مجله علمی پژوهشی «علوم و فناوری‌های پدافند غیرعامل»
سال چهارم، شماره ۴، زمستان ۱۳۹۲؛ ص ۲۹۲-۲۸۵

الگوی ارزیابی آسیب‌پذیری بنادر با استفاده از تلفیق روش فازی و رمکپ

جلال محمدی باغملایی[۱]، حبیب ا.. سهامی[۲*]

۱- کارشناس ارشد پدافند غیرعامل، مدیریت بحران و پدافند غیرعامل اداره کل بنادر و دریانوردی استان بوشهر

۲- استادیار دانشگاه صنعتی مالک اشتر

(دریافت: ۱۳۹۲/۰۵/۱۴، پذیرش: ۱۳۹۲/۱۱/۱۵)

چکیده

یک حمله مؤثر بر علیه زیرساخت‌های دریایی حیاتی این پتانسیل را دارد که موجب اختلالات و آسیب‌های اقتصادی گسترده در سطح ملی گردد. با توجه به درک اهمیت ارزش حیاتی بنادر، برای جلوگیری از حملات احتمالی دشمنان خارجی می‌بایست نقاط آسیب‌پذیر بنادر را شناسایی و هرچه سریع‌تر در جهت ترمیم و یا تقویت آن نقاط، اقدامات لازم را به مرحله اجرا درآورد. بنابراین، در تحقیق حاضر سعی شده یک الگوی کارآمد و مؤثر با هدف ارزیابی آسیب‌پذیری بنادر با رویکرد پدافند غیرعامل جهت استفاده سایر بنادر کشور ارائه شود. این مقاله بر آن است تا یک روش ارزیابی آسیب‌پذیری زیرساخت‌ها و شریان‌های حیاتی را که محصول ترکیب و بومی‌سازی روش‌های بررسی شده در زمینه ارزیابی آسیب‌پذیری است، معرفی نماید. این روش که تحت عنوان روش رمکپ یاد می‌شود، سامانه‌ای بر مبنای ارزیابی خطرپذیری به‌صورت تابعی از تهدید، آسیب‌پذیری و اثرات می‌باشد. در این روش به‌دلیل ویژگی‌های ماهیتی ریسک، از روش فازی برای نمونه‌سازی ارزیابی آسیب‌پذیری استفاده شده و در نهایت، نتایج در قالب نرم‌افزار MATLAB ارائه شده است.

کلید واژه‌ها: ارزیابی آسیب‌پذیری، امنیت بنادر، تهدیدات، دارایی‌ها، نمونه رمکپ.

Vulnerability Assessments' Pattern Using Combined Fuzzy and RAMCAP Approaches

J. Mohammadi Baghmollaei, H. Sahami*

Malek Ashtar University of Technology

(Received: 05/08/2013; Accepted: 04/02/2014)

Abstract

A successful attack against vital maritime infrastructures has the potential to cause major economic disruption and create mass casualties and conflagration at national levels. Taking into considerations the vital importance of the seaports, the vulnerable points in the seaports must be recognized and necessary steps should be implemented in order to prevent potential adversary's attacks. Therefore, a coordinated pattern is provided in this investigation to identify the vulnerabilities and provide security of the ports, through the identification of the assets and the ongoing threats based on passive defence considerations. In this article, attempts have been made to introduce a critical infrastructures' vulnerability assessment method which is the product of combined local and current methods such as RAMCAP. This method is based on risk assessment as a function of threat, vulnerability and effects where assets, threats and vulnerabilities are estimated and security measures are implemented. Therefore, Fuzzy method is used to model the vulnerability assessment and the results are presented through MATLAB software.

Keywords: Vulnerability Assessment, Seaport Security, Threats, Assets, RAMCAP.

* Corresponding Author E-mail: HSahami15@gmail.com

۱. مقدمه

موقعیت ژئوراهبردی کشور ما، به‌ویژه برخورداری از سواحل طولانی در مجاورت حیاتی‌ترین شاهرگ اقتصادی دنیا (خلیج فارس)، از نظر اقتصادی و راهبردی، ایران را به‌عنوان یک کشور وابسته به سواحل و بنادر تبدیل نموده است. بدیهی است یک حمله تهاجمی علیه زیرساخت‌های دریایی در بنادر ما، می‌تواند سبب اختلال عظیمی در اقتصاد کشور شود و حجم عظیمی از تلفات، خسارات و به‌طبع آن بحران بزرگی را برجای گذارد [۱].

با توجه به وجود بیش از ۶۵۰۰ کیلومتر مرز دریایی با کشورهای همسایه و احتمال استفاده از خاک این کشورها برای حمله به کشورمان، به‌نظر می‌رسد که می‌بایست توجه ویژه‌ای به دارایی‌های بنادر و آسیب‌پذیری‌های آنها داشت [۲]. به‌عنوان مثال، از جمله نقاط آسیب‌پذیر بنادر می‌توان به محدوده کانال دسترسی، اسکله‌های نفتی، ساختمان برج کنترل و مخابرات دریایی و غیره اشاره کرد که این نقاط آسیب‌پذیر با استفاده از شناسایی و ارزش‌گذاری دارایی‌ها، نوع تهدیدات موجود و اقدامات جبرانی مؤثر جهت کاهش آسیب‌پذیری‌ها شناسایی و اولویت‌بندی می‌شوند که این مسئله را می‌توان با یک الگوی ارزیابی آسیب‌پذیری بنادر به‌دست آورد. از طرف دیگر با توجه به کارایی بالای روش فازی در نمونه نمودن عدم اطمینان که جزء جدایی‌ناپذیر ارزیابی ریسک می‌باشد، مطالعات زیادی در این زمینه با استفاده از روش فازی صورت گرفته و به‌وسیله مطالعات مختلف، این کارایی اثبات شده است.

در تحقیق حاضر سعی می‌شود موضوع حفاظت از بنادر و زیرساخت‌های دریایی در برابر تهدیدات نامتقارن جدید مورد بررسی قرار گرفته و ضمن ارائه الگویی مناسب جهت ارزیابی آسیب‌پذیری بنادر، بر اساس جستجوهای علمی توصیه و راهکارهای ارزشمندی در تعیین نحوه دفاع از بنادر خودی در این عصر پیشرفته با تأکید بر اصول دفاع غیرعامل ارائه شود. بنابراین، در این تحقیق سعی شده با استفاده از منطق فازی و در قالب روش معتبر، به ارزیابی ریسک امنیتی پرداخته شود. طرح تحقیقاتی حاضر نیز با تکیه بر همین ضرورت‌ها، سعی در معرفی و بومی‌سازی یکی از روش‌های کاهش آسیب‌پذیری امنیتی زیرساخت‌های حیاتی تحت محیط فازی را دارد. هدف از انجام این تحقیق، بیان و اجرای یک روش ارزیابی آسیب‌پذیری امنیتی و خطرپذیری (ریسک) ناشی از آن در حوزه زیرساخت‌های حیاتی نظیر بنادر، به‌عنوان شاهرگ حیات اقتصاد ملی و ارائه روش‌های کاهش این نوع آسیب‌پذیری‌ها با به‌کارگیری اقدامات بازدارندگی، آشکارسازی، به تأخیراندازی و واکنشی همراه با تجهیزات مناسب و مقرون به‌صرفه، متناسب با نیازها و فعالیت‌های امروزی و آینده این دسته از سرمایه‌های ملی است. این هدف کلان به اهداف خردتر زیر تقسیم می‌شود:

- بررسی روش‌های سنتی کاهش خطرپذیری امنیتی (آشنایی با مفهوم آسیب‌پذیری‌های امنیتی و خطرپذیری ناشی از آن).
- اجرای روش‌های مؤثر در برطرف‌کردن آسیب‌پذیری‌های بنادر.

سؤال‌های تحقیق عبارتند از:

- چه الگویی را جهت ارزیابی آسیب‌پذیری بنادر جنوب خلیج فارس می‌توان پیشنهاد داد؟
- آیا نمونه فازی قادر به حل مشکلات مرتبط با عدم یقین موجود در نمونه‌سازی می‌باشد و نتایج روش فازی قابل اطمینان است؟

با توجه به سؤال‌های تحقیق، فرضیات آن [۳] عبارتند از:

- یکی از روش‌های ارزیابی تهدیدات در بنادر، استفاده از نمونه ارزیابی ریسک امنیتی با استفاده از روش تلفیقی و ترکیبی از روش فازی و رمکپ است.
- سامانه‌های فازی، ابزار مناسبی است برای نمونه‌سازی عدم اطمینان ناشی از نبود اطلاعات و یا جایی که داده‌ها قابل اندازه‌گیری نیستند.

۲. پیشینه تحقیق

با وجود آنکه در مورد اهمیت بنادر و نقش تأثیرگذاری که در ارتباط با اقتصاد و توسعه کشور دارد کارشناسان مختلفی گزارش‌های تحقیقی مبسوطی ارائه نموده‌اند و همچنین در مورد ایمنی بنادر و راه‌های مقابله با شرایط اضطرار، مطالب متنوع و راهکارهای گوناگونی ارائه شده است [۴] ولی با توجه به موضوع تحقیق که نگاهی موشکافانه به بحث ارزیابی تهدیدات و آسیب‌پذیری بنادر دارد، گزارش‌ها و مطالب بسیار اندکی در این حوزه تحقیقاتی درخصوص توجه به زیرساخت‌های بنادر، بدون ارائه هیچ‌گونه الگو و راه‌حلی موجود می‌باشد. لازم به‌ذکر است که حادثه حملات ۱۱ سپتامبر، آمریکایی‌ها را واداشت تا آسیب‌پذیری بنادر خود را در صورت وقوع حوادث خراب‌کاری ارزیابی و تحلیل کنند. در این حوزه، به‌تازگی گزارش‌های تحلیلی موجود است که می‌تواند تا حدودی رهیافت مناسبی برای ارزیابی آسیب‌پذیری بنادر را پیش روی نگارنده قرار دهد [۸-۵]. اما نکته قابل تأمل آن است که راهبرد جمهوری اسلامی در ایمن‌سازی و مقابله با تهدیدات در نوع خود، می‌بایست بومی باشد و بر اساس اصول پدافند غیرعامل مورد بررسی و تجزیه و تحلیل قرار گیرد که در این خصوص، گزارش‌های اندکی آن هم در مورد تحلیل آسیب‌پذیری و بهسازی لرزه‌ای ساختمان‌ها وجود دارد که ویژه بنادر نمی‌باشد و در مجموع هیچ‌گونه گزارش مستندی یافت نمی‌شود.

بنابراین مجموعه مستندات و گزارش‌های علمی و تحقیقی که با عنوان ارزیابی و مدیریت ریسک توسط مؤسسه FEMA به‌ویژه بعد از وقوع حوادث ۱۱ سپتامبر منتشر شد، عمدتاً شامل نکات تحلیلی - علمی و دستورالعمل‌هایی در حوزه طراحی زیر ساخت‌های حیاتی و مراکز مهم درون‌شهری و سازه‌ها در برابر تهدیدات تروریستی می باشد [۹]. در این مجموعه‌های مستند و علمی، روش‌های ارزیابی تهدیدات، تحلیل ریسک، تعیین تهدید مبنا و طراحی امنیتی بر اساس تهدید مبنا برای انواع مختلف کاربری‌ها بیان شده است، اما حوزه شمول تهدیدات آنها با تهدیدات متصور برای کشور ما متفاوت بوده و

تنها جوابگوی نیازهای نوع خاصی از تهدیدات است که همان پدیده تروریسم می‌باشد [۱۰]. از آنجا که تاکنون طرح‌های ارائه شده در حوزه زیرساخت‌های حیاتی کشور همچون بنادر، پالایشگاه‌ها، سدها، نیروگاه‌ها و غیره با رویکرد ایمنی صورت گرفته‌اند، به‌نظر می‌رسد طرح حاضر که در پی ارزیابی آسیب‌پذیری‌های امنیتی و کاهش خطرپذیری‌های ناشی از آنها است، بدیع و نوآورانه باشد. از طرفی با توجه به عدم اطمینان موجود در جمع‌آوری داده‌ها و تصمیم‌گیری، استفاده از منطق فازی می‌تواند مفید باشد. یکی از روش‌های ارزیابی تهدیدات، استفاده از نمونه‌ای است که تهدیدات علیه زیرساخت‌های حیاتی را تحلیل و مدیریت می‌کند. در این تحقیق نگارنده از نمونه موسوم بهرمکپ[1] یا مدیریت و تجزیه و تحلیل خطرپذیری برای حفاظت از دارایی‌های حیاتی استفاده نموده است. در این نمونه، ارزیابی تهدیدات و ریسک خطرها در زیرساخت‌های حیاتی شامل روش‌های تشخیص، تحلیل، سنجش و ارتباطات، میان ویژگی‌هایی است که مهاجم را به سمت هدف خاصی سوق می‌دهد [۱۱]. علاوه بر این، راه‌های تشخیص نقاط آسیب‌پذیر و ارزیابی گزینه‌های موجود برای بهبود آنها نیز ارائه می‌شود. با توجه به اینکه یکی از اقدامات مهم در هر سازمانی، بررسی روش‌های ارزیابی ریسک، انتخاب و بومی‌سازی روش‌های مناسب جهت اجرا است، تحقیق حاضر بر آن است تا یک روش ارزیابی امنیتی مناسب با ساختار فازی را که محصول ترکیب روش‌های بررسی شده است، معرفی نماید. این روش سامانه‌ای است بر مبنای ارزیابی خطرپذیری ناشی از عملیات خصمانه به‌صورت تابعی از پیامد و احتمال که در نهایت پس از ارزیابی دارایی‌ها، تهدیدها و آسیب‌پذیری‌ها، اقدامات امنیتی همراه با تجهیزات مورد نیاز اجرا می‌گردند. در این سامانه، می‌توان دارایی‌ها را هم به‌صورت کلی و هم به‌صورت جزئی مورد بررسی قرار داد.

ارزیابی تهدیدها و ریسک خطرها در زیرساخت‌های حیاتی شامل هفت مرحله می‌باشد که شامل موارد زیر است [۱۲]:

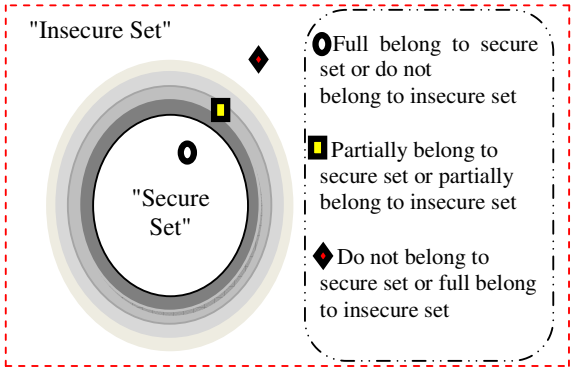
- توصیف و غربال سرمایه و دارایی‌های حیاتی
- توصیف تهدید
- تحلیل رخداد
- تحلیل آسیب‌پذیری
- ارزیابی جذابیت‌های سرمایه و دارایی زیرساختی و تهدیدات
- ارزیابی ریسک خطر
- مدیریت خطر (ریسک)

ارزیابی تهدیدات و ریسک خطرات براساس این فرضیه که سرمایه‌های موجود در همه بخش‌ها ممکن است مورد هدف دشمن قرار گیرند عمل نمی‌کند، به این دلیل که ارزیابی دقیق همه این سرمایه‌ها عملاً کاری غیر ممکن است. هدف ارزیابی تهدیدات و ریسک خطرات در زیر ساخت‌های ملی شناسایی و بررسی سرمایه‌های ملی در نقاط بحرانی و حیاتی است [۱۳].

[1] Risk Analysis and Management for Critical Asset Protection

۳. تجزیه و تحلیل داده‌ها بر اساس منطق فازی

منطق فازی که یکی از ابزارهای مهم در نمونه‌سازی عدم یقین موجود در مسائل مهندسی و علوم می‌باشد، به‌جای استفاده از دو عبارت کاملاً صحیح و کاملاً غلط از یک رنجی از اعداد بین صفر و یک استفاده می‌کند [۱۴]. این توانایی سامانه‌های فازی سبب شده تا این ابزار به‌عنوان یکی از مهم‌ترین ابزارهای نمونه‌سازی مورد استفاده قرار گیرد (شکل ۱).



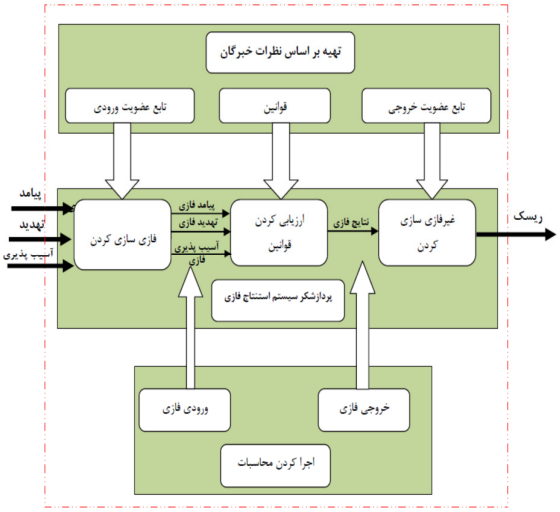
شکل ۱. نمایش گرافیکی ریسک امنیتی فازی [۱۴]

برای طراحی سیستم استنتاج فازی باید چهار ساختار شبکه یعنی: فازی‌ساز، پایگاه قواعد فازی، موتور استنتاج فازی و غیر فازی‌ساز، طراحی و ساخته شوند [۱۵]. برای این منظور، با استفاده از نرم‌افزار متلب به ساخت پایگاه دانش بر اساس قوانین اگر ... آنگاه ... با استفاده از نظرات خبرگان پرداخته شده است. در این تحقیق با توجه به ساختار مسئله مورد بررسی برای ارزیابی و مدیریت، ریسک امنیتی از نوع ممدانی می‌باشد که یکی از پرکاربردترین روش‌های استفاده شده در ایجاد سیستم استنتاج بوده است [۱۶].

اولین مرحله در ساخت نمونه تعیین متغیرهای ورودی برای پیدا کردن رابطه بین این ورودی‌ها و خروجی مورد نظر که در اینجا ریسک امنیتی می‌باشد، باید صورت پذیرد. با توجه به روش رمکپ که از سه معیار اصلی پیامد، آسیب‌پذیری و تهدید برای به‌دست آوردن ریسک استفاده می‌نماید. بنابراین، در این تحقیق همه معیارهای پیامد، آسیب‌پذیری، تهدید و ریسک به‌صورت فازی ارائه شده‌اند. شکل (۲) روند به‌دست آوردن ریسک با استفاده از روش به‌کار رفته در تحقیق را نشان می‌دهد.

ساختار کلی ورودی- خروجی سامانه استنتاج مورد استفاده قرار گرفته در این تحقیق در شکل (۳) نمایش داده شده است. تابع عضویت هر یک از پارامترهای آسیب‌پذیری، تهدید و ریسک با توجه به روش رمکپ شامل ۵ تابع عضویت با مقادیر زبانی خیلی کم (VL)، کم (L)، متوسط (M)، بالا (H) و خیلی بالا (VH) درنظر گرفته شده است. در حالی که توابع عضویت برای پارامتر پیامد شامل ۵ تابع

عضویت با مقادیر زبانی ناچیز (N)، کم (Mi)، متوسط (Mo)، زیاد (S) و خیلی زیاد (C) نمایش داده شده است. برای درک بهتر هر یک از این متغیرهای فازی، این توابع عضویت در شکل‌های (۷-۴) ارائه شده است.



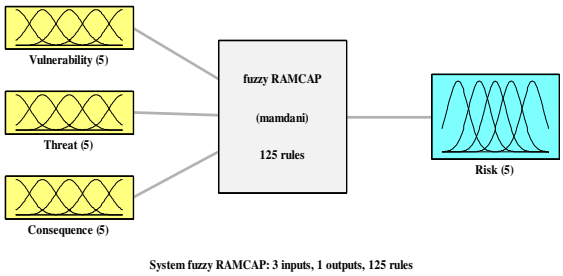
شکل ۲. روند به‌دست آوردن ریسک [۱۵]

۳-۱. اجرای روش

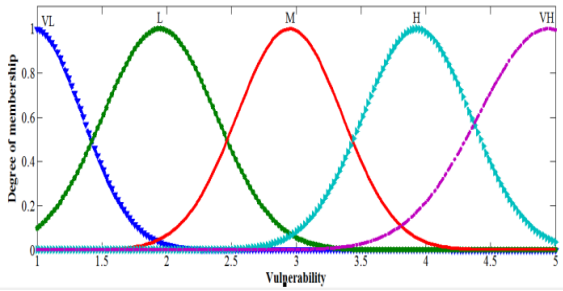
همان‌گونه که از شکل‌های (۷-۴) پیداست، توابع عضویت به‌کار رفته در این مطالعه از نوع گوسین[1] می‌باشند. زیرا این توابع عضویت مشخصه‌های محاسباتی و ریاضیاتی را به‌گونه‌ای ساده نمایش می‌دهند. علاوه بر این، توابع گوسین دارای حالت پیوستگی می‌باشند که باعث می‌شود این توابع به‌صورت هموار و غیر صفر باشند. این هموار بودن و مختصر بودن توابع گوسین سبب شده این توابع عضویت به‌عنوان توابع عضویت رایج برای نمایش دادن مجموعه‌های فازی مورد استفاده قرار بگیرند [۱۷]. تابع عضویت گوسی را می‌توان به‌صورت زیر نشان داد:

$$G(x;c,\sigma)=e^{-\frac{1}{2}\left(\frac{x-c}{\sigma}\right)^2} \qquad (۱)$$

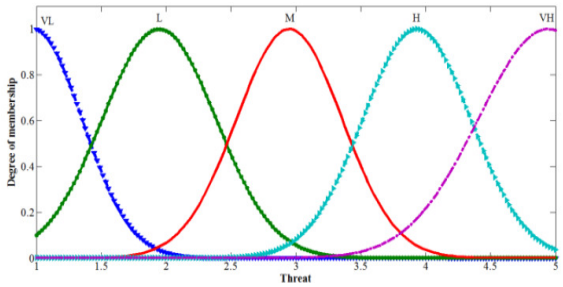
که c و σ به‌ترتیب مرکز و عرض تابع عضویت می‌باشند. در این مطالعه به‌عنوان مثال برای هر ورودی متغیر آسیب‌پذیری، c دارای مقادیر ثابت ۰ برای عبارت زبانی اول و ۵ برای عبارت زبانی نهایی می‌باشد و برای سایر موارد، مرکز عبارت زبانی می‌باشد. پارامتر σ نیز طوری تطابق داده می شود که هر تابع عضویت به‌طور تقریبی ۵۰ درصد همپوشانی داشته باشد. این امر سبب می‌شود ریسک مربوط به عدم درنظر گرفتن یک موقعیت خاص حذف شود. شکل (۸) عملکرد سیستم استنتاج فازی با توابع عضویت فازی را نشان می‌دهد که تحت تأثیر عملگر AND (اشتراک دو مجموعه فازی) واقع شده است.



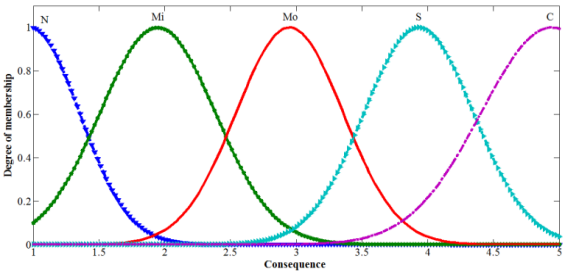
شکل ۳.ساختار کلی سامانه استنتاج به‌کار رفته [۱۶]



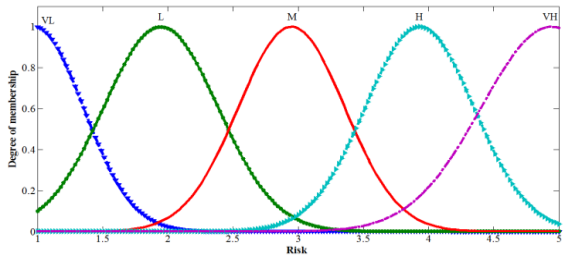
شکل ۴. توابع عضویت پارامتر آسیب‌پذیری (رتبه عضویت / آسیب پذیری)



شکل ۵. توابع عضویت پارامتر تهدید (رتبه عضویت / تهدید)

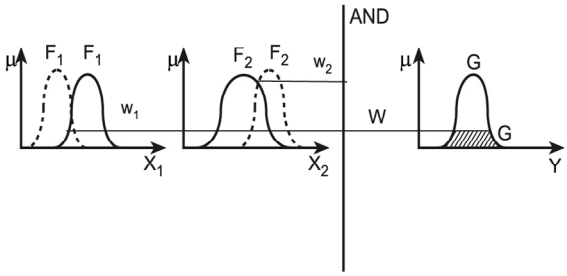


شکل ۶. توابع عضویت پارامتر پیامد (رتبه عضویت / پیامد)



شکل ۷.توابع عضویت پارامتر ریسک (رتبه عضویت / ریسک)

[1] Gaussian



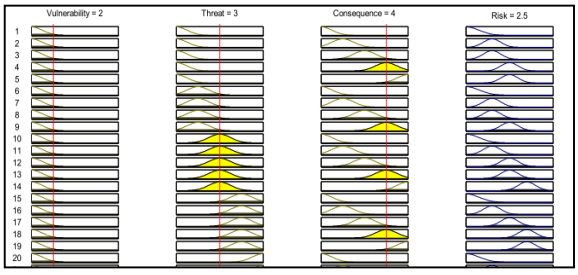
شکل ۸. سیستم استنتاج فازی با توابع گوسین [۱۷]

برای تشکیل پایگاه دانش، ۱۲۵ قانون اگر .... آنگاه .... نوشته شده است و نمونه‌ای از قوانین مربوط به ریسک به‌صورت قوانین اگر آنگاه در زیر آورده شده است و همچنین به‌صورت گرافیکی در شکل (۹) ارائه شده است.

Rule 1. If (Vulnerability is VL) and (Threat is VL) and (Consequence is N) then (Risk is VL)
Rule 2. If (Vulnerability is VL) and (Threat is VL) and (Consequence is Mi) then (Risk is VL)
Rule 3. If (Vulnerability is VL) and (Threat is VL) and (Consequence is Mo) then (Risk is VL)
Rule 4. If (Vulnerability is VL) and (Threat is VL) and (Consequence is S) then (Risk is L)
Rule 5. If (Vulnerability is VL) and (Threat is VL) and (Consequence is C) then (Risk is L)
Rule 6. If (Vulnerability is VL) and (Threat is L) and (Consequence is N) then (Risk is VL)
Rule 7. If (Vulnerability is VL) and (Threat is L) and (Consequence is Mi) then (Risk is L)

.
.

Rule 120. If (Vulnerability is VH) and (Threat is H) and (Consequence is C) then (Risk is VH)
Rule 121. If (Vulnerability is VH) and (Threat is VH) and (Consequence is N) then (Risk is M)
Rule 122. If (Vulnerability is VH) and (Threat is VH) and (Consequence is MI) then (Risk is H)
Rule 123. If (Vulnerability is VH) and (Threat is VH) and (Consequence is Mo) then (Risk is H)
Rule 124. If (Vulnerability is VH) and (Threat is VH) and (Consequence is S) then (Risk is VH)
Rule 125. If (Vulnerability is VH) and (Threat is VH) and (Consequence is C) then (Risk is VH)



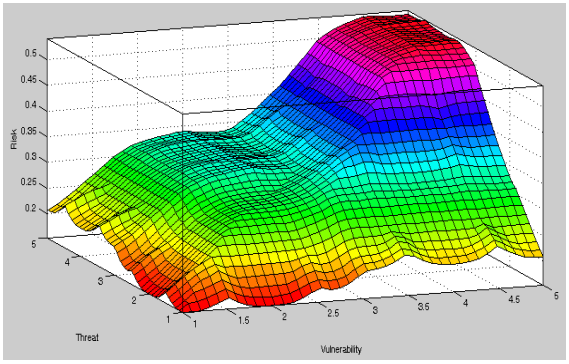
شکل ۹. نمونه گرافیکی قوانین احتمال [۱۷]

شکل‌های (۱۰، ۱۱ و ۱۲) حساسیت خروجی نمونه ریسک با استفاده از تغییرات تهدید، آسیب‌پذیری و تهدید را نشان می‌دهند. همان‌گونه که از شکل (۱۰) مشاهده می‌شود، رفتار ریسک نسبت به دو ورودی آسیب‌پذیری و تهدید متناظر می‌باشد به‌گونه‌ای که با افزایش هر یک باعث افزایش سطح ریسک می‌شود یا با افزایش آسیب‌پذیری و تهدید، ریسک افزایش می‌یابد.

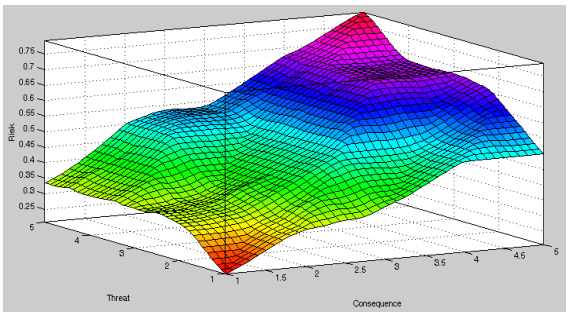
شکل (۱۱) تأثیر افزایش همزمان تهدید و پیامد با درنظر گرفتن مقدار ثابت برای آسیب‌پذیری بر روی ریسک را نشان می‌دهد. به‌طوری که از این شکل پیداست، یک افزایش تقریباً خطی بین دو متغیر ورودی مورد بررسی بر سطح ریسک دارد. همچنین شکل (۱۲) افزایش میزان ریسک با افزایش مقادیر مربوط به پیامد و آسیب‌پذیری را در زمانی که متغیر تهدید ثابت می‌باشد، نشان می‌دهد.

۴. نمونه مطالعاتی

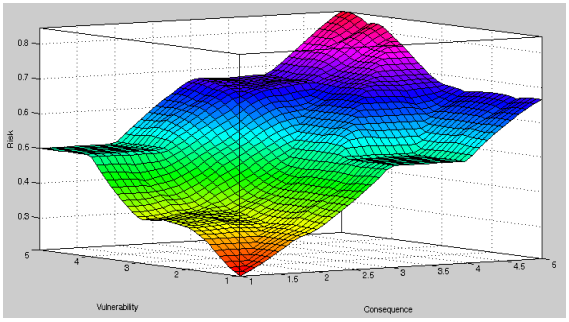
به‌منظور نشان دادن قابلیت‌های بالقوه نمونه پیشنهاد شده FUZZY RAMCAP یک مورد مطالعاتی در زمینه بنادر توضیح داده شده است. فعالیت بنادر با اتکا به مدیریت، فعالیت نیروهای انسانی، تأسیسات و تجهیزات ناوبری اقدام به تخلیه و بارگیری نموده و کالای کشتی‌های ورودی و خروجی به بنادر را دریافت و ارسال می‌کند. محوطه‌ها، انبارها و مخازن موجود در بنادر محل‌هایی برای نگهداری کالاهای مختلف برای مدتی قبل از صادرات و یا مدتی پس از واردات، محسوب می‌گردند، از این رو با تعریف این فرایند کاری و فعالیت و با توجه به انحصاری بودن برخی از فضاها و فعالیت‌ها، می‌توان حوزه‌های مورد توجه دشمن، آسیب‌پذیر و با اهمیت بنادر را به ترتیب اولویت به شرح ذیل معرفی نمود.



شکل ۱۰. حساسیت ریسک به تغییرات آسیب‌پذیری و تهدید



شکل ۱۱. حساسیت ریسک به تغییرات تهدید و پیامد



شکل ۱۲. حساسیت ریسک به تغییرات آسیب‌پذیری و پیامد

ساختمان‌های اداری و مدیریتی: این فضاها به این دلیل که محل استقرار جمعیت و نیروهای انسانی در مجموعه تلقی می‌گردند، از درجه اهمیت بالایی برخوردارند. هرچند که در مواقع احتمال وقوع بحران، می‌توان ساختمان‌ها را تخلیه نمود و یا سرانه و تراکم حضور افراد را در آنها کاهش داد، اما به‌دلیل شاخص و با اهمیت بودن، مورد تهدید قرار می‌گیرند. ساختمان اداری، گمرک و خدمات بنادری از آن جمله‌اند.

تأسیسات برقی: انرژی برق در فعالیت‌های جاری و حوزه‌های مختلف خدماتی، تولیدی و ارتباطی، نقشی انکارناپذیر دارد. در بنادر، برق به‌عنوان انرژی مصرفی در سازوکار ارتباطی، اتوماسیون و تشریفات اداری، گمرکی و امور مربوط به ورود و خروج کالا، نقشی حیاتی دارد. برق شهری در بسیاری از عملیات بنادری دارای نقشی محوری است. تجهیزات تخلیه و بارگیری با برق فشار قوی کار می‌کنند. بدیهی است به همان نسبت که در جریان برق بنادر اختلال ایجاد شود، در فعالیت بنادر نیز مشکل به‌وجود می‌آید.

مرکز رادیویی و مخابراتی: یک مرکز رادیویی و مخابراتی دریایی است که زمینه برقراری ارتباطات ناوبری، اسنادی و مدارک تجاری و کالاها برای انجام تشریفات واردات و صادرات را انجام می‌دهد. این مرکز به‌عنوان مرکز کنترل، هدایت و راهبری دریایی، با سایر بخش‌های اداری و امدادی بنادر در تماس و ارتباط است. تسهیل و تسریع فعالیت‌های دریایی و وابستگی بنادر به آن از جمله ویژگی‌های این مرکز رادیویی، مخابراتی است.

اسکله‌ها: اسکله‌های بنادر امکان پهلوگیری امن و ایمن کشتی‌های مختلف را فراهم می‌آورند. در این بنادر، کشتی‌های تا ظرفیت چندین هزارتن پذیرفته می‌شوند. کارکرد مناسب اسکله‌ها باعث عملکرد مناسب بنادر می‌شود. اسکله‌ها همچنین دارای پس‌کرانه سازه‌ای و محوطه‌ای برای استقرار اولیه کالاهای ورودی و خروجی هستند. هرچند ممکن است آسیب‌پذیری کلی اسکله‌ها کم باشد اما آنها از حساسیت و اهمیت عملکردی برخوردارند.

کانال ورودی و حوضچه: یک مایلی بنادر مانند یک دسترسی به عرض حدود ۵۰۰ متر لایروبی شده و از این مسیر از لنگرگاه در فاصله نزدیک به ۵ عمق مناسب برای تردد کشتی‌ها برخوردار است. در صورت غرق شدن و یا به گل نشستن یک کشتی در این مسیر، راه منتهی به بنادر قطع می‌شود. در این خصوص علاوه بر لزوم تلاش برای کاهش حساسیت و اهمیت، با ایجاد مسیرهای جایگزین، باید نحوه فعالیت و تردد را نیز تحت تأثیر تهدیدات احتمالی ساماندهی نمود.

۵. تهدیدات متصور و سطوح تأثیر آن

در بررسی‌های صورت گرفته، تهدیدات متصور برای بنادر بر اساس منشاء اثر تهدید به سه دسته زیر تقسیم می‌شوند:

تهدیدات داخلی(عملکردی): دامنه این تهدیدات در حوزه فعالیتی بنادر و در اثر حوادث و اتفاقات مختلف ناشی از عملکرد مجموعه است حوادثی نظیر آتش‌سوزی انبارها، برخورد کشتی‌ها به اسکله و بسته شدن راه‌های ارتباطی داخلی بنادر بر اثر ازدحام تریلرها و دیگر وسایل عبور و مرور و غیره سطح تأثیر این تهدید، محدود به بخشی از بنادر می‌شود و در روند کلی فعالیت بنادر تأثیر ناچیزی دارد ولی در تردد کشتی‌ها به داخل و خارج بنادر تأثیری ندارد.

تهدیدات داخلی (خرابکارانه و تروریستی): دامنه این تهدیدات در دو حوزه خشکی و دریا قابل تصور است. قرارگیری بنادر در سواحل وضعیت امنیتی آن، این سطح از تهدیدات را پررنگ‌تر از سایر نقاط کشور کرده است، بنابراین تلاش می‌شود تا تهدیدات داخلی با نگاهی ویژه و برخوردار از اطلاعات مربوط به منطقه مورد بررسی قرار گیرند.

در حوزه دریا، احتمال خطر غرق شدن کشتی در کانال ورودی حوضچه به‌منظور از کار انداختن فعالیت بنادر وجود دارد. این مهم می‌تواند در روند عادی فعالیت بنادر تأثیر بسزایی گذاشته و روند کلی فعالیت در بنادر را با مشکل مواجه سازد.

در حوزه خشکی: احتمال خطر بمب‌گذاری و انفجار که رخداد بمب‌گذاری توسط عوامل مختلف داخلی و یا تریلرهای حامل بار و همچنین از طریق سلاح های سبک (خمپاره اندازها و دوش پرتاب‌ها)، قابل تصور است. این مهم به‌منظور کاهش سطح امنیت در منطقه و به تبع آن ایجاد رعب و وحشت در دل صاحبان کالا و کشتی‌ها صورت می‌گیرد. لازم به‌ذکر است که عوامل داخلی با هدایت از خارج از کشور، در ایجاد آن مؤثر می‌باشند.

تهدیدات خارجی: دامنه این تهدیدات در دو حوزه نرم و سخت قابل تصور است.

حوزه نرم: از طریق اعمال فشارها و تحریم‌های اقتصادی و یا ایجاد جنگ روانی و همچنین انواع جنگ‌افزارهای غیر تخریبی مانند انواع حملات رایانه‌ای، الکترومغناطیسی و تهدید صورت می‌پذیرد که به موجب آن، علاوه بر ایجاد تبعات روانی، اجتماعی و اقتصادی در کل کشور، در حوزه بنادر نیز موجب تخریب فعالیت‌ها و کاهش سطح فعالیت ناشی از کاهش تردد کشتی‌ها و کاهش تبادل کالا (واردات و صادرات) می‌شود.

حوزه سخت: دشمن همواره به‌دنبال آن بوده که با ایجاد مشکلات متعدد برای کشورهای هدف، شرایطی را فراهم آورد تا خواسته‌های خود را به این کشورها تحمیل نماید و در صورتی که به این خواسته‌ها نرسد با ایجاد اجماع نسبی در بین هم‌پیمانان خود، کشور را مورد تهاجم قرار می‌دهد. در این حوزه، دشمن بر اساس سناریوی ازپیش تعیین شده به‌دنبال رسیدن به اهداف خود می‌باشد که این مهم در سناریوی تهدید مورد بررسی قرار می‌گیرد.

۶. سناریوی تهدید

حمله، تهاجم و تهدید به‌منظور نابودی، حذف و یا ناکارآمدی یک

کشور، سامانه، فعالیت و یا نیروهای انسانی مانند هر پدیده ذهنی، فکری و فرآیند فعالیتی، دارای یک پشتوانه برنامه‌ریزی و برنامه‌ای است. به‌عبارتی، مراحل مختلف آغاز تهدید تا پایان یک تهاجم و حمله، دارای دامنه وسیعی از امکان‌پذیری‌های مختلف در مقیاس‌های کلان بین‌المللی تا کشوری و منطقه‌ای است. عامل یا کشور تهدید کننده بنا به سیاست و اهداف خود، برنامه‌های مختلف تهدید را در دامنه جغرافیایی خاصی از سرزمین هدف، تنظیم می‌کند. این دامنه ممکن است کل وسعت و محدوده جغرافیایی هدف را دربر گرفته و یا بخشی از حدود مورد نظر را شامل گردد.

علاوه بر دامنه جغرافیایی و وسعت محدوده هدف، شدت تهدید تا تهاجم نیز از جمله راهبردهای مهاجم محسوب می‌شود. اهداف و سیاست‌های کلان، راهبرد شدت تهدید را تعیین می‌کند. این موضوع نیز خوددارای دامنه وسیعی از امکان‌پذیری‌ها را دربر می‌گیرد. در کنار عاملی مانند شدت در ادبیات سیاسی جنگ و دفاع، سرعت و دقت نیز می‌توانند مورد توجه قرار گیرند که در این تقسیم‌بندی در یک حوزه اصلی قرار می‌گیرند.

۷. بررسی و ارزیابی ریسک و مخاطرات در بنادر

در این مثال هشت دارایی حیاتی مورد بررسی قرار گرفته‌اند که شامل ساختمان مجموعه اداری و مدیریتی (A_1)، تأسیسات دریافت، تولید و انتقال برق (A_2)، مجموعه رادیویی و مخابراتی (A_3)، اسکله‌ها (A_4)، کانال ورودی و حوضچه (A_5)، تجهیزات تخلیه و بارگیری (A_6)، دروازه و گارد و حراست (A_7)، دسترسی‌های داخلی و بیرونی (A_8)، مخازن سوخت شرکت نفت (A_9)، انبارها (A_{10})، آب شیرین‌کن و مخازن آب (A_{11})، مجموعه خدماتی و رفاهی (A_{12}) و لنگرگاه (A_{13}) می‌باشد.

در جداول محاسباتی ارزیابی ریسک، سه مؤلفه احتمال، تهدید و پیامد بر اساس جدول "محاسباتی اعداد اولویت ریسک"، عددگذاری شده و از حاصل ضرب سه عدد احتمال، تهدید و پیامد عدد اصلی ریسک به‌دست می‌آید.

تیم ارزیاب شامل ۶ خبره با درجه بالایی از دانش در زمینه تحلیل ریسک، دارایی‌های موجود را تحت سه مؤلفه آسیب‌پذیری، تهدید و پیامد مورد ارزیابی قرار دادند به‌طوری‌که دارایی با بالاترین ارزش دارای بیشترین میزان ریسک می‌باشد.

با توجه به مشکلات مربوط به عدم اطمینان حاصل از ارزیابی فاکتورهای ریسک و وزن‌های مرتبط با آنها، تیم ارزیاب موافقت نمودند تا دارایی‌ها را با استفاده از متغیرهای زبانی مورد ارزیابی قرار داده و سپس خروجی‌ها با خروجی روش رمکپ مرسوم، مورد مقایسه قرار دهند. نتایج این مقایسه را می‌توان در جدول (۱) مشاهده نمود.

یکی از عیب‌های اصلی مربوط به روش رمکپ این است که مجموعه‌های مختلفی از سه پارامتر آسیب‌پذیری، تهدید و پیامد ممکن است مقادیر یکسانی برای سطح ریسک ارائه دهند، در حالی که ضرورتاً این مقادیر نباید یکسان باشند. برای مثال چهار دارایی A_2، A_3، A_5 و A_7 دارای ارزش‌های ۳، ۲، ۴ و ۲، ۳، ۴ و ۴، ۲، ۳ و ۳، ۴، ۲ برای آسیب‌پذیری، تهدید و پیامد هستند. هر چهار دارایی‌ها دارای ارزش ریسکی برابر با ۲۴ می‌باشند که به هر حال ریسک این چهار دارایی ممکن است به‌طور کامل متفاوت باشد. این ممکن است باعث شود مقداری از منابع و زمان برای کاهش ریسک دارایی که در اولویت نیست صرف شده و از بین برود.

دیگر عیب روش رمکپ مرسوم این است که این روش اهمیت نسبی بین سه پارامتر تعیین کننده میزان ریسک را درنظر نمی‌گیرد. این موضوع با مسائل دنیای واقعی تطابق ندارد و به‌طور حتم قرار بر این نیست که تمام معیارها اثر یکسانی داشته باشند. بنابراین، خروجی روش پیشنهاد شده دقیق‌تر، مطمئن‌تر و صحیح‌تر می‌باشد. در جدول ذیل، مقایسه خروجی روش رمکپ معمولی و روش پیشنهادی ارائه شده است.

جدول ۱. مقایسه خروجی روش رمکپ معمولی و روش پیشنهادی

Assets	Input						Output			
	Crisp			Fuzzy			Traditional RAMCAP	Rank	Fuzzy RAMCAP	Rank
	V	T	C	V	T	C				
A_1	۵	۱	۲	۴/۳۸	۱/۰۶	۲/۳۷	۱۰	۹	۲/۱۲	۱۰
A_2	۳	۲	۴	۳/۰۲	۲/۵۳	۳/۹۶	۲۴	۳	۳/۰۵	۵
A_3	۲	۳	۴	۲/۵۷	۳/۱۵	۴/۰۵	۲۴	۳	۳/۱۱	۴
A_4	۴	۳	۵	۳/۸۴	۳/۲۲	۴/۵۳	۶۰	۱	۳/۷۸	۱
A_5	۳	۲	۴	۲/۶۵	۲/۳۳	۳/۶۹	۲۴	۳	۲/۸۴	۷
A_6	۲	۳	۲	۱/۶۹	۳/۱۴	۲/۲۱	۱۲	۸	۱/۷۹	۱۱
A_7	۲	۴	۳	۱/۸۷	۴/۰۰	۳/۶۳	۲۴	۳	۲/۷۵	۸
A_8	۳	۳	۴	۲/۹۵	۲/۸۴	۴/۰۷	۳۶	۲	۳/۲۷	۲
A_9	۲	۱	۱	۲	۱/۱۱	۱/۲۴	۲	۱۳	۱/۱۲	۱۳
A_{10}	۱	۳	۲	۱/۲۳	۲/۶۷	۱/۹۸	۶	۱۱	۲/۲۳	۹
A_{11}	۲	۴	۲	۱/۵۸	۴/۲۱	۱/۶۹	۱۶	۷	۳/۰۳	۶
A_{12}	۱	۱	۳	۱/۲۱	۱/۰۹	۲/۸۷	۳	۱۲	۱/۶۷	۱۲
A_{13}	۲	۱	۵	۲/۱۲	۱/۳۲	۴/۹۱	۱۰	۹	۳/۲۳	۳

سامانه‌های فازی، در گروه آن دسته از سیستم‌های دینامیکی هستند که با پردازش روی داده‌های موجود که به‌صورت زبانی هستند به نمونه نمودن فرایندهای پیچیده می‌پردازند. قدرت بالای سامانه‌های فازی در تشخیص انواع الگوهای موجود در داده‌ها، توان تقریب توابع پیچیده، نمونه‌سازی عدم اطمینان، غیر خطی بودن و توانایی نمونه کردن فرآیندهای آشوبی از جمله ویژگی‌هایی است که سامانه‌های فازی را از دیگر روش‌ها متمایز کرده و سبب شده است که این رویکرد، به‌عنوان یکی از پرکاربردترین روش‌های ارزیابی ریسک مطرح شود.

سامانه‌های فازی به‌عنوان یک روش بر پایه دانش خبرگان فارغ از فرضیات لازم در روش‌های نمونه‌گرا است که رویکردی نوین و قدرتمند در جهت نمونه‌سازی توابع پیچیده و برخورد با مسائل ارزیابی ریسک محسوب می‌شود [۱۸].

این مزایا در کنار ضعف روش‌های کلاسیک مورد استفاده برای ارزیابی ریسک، سبب شده است این رویکرد به‌عنوان یکی از روش‌های پیشرو در ارزیابی ریسک مورد استفاده باشد. مزایای بالای آن در مقایسه با روش‌های کلاسیک، برتری و ضرورت استفاده از آن را در زمینه ریسک امنیتی روشن می‌سازد.

بدون تردید بنادر به‌عنوان یکی از مهم‌ترین بخش‌ها در امنیت و پایداری ملی همواره یکی از اولین گزینه‌ها برای دشمن به‌منظور فلج کردن سامانه تولید و توزیع مطرح بوده است. بنابراین، با توجه به نیاز این بخش و همچنین با توجه به عملکرد مناسب سامانه‌های فازی در رویارویی با نمونه‌سازی مسائل دنیای واقعی، ارزیابی ریسک امنیتی در بنادر مورد بررسی قرار گرفته است.

۸. نتیجه‌گیری

در تحقیق حاضر، نمونه‌سازی ریسک امنیتی در بنادر با استفاده از سامانه‌های فازی انجام گرفته است. به‌طور کلی دو سناریو مطرح شده که عبارتند از:

- ارزیابی ریسک امنیتی در بنادر رویکرد روش ارزیابی ریسک کلاسیک رمکپ.
- ارزیابی ریسک امنیتی بنادر با استفاده از روش پیشنهادی تلفیقی که ترکیبی از روش فازی و رمکپ است.

بر اساس یافته‌های این تحقیق، روش پیشنهاد شده بر پایه سامانه‌های فازی نسبت به روش کلاسیکرمکپ دارای توانایی بالایی در نمونه‌سازی سامانه‌های پیچیده دارد. سامانه‌های فازی ابزارهای مناسبی برای نمونه‌سازی عدم اطمینان ناشی از نبود اطلاعات و یا جایی که داده‌ها قابل اندازه‌گیری نیستند، می‌باشند. از طرف دیگر، سامانه‌های فازی ابزار دانش محور هستند و قادر به نمونه‌سازی فرایندهای پیچیده بر پایه متغیرهای کلامی یا زبانی و بر اساس دانش خبرگان می‌باشند. باتوجه به مأموریت و اهداف پدافند غیرعامل و تجارب حاصل مبتنی بر تجربیات و یافته‌های برخی از کشورها، ارزیابی تهدیدات و ریسک خطرات در فرآیند انجام مطالعات پدافند غیرعامل نقش بسزا و تعیین کننده‌ای را در راستای کاهش آسیب‌پذیری زیرساخت‌های ملی به‌ویژه بنادر دارد. ارزیابی تهدیدات و ریسک خطرات در زیر ساخت‌های ملی با سه محور اصلی توسعه داده شده است:

- چارچوبی را معین می‌کند تا از این طریق تهدیدات مربوط به سیستم‌ها و دارایی‌ها شناسایی شوند.
- راهنما و الگویی مشترک برای روش‌هایی که در تشخیص و ارزیابی اطلاعات مربوط به تهدیدات کاربرد دارند، فراهم می‌کند.
- روش‌های نوآورانه و مؤثر و کارایی را در زمینه جمع‌آوری اطلاعات مورد نیاز بخش پدافند غیرعامل برای اجرا و سیاست‌گذاری تعریف می‌کند.

۹. مراجع

[1] Eftekhari, A. “Threat Autopsy”; Centre of Defence Studies and National Security, Tehran, 1385 (In Persian).

[2] Divsalar, A. “Military Ecology”; Maleke Ashtar Univ., Tehran, 2007 (In Persian).

[3] Khaki, G. “Research Methodology in Management”; Centre of Scientific Publication, Islamic Azad Univ., 2003 (In Persian).

[4] Karimipour, Y. “The Role of Politic and Security in ICZM”; Report No. 3 Ports and Maritime Organization, 2007 (In Persian).

[5] Bajpai, Sh.; Sachdeva, A.; Gupta, J. P. “Security Risk Assessment: Applying the Concepts of Fuzzy Logic”; J. Hazard. Mat. 2010, 173, 258–264.

[6] Chen, Sh-M.; Sanguansat, K. “Analyzing Fuzzy Risk Based on a New Fuzzy Ranking Method Between Generalized Fuzzy Numbers”; Expert Systems with Applications 2011, 38, 2163-2171.

[7] Nieto-Morote, A.; Ruz-Vila, F. “A Fuzzy Approach to Construction Project Risk Assessment”; Int. J. Proj. Manag. 2011, 29, 220–231.

[8] Flores, W. C.; Mombello, E.; Jardini, J. A.; Rattá G. “Fuzzy Risk Index for Power Transformer Failures due to External Short-Circuits”; Elec. Power Sys. Res. 2009, 79, 539–549.

[9] Wei, Sh-H.; Chen, Sh-M. “Fuzzy Risk Analysis Based on Interval-Valued Fuzzy Numbers”; Expert Systems with Application 2009, 36, 2285-2299.

[10] Sadiq, R.; Kleiner, Y.; Rajani, B. “Water Quality Failures in Distribution Networks-Risk Analysis using Fuzzy Logic and Evidential Reasoning”; Risk Analysis 2007, 27, 1381-1394.

[11] Zhao, D-M.; Wang, J-H.; MA, J-F. “Fuzzy Risk Assessment of the Network Security”; Proc. of the Fifth Int. Conf. on Machine Learning and Cybernetics, Dalian, 2006, 4400-4405.

[12] Norman, Th. L. “Risk Analysis and Securit Countermeasures Selection”; CRC press, 2010.

[13] U.S. Coast Guard, “Implementation of National Maritime Security Initiatives”; Federal Register 2003, 68, 39240-39250.

[14] Azadeh, A.; Fam, I. M.; Khoshnoud, M.; Nikafrouz, M. “Design and Implementation of a Fuzzy Expert System for Performance Assessment of an Integrated Health, Safety, Environment (HSE) and Ergonomics System: The Case of a Gas Refinery, Information Sciences”; Information Sci.: An Int. J. 2008, 178, 4280–4300.

[15] Liu, K.; Hao, J.; Pang, Y. “Algorithm Research on Project Risk Fuzzy Evaluation”; First International Workshop on Database Technology and Appllications 2009, 160-164.

[16] Chan, F. T. S.; Kumar, N. “Global Supplier Development Considering Risk Factors using Fuzzy Extended AHP-Based Approach”; Omega-Int. J. Management Sci. 2007, 35, 417-431.

[17] Grassi, A.; Gamberini, R.; Mora, C.; Rimini, B. "A Fuzzy Multi-Attribute Model for Risk Evaluation in Workplaces"; Safety Science 2009, 47, 707–716.

[18] Gürcanli, G. E.; Müngen, U. “An Occupational Safety Risk Analysis Method at Construction Sites Using Fuzzy Sets”; Int. J. Ind. Ergonomics 2009, 39, 371–387.