی AHP و TOPSIS شرح داده می‌شوند.

۳-۱- روش FMEA

با توجه به کاستی‌های رویکرد سنتی FMEA تحقیقات بسیاری با هدف توسعه و بهبود عملکرد آن انجام شده است، یکی از راه‌حل‌های موجود برای رفع این کاستی‌ها، ترکیب این رویکرد با منطق فازی است. در تحقیقی در سال ۱۹۹۵ برای نخستین بار، FMEA با منطق فازی ترکیب شد. این منطق در مواردی که داده‌های کافی در دسترس نیست، جمع‌آوری آنها کار مشکلی است یا داده‌ها به صورت عبارات و متغیرهای زبانی و ذهنی موجود است، ابزار مناسبی به شمار می‌آید.

مزایای استفاده از FMEA فازی عبارتند از [۲۲]:

- خبرگان با استفاده از متغیرهای زبانی در رویکرد فازی مقادیر معنادارتر و ملموس‌تری را به معیارهای سه گانه اختصاص می‌دهند.

مجموعه‌های فازی، مجموعه‌ای از اشیا نادقیق با درجات عضویت مختلف می‌باشد. تابع عضویت تابعی با برد $[0,1]$ است [۲۳].

منطق فازی جهت استدلال‌های تقریبی در مقابل استدلال‌های دقیق در محیط عدم قطعیت از تئوری مجموعه‌های فازی استخراج شده است. این موضوع باعث ترکیب آسان نظرات مختلف کارشناسان در برآورد پارامترهای موضوعات مختلف می‌شود.

از میان اعداد مختلف فازی، اعداد فازی مثلثی متداول تر بوده، که با سه درجه نشان داده می‌شوند [۲۴]:

$$A = (a_1, a_2, a_3) \quad (1)$$

تابع عضویت این اعداد بصورت زیر می‌باشد:

$$\mu_{\tilde{A}}(x) = \begin{cases} 0 & , x < a_1 \\ \frac{x-a_1}{a_2-a_1} & , a_1 \leq x \leq a_2 \\ \frac{a_3-x}{a_3-a_2} & , a_2 \leq x \leq a_3 \\ 0 & , a_3 < x \end{cases} \quad (2)$$

اگر دو عدد فازی A و B را بصورت $A = (a_1, a_2, a_3)$ و $B = (b_1, b_2, b_3)$ تعریف شوند آنگاه:

- جمع این دو، عدد C:

$$C = (a_1 + b_1, a_2 + b_2, a_3 + b_3) \quad (3)$$

- تفریق آنها، عدد D:

$$D = (a_1 - b_3, a_2 - b_2, a_3 - b_1) \quad (4)$$

- ضربشان، عدد E:

$$E = (a_1 \cdot b_1, a_2 \cdot b_2, a_3 \cdot b_3) \quad (5)$$

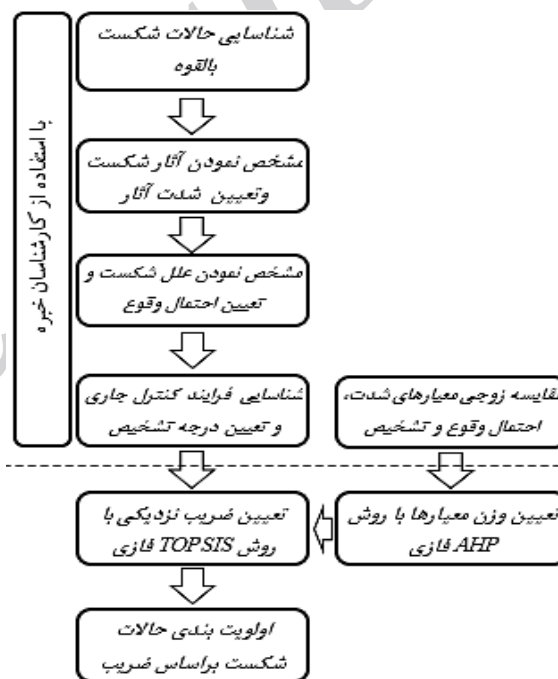
۳-۳-۳ AHP فازی

فرایند تحلیل سلسله مراتبی به صورت مقایسات زوجی توسط خبرگان صورت می‌گیرد که از منطق فازی جهت واقعی‌تر کردن این توصیفات زبانی و مبهم می‌توان استفاده نمود. در ادامه روش

- انعطاف‌پذیری در تخصیص وزن به سه متغیر روش FMEA فازی

- استنتاج فازی، قابلیت ترکیب شدن با دانش خبرگان را داشته و نتایج قابل تفسیر ی را توسط آنان ارائه می‌دهد.

از دیگر کاستی‌های FMEA سنتی تاثیر یکسان متغیرهای سه-گانه در محاسبه درجه اولویت ریسک^۱ می‌باشد که با استفاده از روش AHP فازی و نظرات خبرگان می‌توان وزن معیارهای FMEA را با توجه به نظر کارشناسان محاسبه نموده و این موضوع را نیز بهبود بخشید و در نهایت با استفاده از روش تصمیم‌گیری چندگانه TOPSIS فازی، بجای محاسبه RPN سنتی، ضریب نزدیکی هر کدام از عوامل شکست را نسبت به امتیاز ایده‌آل محاسبه، آنها را اولویت‌بندی نمود [۶].



شکل ۱: مراحل ارزیابی حالات شکست براساس روش FMEA بهبود یافته

۳-۲-۲ تئوری فازی

نظریه مجموعه‌های فازی بصورت رسمی اولین بار توسط پرفسور لطفی عسگرزاده با انتشار مقاله در مجله "اطلاعات و کنترل"، در سال ۱۹۶۹ مطرح گردید. این نظریه از آن زمان تاکنون گسترش زیادی یافته و کاربرد های گوناگونی یافته است.

¹ RISK PRIORITY NUMBER (RPN)

مرحله سوم: برای $\tilde{M} \geq \tilde{M}_1, \tilde{M}_2, \dots, \tilde{M}_k$ خواهیم داشت:

(۱۲)

$$V(\tilde{M} \geq \tilde{M}_1, \tilde{M}_2, \dots, \tilde{M}_k) = \min V(\tilde{M} \geq \tilde{M}_i), \quad i = 1, 2, \dots, k$$

(۱۳)

$$\hat{d}(A_i) = \min V(S_i \geq S_k), \quad k = 1, 2, \dots, n, \quad k \neq i$$

در نتیجه وزن برداری برای Π شی برابر می‌شود با:

(۱۴)

$$\hat{W} = (\hat{d}(A_1), \hat{d}(A_2), \dots, \hat{d}(A_n))^T, \quad i = 1, 2, \dots, n$$

و با نرمالیزه کردن وزن برداری:

(۱۵)

$$W = (d(A_1), d(A_2), \dots, d(A_n))^T, \quad i = 1, 2, \dots, n$$

که عدد W یک عدد غیرفازی می‌باشد.

جدول ۱: امتیازات ارزیابی فازی جهت روش AHP فازی

امتیازات فازی	متغیرهای زبانی	علائم اختصاری
(۲و۵، ۲و۳)	کاملاً قوی	AS
(۳، ۲و۵، ۲)	بسیار قوی	VS
(۱و۳، ۲و۲)	نسبتاً قوی	FS
(۱و۳، ۲)	کمی قوی	SS
(۱و۱)	برابر	E
(۲، ۳و۱)	کمی ضعیف	SW
(۱، ۲و۲، ۳و۱)	نسبتاً ضعیف	FW
(۲، ۵و۱، ۲و۲، ۳)	بسیار ضعیف	VW
(۱، ۳و۲، ۵و۱، ۲)	کاملاً ضعیف	AW

تحلیل سلسله مراتبی فازی بصورت مختصر شرح داده می‌شود [۲۵]:

اگر $X=(x_1, x_2, \dots, x_n)$ را مجموعه اشیا و $U=(u_1, u_2, \dots, u_n)$ مجموعه اهداف باشند آنگاه با توجه به این روش می‌توان مقدار هر شی به ازای هر یک از اهداف را به ترتیب بدست آورد:

m ارزش بدست آمده برای هر شی می‌باشد و $\tilde{M}_{gi}^1, \tilde{M}_{gi}^2, \dots, \tilde{M}_{gi}^j$ اعداد فازی ($j=1, 2, \dots, m$ و $i=1, 2, \dots, n$) هستند.

مرحله اول: ارزش ترکیبی فازی برای هر شی بصورت زیر تعریف می‌شود:

$$\tilde{S}_i = \sum_{j=1}^m \tilde{M}_{gi}^j \odot [\sum_{i=1}^n \sum_{j=1}^m \tilde{M}_{gi}^j]^{-1} \quad (۶)$$

$$\tilde{M}_{gi}^j = [\sum_{j=1}^m l_j, \sum_{j=1}^m m_j, \sum_{j=1}^m u_j]^{-1} \quad (۷)$$

$$\sum_{i=1}^n \sum_{j=1}^m \tilde{M}_{gi}^j = (\sum_{i=1}^n l_i, \sum_{i=1}^n m_i, \sum_{i=1}^n u_i) \quad (۸)$$

$$[\sum_{i=1}^n \sum_{j=1}^m \tilde{M}_{gi}^j]^{-1} = \left(\frac{1}{\sum_{i=1}^n u_i}, \frac{1}{\sum_{i=1}^n m_i}, \frac{1}{\sum_{i=1}^n l_i} \right) \quad (۹)$$

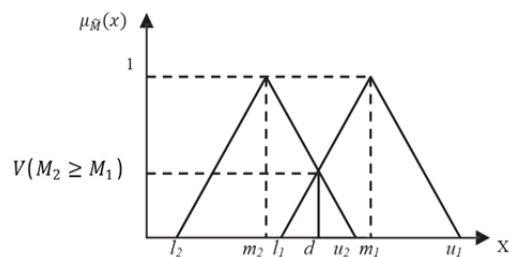
مرحله دوم: \tilde{M}_1 و \tilde{M}_2 دو عدد فازی مثلثی هستند که $\tilde{M}_1 \geq \tilde{M}_2$ تعریف می‌شود:

(۱۰)

$$V(\tilde{M}_1 \geq \tilde{M}_2) = \sup_{x \geq y} [\min(\mu_{\tilde{M}_1}(x), \mu_{\tilde{M}_2}(y))]$$

$$V(\tilde{M}_2 \geq \tilde{M}_1) = \mu(d) = \begin{cases} 1, & \text{if } m_1 \geq m_2 \\ 0, & \text{if } l_2 \geq u_1 \\ \frac{l_1 - u_2}{(m_2 - u_2) - (m_1 - l_1)}, & \text{otherwise} \end{cases} \quad (۱۱)$$

با توجه به شکل ۲، d در نقطه D بزرگترین تقاطع بین $\mu_{\tilde{M}_1}$ و $\mu_{\tilde{M}_2}$ عمود می‌شود و در مقایسه \tilde{M}_1 و \tilde{M}_2 نیاز به $V(\tilde{M}_1 \geq \tilde{M}_2)$ و $V(\tilde{M}_2 \geq \tilde{M}_1)$ پیدا می‌شود.



شکل ۲: درجه بزرگی اعداد فازی

مقیاس‌های معیارهای مختلف به مقیاس قابل مقایسه استفاده می‌شود. بنابراین می‌توان از \tilde{R} ماتریس تصمیمات فازی نرمال شده بدست آورد:

جدول ۲: امتیازات ارزیابی فازی جهت روش TOPSIS فازی

امتیازات فازی	متغیرهای زبانی	علائم اختصاری
(۰ و ۱)	بسیار کم	VP
(۰ و ۱/۳)	کم	P
(۱/۳ و ۱/۵)	نسبتاً کم	MP
(۳/۵ و ۷/۹)	متوسط	F
(۵/۷ و ۹)	نسبتاً زیاد	MG
(۷/۹ و ۱)	زیاد	G
(۹/۱۰ و ۱)	بسیار زیاد	VG

$$\tilde{R} = [\tilde{r}_{ij}]_{m \times n} \quad (20)$$

اگر C مجموعه معیار هزینه و B مجموعه معیار سود باشد آنگاه:

$$\tilde{r} = \left(\frac{a_{ij}}{c_j^*}, \frac{b_{ij}}{c_j^*}, \frac{c_{ij}}{c_j^*} \right), \quad j \in B; \quad (21)$$

$$\tilde{r} = \left(\frac{a_j^-}{c_{ij}}, \frac{a_j^-}{b_{ij}}, \frac{a_j^-}{a_{ij}} \right), \quad j \in C; \quad (22)$$

$$c_j^* = \max_i c_{ij}, \quad \text{if } j \in B \quad (23)$$

$$a_j^- = \min_i a_{ij}, \quad \text{if } j \in C \quad (24)$$

روش نرمال کردن ذکر شده ویژگی دامنه اعداد فازی مثلثی که در بازه $[0,1]$ قرار دارد را حفظ می‌نماید.

برای در نظر گرفتن وزن اهمیت معیارها می‌توان ماتریس نرمال فازی وزنی ایجاد نمود:

$$\tilde{V} = [\tilde{v}_{ij}]_{m \times n}, \quad i = 1, 2, \dots, m, \quad j = 1, 2, \dots, n \quad (25)$$

وقتی که

$$\tilde{v}_{ij} = \tilde{r}_{ij}(\cdot) d(C_j) \quad (26)$$

مقیاسات زوجی با استفاده از جدول ۱ صورت می‌پذیرد. بعد از انجام مقایسات لازم است که درجه سازگاری چک شود، برای اینکار از رویکرد روش ادغام متوسط جهت غیرفازی کردن ماتریس استفاده می‌شود. برای تبدیل عدد فازی $A = (a_1, a_2, a_3)$ به عدد قطعی باید از معادله زیر استفاده نمود:

$$P(\tilde{A}) = A = \left(\frac{a_1 + 4a_2 + a_3}{6} \right) \quad (16)$$

و پس از غیرفازی کردن ارزش‌های داخل ماتریس، درجه سازگاری ماتریس را محاسبه می‌گردد.

۳-۴- TOPSIS فازی:

جهت استفاده از روش TOPSIS در تصمیم‌گیری گروهی فازی، اعداد مثلثی فازی در نظر گرفته شده و فاصله اقلیدسی قطعی بین دو عدد فازی تعریف می‌گردد.

در جدول ۲ متغیرهای زبانی همراه با ارزش‌های فازی معادل مشخص گردیده که کارشناسان می‌توانند جهت ارزیابی معیارها از این متغیرها استفاده نمایند.

اگر گروه تصمیم‌گیرندگان متشکل از K نفر باشند آنگاه داریم:

$$\tilde{x}_{ij} = (\tilde{x}_{ij}^1(+) \tilde{x}_{ij}^2(+) \dots (+) \tilde{x}_{ij}^k) \quad (17)$$

که \tilde{x}_{ij}^k رتبه تصمیم‌گیرنده K ام با توجه به معیار j ام برای مورد i ام می‌باشد.

$$(18)$$

$$D = \begin{matrix} & C_1 & C_2 & \dots & C_n \\ A_1 & \tilde{x}_{11} & \tilde{x}_{12} & \dots & \tilde{x}_{1n} \\ A_2 & \tilde{x}_{21} & \tilde{x}_{22} & \dots & \tilde{x}_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_m & \tilde{x}_{m1} & \tilde{x}_{m2} & \dots & \tilde{x}_{mn} \end{matrix}$$

$$W = [w_1, w_2, \dots, w_j], \quad j=1, 2, \dots, n \quad (19)$$

عدد \tilde{x}_{ij} رتبه مورد A_i با توجه به معیار C_j بوده و w_j وزن این معیار می‌باشد. بجای استفاده از فرمول نرمالیز اعداد فازی، در روش TOPSIS سنتی از تبدیل مقیاس خطی جهت تبدیل

در نهایت با بهره‌گیری از مدل معرفی شده در بخش قبل، ریسک‌های شناسایی و پیش‌بینی شده با استفاده از ابزار FMEA فازی و نظرات خبرگان سامانه ارزیابی و با بکارگیری مدل ترکیبی روش‌های تصمیم‌گیری AHP و TOPSIS، ابتدا اوزان معیارهای ابزار FMEA اندازه‌گیری و در نهایت با محاسبه ضریب نزدیکی هر یک از ریسک‌های شناسایی شده، با توجه به نزدیکی ضرایب به عدد یک ریسک‌ها رتبه‌بندی و اولویت‌بندی می‌شوند.

۴-۱- فرآیندهای اصلی سامانه

فرآیندهای موجود در سامانه اطلاعاتی تحقیقاتی گنج در سه بخش کلی تعریف می‌شوند که این بخش‌ها به ترتیب و توالی فراهم‌آوری اطلاعات، تجزیه و تحلیل اطلاعات و اشاعه اطلاعات تحقیقاتی می‌باشند.

ورودی‌های فرایند فراهم‌آوری در سامانه‌های تحقیقاتی عموماً اطلاعاتی مربوط به پژوهش‌ها پایان‌نامه‌ها و تحقیقات هستند که توسط کاربران بیرونی و درونی در این بخش ثبت می‌گردند و پس از بررسی از صحت و رفع نواقص احتمالی که در مرحله ثبت امکان دارد اتفاق بیفتد خروجی این مرحله به عنوان ورودی فرایند تجزیه و تحلیل اطلاعات استفاده شده و مورد ارزیابی ویرایش و نمایه سازی می‌گردند و در نهایت وارد فرایند نگهداری و اشاعه اطلاعات خواهد شد.

۴-۱-۱- فرایند فراهم‌آوری اطلاعات

فرایند فراهم‌آوری اطلاعات شامل بخش‌های تهیه مدارک و ثبت اطلاعات می‌باشد. در تمامی این زیر بخش‌ها و در تمامی فرآیند-های ذکر شده عملیات کنترل کیفی اجرا خواهد شد تا از صحت و بی‌مشکل بودن اطلاعات در سیستم، اطمینان خاطر کسب شود.

۴-۱-۲- فرایند تجزیه و تحلیل اطلاعات

وظایف فرایند تجزیه و تحلیل اطلاعات شامل ویرایش اطلاعات دریافتی و نمایه‌سازی اطلاعات است. که در بخش نمایه‌سازی در صورت وجود نواقص مربوط به ثبت اطلاعات دوباره به واحد فراهم‌آوری عودت داده می‌شود. سپس در صورت کامل بودن فایل‌های اطلاعات ارقام اطلاعاتی مندرج دقیقاً مورد بررسی قرار

باید مطمئن شد \tilde{v}_{ij} به ازای تمام i و j ها، اعداد مثلثی فازی نرمال مثبت هستند و در محدوده $[0,1]$ قرار دارند و سپس می‌توان حل ایده آل مثبت فازی و ایده آل منفی فازی تعریف نمود:

$$A^* = (\tilde{v}_1^*, \tilde{v}_2^*, \dots, \tilde{v}_n^*) \quad (27)$$

$$A^- = (\tilde{v}_1^-, \tilde{v}_2^-, \dots, \tilde{v}_n^-) \quad (28)$$

وقتی که،

$$\tilde{v}_1^* = (1,1,1) \text{ و } \tilde{v}_1^- = (0,0,0), \quad j = 1,2, \dots, n \quad (29)$$

فاصله هر مورد از A^* و A^- بصورت زیر محاسبه می‌شود:

$$d_i^* = \sum_{j=1}^n d(\tilde{v}_{ij}, \tilde{v}_j^*), \quad i = 1,2, \dots, m \quad (30)$$

$$d_i^- = \sum_{j=1}^n d(\tilde{v}_{ij}, \tilde{v}_j^-), \quad i = 1,2, \dots, m \quad (31)$$

و فاصله دو عدد فازی بصورت ذیل محاسبه می‌گردد:

$$d(\tilde{\rho}, \tilde{\tau}) = \sqrt{\frac{1}{3}[(\rho_1 - \tau_1)^2 + (\rho_2 - \tau_2)^2 + (\rho_3 - \tau_3)^2]} \quad (32)$$

که $\tilde{\rho} = (\rho_1, \rho_2, \rho_3)$ و $\tilde{\tau} = (\tau_1, \tau_2, \tau_3)$ دو عدد فازی مثلثی هستند.

و نهایتاً ضریب نزدیکی بصورت زیر محاسبه می‌گردد:

$$CC_i = \frac{d_i^-}{d_i^* - d_i^-}, \quad i = 1,2, \dots, m \quad (33)$$

موارد A_i با توجه به نزدیکیشان به عدد یک رتبه‌بندی می‌شوند.

۴- تجزیه و تحلیل یافته‌ها

در این بخش ابتدا فرایندهای انتشار اطلاعات در سامانه اطلاعاتی تحقیقاتی برخط گنج و دارایی‌های حوزه نرم افزاری شناسایی و در ادامه با استفاده از جلسات طوفان فکری کارشناسان خیره سامانه، عدم انطباق‌ها و ریسک‌های نرم‌افزاری این سامانه پیش‌بینی و جمع‌بندی می‌گردد.

سرور اصلی: مقالات، رساله‌ها، مشخصات کاربران و داوران، فایل-های پشتیبان، گزارشات، کد نویسی‌ها و...

اینترنت: اطلاعات نمایشی پیش فرض در بخش‌های مختلف، درخواست‌های کاربران، نامه‌های الکترونیکی و...

۴-۲- عدم انطباق‌ها و ریسک‌های شناسایی شده

ریسک‌های نرم‌افزاری شناسایی شده و پیش‌بینی شده توسط کارشناسان خبره سامانه گنج، در سه حوزه دسترسی غیرمجاز به اطلاعات، عدم دسترسی بودن اطلاعات و درست و یکپارچه نبودن اطلاعات به شرح ذیل می‌باشد:

۴-۲-۱- ریسک‌های شناسایی شده حوزه دسترسی غیرمجاز به اطلاعات:

- دسترسی غیرمجاز به گزارشات امنیتی شبکه داخلی سازمان (شامل مکاتبات، نرم افزارها و ...)
- دسترسی غیرمجاز به اطلاعات کارکنان
- دسترسی غیرمجاز به مشاهده یا تغییر اطلاعات ذخیره سرور (مانند گزارشات امنیتی، فایل‌های پشتیبان)
- دسترسی کاربران غیرمجاز به سیستم عامل و نرم افزارهای کاربردی سرور
- دسترسی کاربران غیرمجاز به اطلاعات پایه سایت اینترنتی
- دسترسی کاربران غیرمجاز به ایمیل‌های ارسالی و دریافتی کاربران
- دسترسی کاربران غیرمجاز به فایل تمام متن پایان‌نامه / رساله

۴-۲-۲- ریسک‌های شناسایی شده در حوزه عدم دسترسی بودن اطلاعات:

- عدم دسترسی کاربران مجاز به نرم‌افزارها و گزارشات امنیتی شبکه داخلی
- عدم دسترسی کاربران مجاز طبق طبقه بندی مشخص شده جهت مشاهده یا تغییر اطلاعات پایگاه داده، گزارشات امنیتی، فایل‌های پشتیبان، نرم‌افزارهای کاربردی و ...
- عدم دسترسی کاربران مجاز به اطلاعات پایه، گزارشات امنیتی، ایمیل‌های مرتبط با سایت اینترنتی
- عدم دسترسی کاربران مجاز به مقاله‌ها / رساله‌های دسترسی محدود

گرفته و کامل می‌گردد. باتوجه به اینکه اطلاعات وارد شده در این بخش قبلاً توسط کاربران ثبت گردیده است لازم است کلیه نواقص در این مرحله مرتفع گردد. همچنین کلیدواژه‌های مولف بررسی و کنترل می‌گردد و در صورت لزوم اصلاحات مقتضی صورت خواهد پذیرفت. در بخش ویراستاری به بررسی کلی اطلاعات کتاب-شناختی و کلیدواژه‌ها پرداخته خواهد شد و در صورت فاقد مشکل بودن مدرک تایید شده و اشاعه داده می‌شود.

۴-۱-۳- فرایند اشاعه اطلاعات تحقیقاتی

همانطور که گفته شد این بخش وظیفه نگهداری و اشاعه اطلاعات را برعهده دارد اما با توجه به این که در این بخش از اطلاعات خروجی بخش‌های قبلی استفاده می‌شود در صورت وجود و شناسایی مشکلات کیفی این اطلاعات مجدداً به واحد تجزیه و تحلیل اطلاعات عودت داده می‌شود.

۴-۳- شناسایی دارایی‌ها و ریسک‌های نرم‌افزاری

ساختار نرم‌افزاری سازمان‌های اطلاعاتی تحقیقاتی برخط شامل بخش‌های زیر می‌باشد:

شبکه داخلی: سیستم‌عامل‌ها ، وپروس‌یاب‌ها ، فایروال‌ها ، نرم-افزارهای کاربردی

سرور اصلی: سیستم‌عامل ، وپروس‌یاب‌ها ، فایروال‌ها ، نرم‌افزار Database ، نرم‌افزارهای کاربردی

اینترنت: نرم‌افزار Interface ، وپروس‌یاب‌ها ، نرم‌افزارهای کاربردی ، پست‌الکترونیکی

با توجه به بخش‌های مختلف اینگونه سازمان‌ها، دارایی‌های مرتبط با بخش‌های نرم‌افزاری بصورت زیر می‌باشند:

شبکه داخلی: مکاتبات داخلی، محاسبات مالی، فایل‌های پشتیبان، برنامه ریزی داورها، گزارشات، مشخصات کارمندان و داوران و...

۴-۲-۳- ریسک‌های شناسایی شده در حوزه درست و یکپارچه نبودن اطلاعات:

- ناقص بودن و یا بهم ریخته بودن مکاتبات داخل سازمانی
- ناقص بودن یا صحیح نبودن و یا بهم ریخته بودن ایمیل‌های دریافتی یا ارسالی کاربران
- ناقص بودن یا صحیح نبودن نتایج عملیات کاربر در سایت اینترنتی
- عدم ثبت نام کاربر در سایت
- ناقص بودن و یا بهم ریخته بودن مقالات ارسالی کاربران

۴-۳- نتایج حاصل از اجرای مدل پیشنهادی

در ادامه به کمک تکنیک FMEA ریسک‌های شناسایی شده با نظرسنجی از خبرگان در سه معیار شدت اثر، احتمال وقوع و احتمال شناسایی و با استفاده از اعداد فازی معرفی شده در بخش قبل، مورد بررسی و ارزیابی قرار گرفت. جدول (۳) نتایج جمع‌آوری شده در این خصوص را نمایش می‌دهد.

جدول ۳: امتیازات خبرگان به ریسک‌ها با توجه به سه معیار روش FMEA

ریسک	شدت اثر	احتمال وقوع	احتمال شناسایی
دسترسی غیر مجاز به گزارشات امنیتی شبکه داخلی سازمان (شامل مکاتبات، نرم افزارهاو...)	MP,MG,M G,MG,G,G, G,VG,VG	VP,P,MP, MP,F,F,M G,G,G	VG,G,MG, F,MP,P,P P,VP
دسترسی غیرمجاز به اطلاعات کارکنان	P,F,F,MG, MG,MG,M G,G,G	P,P,P,MP, F,F,MG,G, VG	G,G,MG, F,F,F,MP, P,P
دسترسی غیر مجاز به مشاهده یا تغییر اطلاعات ذخیره سرور (مانند گزارشات امنیتی، فایل‌های پشتیبان)	MP,MG,G, G,G,G,VG, VG,VG	P,P,P,P,M P,MP,MP, MP,F	G,G,MG, F,MP,MP, P,P,P
دسترسی کاربران غیر مجاز به سیستم عامل و نرم افزار های کاربردی سرور	VP,P,F,F,G G,G,G,VG	VP,VP,P,F, F,F,MG,M G,G	G,G,MG, G,MG,M G,MG,F, MP

ریسک	شدت اثر	احتمال وقوع	احتمال شناسایی
دسترسی کاربران غیرمجاز به اطلاعات پایه سایت اینترنتی	VP,MP,MP F,MG,G,G .G,G	VP,P,P,M P,F,F,G,V G,VG	VG,G,G, G,MG,MP ,MP,P,P
دسترسی کاربران غیرمجاز به ایمیل های ارسالی و دریافتی کاربران	MP,MP,MP ,MG,G,G,G ,G,VG	VP,VP,P, MP,F,MG, G,G,G	G,MG,M G,MP,P,P, P,P,VP
عدم دسترسی کاربران مجاز به نرم افزار ها و گزارشات امنیتی شبکه داخلی	VP,P,F,MG ,MG,MG, MG,G,G	VP,P,MP, MP,F,MG, MG,G,G	VG,VG,V G,VG,G, G,G,MP, MP
عدم دسترسی کاربران مجاز طبق طبقه بندی مشخص شده جهت مشاهده یا تغییر اطلاعات پایگاه داده، گزارشات امنیتی، فایل‌های پشتیبان، نرم افزارهای کاربردی و ...	P,MP,MP,F ,MG,G,G,G ,VG	VP,VP,P, MP,F,F,M G,G,G	VG,VG,G ,G,MG,M G,MG,F,P
عدم دسترسی کاربران مجاز به اطلاعات پایه، گزارشات امنیتی، ایمیل‌های مرتبط با سایت اینترنتی	VP,MP,F,F, F,MG,MG, G,G	P,P,MP,M P,MP,MG, MG,G,G	VG,VG,G ,G,MG,M G,F,F,MP
ناقص بودن و یا بهم ریخته بودن مکاتبات داخل سازمانی	VP,P,P,F,F, MG,MG,G, VG	P,MP,MP, MP,F,MG, G,G,G	VG,VG,G ,G,MG,M G,MG,F, MP
ناقص بودن یا صحیح نبودن و یا بهم ریخته بودن ایمیل های دریافتی یا ارسالی کاربران	P,MP,MP,F ,F,MG,G, G	VP,MP,M P,MP,MP, F,MG,G,G	VG,VG,G ,G,G,MG, MG,F,MP
ناقص بودن یا صحیح نبودن نتایج عملیات کاربر در سایت اینترنتی	VP,MP,MP ,MP,MP,M P,F,MG,G	VP,P,MP, MP,MP,F, MG,MG, MG	G,G,G,G, G,MG,F,P ,P
عدم ثبت نام کاربر در سایت	VP,VP,P,F, F,F,MG,M G,G	VP,MP,M P,F,MG,G, G,G,VG	VG,G,G, G,MG,M G,MG,F, MP

ردیف	ریسک	ضریب نزدیکی	اولویت
	داخلی سازمان (شامل مکاتبات، نرم افزارها...)		
۲	دسترسی غیرمجاز به اطلاعات کارکنان	۰,۳۰	۹
۳	دسترسی غیر مجاز به مشاهده یا تغییر اطلاعات ذخیره سرور (مانند گزارشات امنیتی، فایل‌های پشتیبان)	۰,۴۴	۱
۴	دسترسی کاربران غیر مجاز به سیستم عامل و نرم افزارهای کاربردی سرور	۰,۳۵	۵
۵	دسترسی کاربران غیرمجاز به اطلاعات پایه سایت اینترنتی	۰,۲۸	۱۲
۶	دسترسی کاربران غیرمجاز به ایمیل‌های ارسالی و دریافتی کاربران	۰,۳۶	۴
۷	عدم دسترسی کاربران مجاز به نرم افزارها و گزارشات امنیتی شبکه داخلی	۰,۳۰	۱۰
۸	عدم دسترسی کاربران مجاز طبق طبقه بندی مشخص شده جهت مشاهده یا تغییر اطلاعات پایگاه داده، گزارشات امنیتی، فایل‌های پشتیبان، نرم افزارهای کاربردی و ...	۰,۲۷	۱۳
۹	عدم دسترسی کاربران مجاز به اطلاعات پایه، گزارشات امنیتی، ایمیل‌های مرتبط با سایت اینترنتی	۰,۳۰	۱۱
۱۰	ناقص بودن و یا بهم ریخته بودن مکاتبات داخل سازمانی	۰,۳۳	۶
۱۱	ناقص بودن یا صحیح نبودن و یا بهم ریخته بودن ایمیل‌های دریافتی یا ارسالی کاربران	۰,۳۲	۸

ریسک	شدت اثر	احتمال وقوع	احتمال شناسایی
ناقص بودن و یا بهم ریخته بودن مقالات ارسالی کاربران	P,P,F,F,MG .G,G,VG,V G	VP,P,MP, MP,F,F,M G,G,VG	VG,VG,G .G,MG,M G,MG,M G,MP

سپس بمنظور تعیین درجه اهمیت هر یک از سه مشخصه شدت اثر، احتمال وقوع و احتمال شناسایی وزن نسبی معیارها با توجه به نظر کارشناسان تعیین گردید، که در جدول (۴) نتایج حاصل قابل مشاهده است. رویکرد مورد استفاده در این خصوص روش AHP فازی بوده است که در بخش قبلی به آن اشاره گردید.

جدول ۴: وزن اهمیت معیارهای روش FMEA

شدت اثر	احتمال وقوع	احتمال شناسایی	شدت اثر
-	VW.FW,E, E,E,SS,SS, FS,VS	FW.FW,E,SS, SS,FS,FS,VS, VS	شدت اثر
-	-	AW,AW,E,E, SS,FS,FS,VS, VS	احتمال وقوع
-	-	-	احتمال شناسایی
۰,۳۸	۰,۴۰	۰,۲۲	وزن های حاصل شده

در نهایت ضریب نزدیکی ریسک‌ها با استفاده از روش TOPSIS فازی و اعمال اوزان اهمیت جدول (۴)، تعیین و سپس ریسک‌های شناسایی شده سامانه اطلاعاتی تحقیقاتی بر خط گنج بر اساس فاصله ضریب نزدیکی تا عدد یک، اولویت‌بندی گردیدند (جدول ۵).

جدول ۵: ضریب نزدیکی ریسک‌ها و اولویت بندی آنها

ردیف	ریسک	ضریب نزدیکی	اولویت
۱	دسترسی غیر مجاز به گزارشات امنیتی شبکه	۰,۳۲	۷

رویکرد Fuzzy FMEA برای تشخیص، ارزیابی و رتبه‌بندی ریسک‌ها در کلیه سامانه‌های اطلاعاتی (اعم از تحقیقاتی و غیره) و با بکارگیری دیگر ابزارهای ارزیابی ریسک می‌تواند مورد استفاده قرار گرفته و به بهبود امنیت اطلاعاتی کمک شایانی نماید.

مراجع

- [1] T. Yuan and P. Chen, "International Workshop on Information and Electronics Engineering Data Mining Applications in E-Government Information Security," *Procedia Engineering*, vol. 29, pp. 235-240, 2012.
- [2] D. Feledi, S. Fenz, and L. Lechner, "Toward web-based information security knowledge sharing," *Information Security Technical Report*, vol. 17, no. 4, pp. 199-209, 2013.
- [3] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," *Computers & Security*, vol. 32, pp. 90-101, 2013.
- [4] S. A. Chaharsoughi, M. A. Doustari, A. Y. Varjani, A. M. Ardestani, "Application of artificial neural networks in assessing information security risk," *Journal Of Electronical & Cyber Defence*, vol. 1, no. 4, pp. 23-33, 2014 (In Persian).
- [5] M. S. Saleh, and A. Alfantookh, "A new comprehensive framework for enterprise information security risk management," *Applied Computing and Informatics*, vol. 9, no. 2, pp. 107-118, 2011.
- [6] Liu, Hu-Chen, Liu, Lang, and Liu, Nan" Risk evaluation approaches in failure mode and effects analysis: A literature review," *Expert Systems with Applications*, vol. 40, no. 2, pp. 828-838, 2013.
- [7] J. S. Broderick, "ISMS, security standards and security regulations," *Information Security Technical Report*, vol. 11, no. 1, pp. 26-31, 2006.
- [8] J. I. Fernando, and L. L. Dawson, "The health information system security threat lifecycle: An informatics theory," *International Journal of Medical Informatics*, vol. 78, no. 12, pp. 815-826, 2009.
- [9] G. Wei, X. Xiang, X. Zhang, and Z. Huang, "Research on E-government Information Security Risk Assessment - Based on Fuzzy AHP and Artificial Neural Network Model," Paper presented at 2010 First International Conference on Networking and Distributed Computing (ICNDC).
- [10] Y.-P. Ou Yang, H.-M. Shieh, and G.-H. Tzeng, "A VIKOR technique based on DEMATEL and ANP for information security risk control assessment," *Information Sciences*, vol. 232, pp.482-500, 2013.
- [11] M. M. Silva, A. P. H. de Gusmão, T. Poletto., L. C. e. Silva, and A. P. C. S. Costa, "A multidimensional approach to information security risk management using FMEA and fuzzy theory," *International Journal of Information Management*, vol. 34, no. 6, pp. 733-740, 2014.
- [12] N. Feng, H. J. Wang, and M. Li, "A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis," *Information Sciences*, vol. 256, pp. 57-73, 2014.

ردیف	ریسک	ضریب نزدیکی	اولویت
۱۲	ناقص بودن یا صحیح نبودن نتایج عملیات کاربر در سایت اینترنتی	۰,۳۸	۲
۱۳	عدم ثبت نام کاربر در سایت	۰,۳۸	۳
۱۴	ناقص بودن و یا بهم ریخته بودن مقالات ارسالی کاربران	۰,۲۶	۱۴

رتبه‌بندی فوق نشان می‌دهد ریسک‌های پیش‌بینی شده مربوط به حوزه‌های دسترسی غیرمجاز به اطلاعات و در دست و یکپارچه نبودن اطلاعات از نظر کارشناسان خبره این سازمان در اولویت بالاتری قرار دارد.

جهت کاهش خطرات آتی در خصوص عملکرد این سامانه لازم است، کاهش، حذف و یا انتقال ۱۴ ریسک شناسایی شده مطابق اولویت مشخص شده برنامه‌ریزی و در این راستا اقدامات اصلاحی و پیشگیرانه مورد نیاز را پیش‌بینی نمود.

۵- نتیجه گیری

مطالعه حاضر با هدف شناسایی و ارزیابی ریسک‌های نرم‌افزاری امنیت اطلاعات سامانه اطلاعاتی تحقیقاتی برخط گنج مورد مطالعه صورت گرفته است. در این پژوهش با استفاده جلسات طوفان فکری حالات شکست بالقوه نرم‌افزاری این سامانه شناسایی و با بهره‌گیری از روش FMEA فازی و کارشناسان خبره این سازمان ارزیابی شده و سپس جهت کاهش کاستی‌های روش FMEA سنتی با استفاده از روش AHP فازی و TOPSIS فازی معیارها و وزن‌دهی رتبه‌بندی گردیده‌اند. نتایج حاصل جهت بهبود وضعیت امنیت اطلاعات سازمان باید در اولویت مدیریت قرار گرفته و با پیش‌بینی اقدامات اصلاحی و پیشگیرانه مناسب احتمال وقوع عدم انطباق‌های مورد نظر را کاهش دهند.

باوجود اینکه مطالعه حاضر در خصوص ریسک‌های نرم‌افزاری امنیت اطلاعات صورت گرفته است اما می‌توان در ادامه در مورد ارزیابی سایر حوزه‌های ریسک‌های امنیت اطلاعات اینگونه سازمان‌ها با استفاده از دیگر ابزارهای نوین انجام پذیرد.

- [20] A. C. Kutlu, and M. Ekmekçiöğlü, "Fuzzy failure modes and effects analysis by using fuzzy TOPSIS-based fuzzy AHP," *Expert Systems with Applications*, vol. 39, no. 1, pp. 61-67, 2012.
- [21] Chang, K.-H., Chang, Y.-C., & Lee, Y.-T. "Integrating TOPSIS and DEMATEL Methods to Rank the Risk of Failure of FMEA," *International Journal of Information Technology & Decision Making*, vol. 13, no. 06, pp. 1229-1257, 2014.
- [22] Kumru, Mesut, and Kumru, Pinar, Yıldiz. "Fuzzy FMEA application to improve purchasing process in a public hospital," *Applied Soft Computing*, vol. 13, no. 1, pp. 721-733, 2013.
- [23] Deng, X., & Jiang, W., "Fuzzy risk evaluation in failure mode and effects analysis using a D numbers based multi-sensor information fusion method", *Sensors*, vol.17, no.9, pp. 1-17, 2017.
- [24] L. A. Zadeh, "Fuzzy logic: computing with words," *IEEE Transactions on Fuzzy Systems*, vol. 4, no. 2, pp.103-111, 1996.
- [25] D. Y. Chang, "Applications of the extent analysis method on fuzzy AHP," *European Journal of Operational Research*, vol. 95, no. 3, pp. 649-655, 1996.
- [13] Mendonça Silva, M., Poletto, T., Camara e Silva, L., Henriques de Gusmao, A. P., & Cabral Seixas Costa, A. P. , "A Grey Theory Based Approach to Big Data Risk Management Using FMEA", *Mathematical Problems in Engineering*, 2016.
- [14] De Gusmão, A. P. H., e Silva, L. C., Silva, M. M., Poletto, T., & Costa, A. P. C. S. "Information security risk analysis model using fuzzy decision theory", *International Journal of Information Management*, vol. 36, no. 1, pp.25-34, 2016.
- [15] Amini, A., Jamil, N., Ahmad, A. R., & Sulaiman, H, "A Fuzzy Logic Based Risk Assessment Approach for Evaluating and Prioritizing Risks in Cloud Computing Environment ", In *International Conference of Reliable Information and Communication Technology*, pp. 650-659, 2017.
- [16] Chanamool, N., & Naenna, T. "Fuzzy FMEA application to improve decision-making process in an emergency department", *Applied Soft Computing*, vol. 43, pp. 441-453, 2016.
- [17] M. Abdelgawad, and A. Fayek, "Risk Management in the Construction Industry Using Combined Fuzzy FMEA and Fuzzy AHP," *Journal of Construction Engineering and Management*, vol. 136, no. 9, pp. 1028-1036, 2010.
- [18] Fattahi, R., & Khalilzadeh, M., "Risk evaluation using a novel hybrid method based on FMEA, extended MULTIMOORA, and AHP methods under fuzzy environment", *Safety Science*, vol. 102, pp. 290-300, 2018.
- [19] Selim, H., Yunusoglu, M. G., & Yılmaz Balaman, Ş., "A dynamic maintenance planning framework based on fuzzy TOPSIS and FMEA: application in an international food company", *Quality and Reliability Engineering International*, vol. 32, no. 3, pp. 795-804, 2016.