فصلنامه علمی-ترویجی پدافند غیرعامل
سال نهم، شماره ۱، بهار ۱۳۹۷، (پیاپی ۳٤): صص ۹٤-۸۳

ارزیابی ریسک حملات خصمانه با تاکید بر مدل فرآیند تحلیل شبکه

محمد ذوالقدر[۱]، محمدجواد غلامی[۲*]

تاریخ دریافت: ۱۳۹۶/۰۳/۰۸
تاریخ پذیرش: ۱۳۹۶/۱۱/۱۶

چکیده

بررسی عوامل و تشخیص نوع تهدید و مخاطرات احتمالی دارایی‌های مهم در زمان بروز حوادث از کلیدی‌ترین اقدامات کاهش آسیب‌پذیری با رویکرد پدافند غیرعامل است. از این‌رو، جهت تدوین محتمل‌ترین سناریو به منظور پیشگیری و یا کاهش آسیب‌پذیری و پیامد نیازمند تدوین شاخص‌های جامع و تکنیک تحلیل ریسک هستیم. در مدل‌های ارایه‌شده کنونی، کلیه مراحل تحلیل ریسک به‌صورت خطی بوده درحالی‌که می‌تواند نقطه ضعف عمده‌ای در فرآیند ارزیابی به‌شمار آید بدین صورت که به‌عنوان مثال در مرحله غربالگری دارایی‌ها، دارایی که فاقد ارزش بالایی به لحاظ دارایی شناسی باشد، حذف شده اما درحالی‌که پتانسیل بالایی برای آسیب‌پذیری بزرگی در سامانه می‌باشد در واقع با توجه به ماهیت خطی‌بودن مدل‌ها، دارایی در مرحله اول حذف شده و مانع ارزیابی در مراحل بعدی (ارزیابی آسیب‌پذیری) می‌شود. با توجه به ضعف مدل‌های خطی جهت تعیین الویت در آسیب‌پذیری سه سایت هسته‌ای از مدل فرآیند تحلیل شبکه استفاده شده است. روش تحقیق پژوهش حاضر برمبنای هدف از نوع توسعه‌ای بوده و از بعد ماهیت، توصیفی که از منابع کتابخانه‌ای و نقطه نظرات نخبگان جهت بررسی مدل‌های ارایه‌شده استفاده شده است. در نهایت، ضمن تبیین شاخص، به تشریح مدل فرایند تحلیل شبکه به منظور ارزیابی نهایی ریسک پرداخته شده است که بیشترین ریسک به ترتیب مربوط به سایت‌های A, B ,C می‌باشد.

کلیدواژه‌ها: اهداف آسیب‌پذیری، پدافند غیرعامل، اهواز، کالبدی- اجتماعی، گاما (Gamma).

۱- کارشناس ارشد مدیریت بحران
۲- دانشجوی دکتری شهرسازی، دانشگاه آزاد اسلامی علوم و تحقیقات تهران، کارشناس مدیریت بحران، Mj_gholamikhooeini@yahoo.com- نویسنده مسئول

۱- مقدمه

بررسی روش‌های رایج ارزیابی ریسک تهدیدات به شناخت و انتخاب روش مناسب کمک می‌کند. یک روش مناسب ارزیابی ریسک باید دارای ویژگی‌های جامعیت، نگرش چندوجهی و ساختارمندبودن باشد. جامعیت به این مفهوم است که مطالعات کل پارامترهای تأثیرگذار و جزئیات آن را شامل شود. نگرش چندوجهی به معنی بررسی ریسک از مناظر و تخصص‌های گوناگون برای کشف امکان وقوع هر نوع تهدید است و در نهایت مطالعه‌ای ساختارمند است که قابل بررسی، بازنگری و اصلاح باشد. مقایسه نظریه‌ها، تجارب و ابزارهای مورد نیاز برای تدوین یک روش خاص ارزیابی ریسک زمانی حاصل خواهد شد که روش‌های مطرح موجود در جهان مورد بررسی قرار گیرد. روش مناسب ارزیابی ریسک تهدیدات در سایت‌های هسته‌ای نیز از این رهگذر حاصل خواهد شد.

روش‌های مختلف ارزیابی ریسک تهدیدات عمدتاً با دو رویکرد کیفی و کمی توسعه یافته‌اند. جهت مقایسه این دو رویکرد کلی به زبان ساده باید گفت که ارزیابی کیفی شامل تفسیر و نتیجه‌گیری از مصاحبه‌ها، عبارت‌ها، ذهنیات و پندارها است و روش‌های کمی شامل تفسیر اعداد از داده‌ها و تخمین‌ها است. به بیان دیگر، ارزیابی کیفی یک شناخت ذهنی است و ارزیابی کمی، ریاضی و عددی است. گزارش‌های کیفی با کلمات و مفاهیم سروکار دارند و نیازمند خوانش و پردازش مفاهیم هستند درحالی‌که گزارش‌های روش کمی حاوی تعداد بسیار زیادی چارت، نمودار و جداولی هستند که ممکن است به سختی درک شوند. لحاظنمودن سطح تجربه فرد ارزیاب در گزارش‌های کمی غالباً با مشکل روبه‌رو است و قضاوت کردن در مورد کیفیت تحلیل‌ها در گزارش‌های کمی نیز کار سختی است. گزارش‌های کمی که به‌دلیل فقدان مهارت‌های خوب تحلیل‌گری داده‌های ساده را از دست می‌دهند از کیفیت خوبی برخوردار نیستند. روش‌های مختلف ارزیابی ریسک زیرمجموعه یکی از رویکردهای کمی و کیفی قرار می‌گیرند با این‌حال، در یک نگاه کلی، تمامی روش‌های ارزیابی ریسک دارای بخش‌های زیر می‌باشد:

- ابتدا دارایی‌های سازمان/ صنعت یا حوزه مورد بررسی را شناسایی می‌کنند.
- سپس تهدیدها و احتمال وقوع آن را مورد بررسی قرار می‌دهند.
- آسیب‌پذیری‌ها را شناسایی می‌کنند.
- برآورد پیامد با توجه به نوع و ماهیت دارایی، تهدید و آسیب پذیری های محتمل، صورت می پذیرد.
- ریسک را محاسبه و سطح‌بندی می‌کنند.
- در نهایت، تمامی روش‌های ارزیابی ریسک به‌دنبال انتخاب راه‌های مقابله و اجرای اقدامات اصلاحی درخصوص ریسک‌های شناسایی‌شده می‌باشند و همواره به‌صورت چرخه‌ای این مراحل تکرار می‌گردد [۱].

بیشتر روش‌های ارزیابی ریسک موجود در جهان از سه جزء اصلی ارزیابی آسیب‌پذیری، ارزیابی تهدیدات و تعیین احتمال وقوع تشکیل شده‌اند. تمامی اجزای اصلی ارزیابی ریسک در یک مجموعه خاص با هم کار می‌کنند. احتمال وقوع، آسیب‌پذیری و پیامد اجزایی هستند که شدیداً به یکدیگر وابسته هستند. وقتی نقش آسیب‌پذیری مورد شناسایی قرار می‌گیرد نقش تجهیزات، دارایی‌ها و تهدیدات نیز مدنظر قرار گرفته است. وقتی دارایی‌ها مورد بررسی هستند، در واقع مقدمه‌ای برای بحث در مورد اهمیت دارایی‌ها یا پیامدهای آن است. اجزای فرآیند ارزیابی ریسک در طول اجرای ارزیابی بهتر درک خواهند شد چرا که نه یکبار بلکه چندین بار به انحای مختلف به‌علت وابستگی به یکدیگر در طول فرآیند تکرار می‌شوند. برای ارزیابی ریسک تهدیدات روش‌های مختلفی وجود دارد که برخی از مهم‌ترین آن‌ها در ادامه توضیح داده شده است.

۲- ضرورت تحقیق

اکثر حملات و بمباران‌هایی که در جنگ‌های شش دهه اخیر در دنیا اتفاق افتاده است، متمرکز بر دارایی‌های دشمن بوده و همواره متخاصمان در نبرد با یکدیگر سعی داشته‌اند تا توان عملیاتی و خدمات ضروری دشمن خود را به هر طریقی ازجمله بمباران و از بین‌بردن نیروگاه‌های برق، سدهای ذخیره آب، تصفیه‌خانه‌های آب، مراکز استحصال گاز، مراکز فرماندهی و تصمیم‌گیری و ... به حداقل کاهش داده تا بتوانند از خلاء موجود استفاده کرده و بر دشمن غلبه نمایند. از این‌رو، کشورها سعی دارند تا در راستای اقدامات دفاعی و پدافندی خود حداکثر حفاظت را از این مراکز داشته باشند.[۲] بنابراین، شناسایی دارایی‌های پر ریسک و الویت‌بندی آن، در کاهش آسیب‌پذیری و پیامد بسیار تاثیرگذار است. از این‌رو، عدم بررسی جامع و همزمان فاکتورهای تحلیل ریسک، منجر به افزایش احتمال موفقیت دشمن در حملات به اهداف مهم و زیرساختی خواهد شد، لذا مطالعه همزمان عوامل ارزیابی ریسک با تدوین شاخص‌های جامع، گام بزرگی در جهت افزایش توان پدافند غیرعامل و به تبع آن مدیریت بحران کشور، محسوب خواهد داشت.

۳- اهداف تحقیق

اهدف خرد پژوهش حاضر تدوین شاخص‌های تحلیل ریسک جهت حفاظت از دارایی‌ها و زیرساخت‌های مهم صنعت کشور و همچنین بررسی دودویی فاکتورهای تحلیل ریسک جهت حصول به هدف کلان "ارتقاء توان پدافند غیر عامل و مدیریت بحران" در صنایع مختلف می‌باشد.

۴- متغیرها و شاخص‌ها

نوع متغییرهای پژوهش از نوع مقدار کیفی- کمی بوده که در نهایت، متغییرهای کیفی با استفاده از طیف‌بندی به متغییرهای کمی تبدیل شده است و از نوع ماهیت متغییرهای وابسته می‌باشد.

۵- روش تحقیق

پژوهش حاضر ازنظر نوع هدف، توسعه‌ای و ازنظر نحوه گردآوری داده‌ها و ماهیت، تحقیق توصیفی به‌شمار می‌آید. بدین صورت که ابتدا با استفاده از اسناد کتابخانه‌ای و مصاحبه با نخبگان، چارچوب نظری تدوین و سپس با استفاده از مدل تحلیل شبکه، ارزیابی ریسک به‌صورت جامع بررسی می‌شود.

۶- تقسیم‌بندی روش‌های ارزیابی ریسک

تقسیم‌بندی‌های مختلفی برای روش‌های ارزیابی ریسک وجود دارد. ازجمله این تقسیم‌بندی‌ها می‌توان به موارد زیر اشاره کرد:

الف) روش‌های قیاسی و استقرایی

روش‌های قیاسی: در روش‌های قیاسی (حرکت از کل به جزء) نحوه ترکیب شکست‌های اجزاء، خطاهای انسانی، نرم‌افزاری و شرایط نامساعد محیطی که منجر به بروز حادثه و یا شکست سامانه می‌گردند، شناسایی و ارزیابی می شوند. به این ترتیب، روش‌های قیاسی واقعه نهایی را درنظر گرفته و عللی که می‌توانند باعث این واقعه شوند را جستجو می‌نمایند.

روش‌های استقرایی: شکست یک جزء را درنظر گرفته و در تحلیل‌های بعدی وقایعی را شناسایی می‌کنند که این شکست می‌تواند باعث وقوع آن‌ها شود. دقت این روش‌ها پایین بوه و معمولاً در طراحی و مراحل اولیه ساخت سامانه ها کاربرد دارند.

ب) روش‌های کیفی، نیمه‌کمی و کمی

روش‌های کیفی: روش های کیفی متشکل از روش‌های شناسایی اولیه خطر، مانند تجزیه‌وتحلیل با روش چک لیست و تجزیه و تحلیل با روش چه می‌شود اگر (what if)، روش مطالعه مخاطرات و راهبری وتحلیل مقدماتی خطر می باشد.

روش‌های نیمه‌کمی: متشکل از روش‌های شاخص‌دهی و ماتریسی مانند شاخص حریق و انفجار، شاخص Mond، شاخص برای رتبه‌بندی ریسک وقایع بالقوه خطرناک و روش تجزیه‌وتحلیل لایه‌های محافظ.

روش‌های کمی: متشکل از روش‌هایی می‌باشد که ریسک را به صورت عددی بیان می‌کنند، مانند روش تجزیه‌وتحلیل حالات شکست و آثار آن [۳].

۶- ۱- روش‌های ارزیابی ریسک امنیتی

با مطالعه روش‌های ارزیابی ریسک امنیتی که در ادامه بدان اشاره خواهد شد، این روش‌ها به‌صورت کمی شاخص‌ها و متغییرهای ارزیابی ریسک را بررسی و درنهایت، عدد ریسک نهایی مربوط به بالاترین احتمال خطر مربوط به دارایی‌ها و یا تهدید ات را استخراج می‌کنند.

۶-۱-۱- برنامه حفاظت از زیرساخت‌های ملی؛ ارائه‌شده توسط اداره امنیت داخلی ایالات متحده و وزارت دفاع

اداره امنیت داخلی با همکاری وزارت دفاع آمریکا، برنامه حفاظت از زیرساخت‌ها[1] را به‌عنوان یک راه‌برد ملی برای شناسایی زیرساخت‌های حیاتی، اولویت‌بندی و محافظت از آن‌ها ارائه نمود[2]. این برنامه برروی زیرساخت‌های حیاتی و منابع مهم و کلیدی متمرکز بود. در این برنامه جلب همکاری سازمان‌های مختلف و ایجاد همکاری بین آن‌ها مورد توجه قرار داشت و مسئولان و فعالان صنایع مختلف در بخش‌های دولتی و غیردولتی برای کسب اطمینان از دستیابی به استانداردهای لازم جهت ارتقاء ایمنی خود بایستی وارد عمل می‌شدند. اسامی برخی از استانداردهای وضع‌شده جهت افزایش امنیت انواع زیرساخت‌های مهم که به نوعی با ارزیابی ریسک تهدیدات خصمانه در ارتباط هستند را بیان می‌کند. زیرساخت‌های

1- National Infrastructure Protection Plan (NIPP)

۲- لازم به‌ذکر است که این سند از نوع برنامه بالادستی بوده و روش ارزیابی ریسک نیست. با این‌حال، چارچوب کلی را مشخص می‌کند که در آن روش‌های ارزیابی ریسک تهدیدات قابل به‌کارگیری است.

حیاتی و منابع کلیدی[1] به عناصر حیاتی و مهم، دارایی‌ها، سامانه‌ها، شبکه‌ها و فعالیت‌هایی که در امنیت ملی، ثبات اقتصادی و تداوم حیات جامعه نقش مؤثری دارد، اطلاق می‌شود. حملات تروریستی می‌تواند آسیب‌های جدی به این زیرساخت‌ها و در نهایت به کل کشور وارد کند، چون هدف قرارگرفتن آن‌ها همراه با عواقب منفی روانی، اقتصادی و فیزیکی است. دو کار عمده‌ای که مورد توجه وزارت دفاع ایالات متحده بود، عبارتند از:

- شناسایی، اولویت‌بندی و محافظت از زیرساخت‌های حیاتی و تعیین وظایف و مسئولیت‌های مربوطه.
- طراحی مراکزی که به‌طور هماهنگ با هم برای شناسایی، ارزیابی و بهبود ریسک زیرساخت‌های حیاتی مربوط به صنایع دفاعی فعالیت کنند.

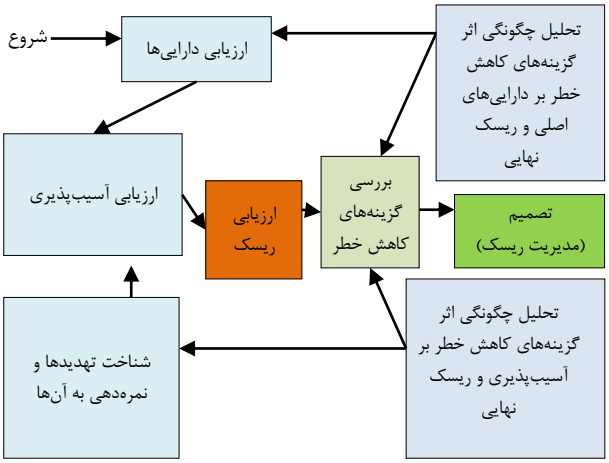
۶-۱-۲- روش مورد استفاده در سند FEMA 452

هدف این سند طرح روش‌هایی جهت تشخیص کاربری‌ها و دارایی‌های اصلی ساختمان‌ها، شناسایی تهدید متوجه آن‌ها و ارزیابی آسیب‌پذیری‌های ناشی از تهدیدات است. بر این اساس، روش‌های ارائه‌شده امکانی را جهت ارزیابی ریسک فراهم می‌کند که بر اساس آن می‌توان در مورد ریسک و روش‌های کاهش آن تصمیم گرفت. این روش‌ها شامل کاهش خرابی فیزیکی اجزای سازه‌ای ساختمان، اجزای غیرسازه‌ای و زیرساخت‌های ساختمانی و کاهش جراحات واردشده در مقابل بمب‌های متحرک و یا عوامل شیمیایی، بیولوژیک و رادیواکتیو است که به‌صورت راهنمای مرحله به مرحله تدوین شده است [۴]. روش ارائه‌شده شامل پنج گام به همراه شرح فعالیت هر گام است که مخاطب را در جهت فرآیند ارزیابی ریسک و انتخاب تصمیمات کاهش آن به‌خوبی هدایت می‌کند. همچنین، به بحث درباره چگونگی جمع‌آوری اطلاعات و محاسبه ریسک دردمقابل انواع تهدیدات می‌پردازد. با وجود این‌که کاربرد اصلی این سند برای ارزیابی ریسک ساختمان‌ها است ولی برای بررسی ریسک سایر زیرساخت‌های حیاتی نیز قابل استفاده است. مبنای روش ارائه‌شده براساس نظرات توسعه‌یافته (انجمن سربازان بازنشسته آمریکا) است که در انجمن ملی علوم ساختمان[2] مطرح شده است. روش ارائه‌شده در این سند بیش‌تر بر حملات تروریستی تمرکز نموده و درمقابل خطرات دیگر مانند آتش‌سوزی کاربرد ندارد. در شکل (۱)، مراحل ارزیابی ریسک مطرح شده در FEMA452 آمده است [۴].

1- Critical Infrastructure and Key Resources (CI/KR)
2- National Institute of Buiding Science

جدول (۱): استانداردهای ارزیابی ریسک

توضیحات	نام سند/ نهاد ارائه دهنده
استانداردهای امنیتی برای ساختمان‌های فدرال	Department of Justice
استانداردهای امنیت تأسیسات برای ساختمان‌های خدمات عمومی	General Services Administration
استانداردهای امنیت صنایع عمومی	Occupation of safety & health act (OSHA) section 1910
راهنمای طراحی برای امنیت فیزیکی تأسیسات	Military standards MIL-HDBK 1013/1 FM 3-19.30
RR-F-191k و RR-F-191	Federal Specification
برنامه‌ریزی کاهش ریسک ناشی از خطرات به‌وجود آمده توسط انسان	FEMA 386-7
دستورالعمل برای طراحی ساختمان از نظر امنیتی	FEMA-426
راهنمای چگونگی کاهش پتانسیل وقوع حملات تروریستی در ساختمان‌ها	FEMA-452
راهنمای امنیت غذایی و زیرساخت‌های حیاتی	DHS-OIG-07-33
برنامهٔ امنیت فیزیکی	DOD-5200-08-R and army regulation-



شکل (۱): مراحل ارزیابی ریسک مطرح‌شده در FEMA452

۶-۱-۳- جدول عوامل ریسک امنیتی SRFT[3]

وضعیت ریسک امنیتی یک سایت صنعتی را می‌توان به‌واسطه جدول عوامل ریسک امنیتی ارزیابی نمود. بدین صورت که کلیه تهدیداتی که بر دارایی‌های حیاتی تأثیر می‌گذارند از صفر (پائین‌ترین ریسک) تا پنج (بالاترین ریسک) رتبه‌بندی می‌گردند. این رتبه‌بندی مبتنی‌بر قضاوت خبرگان است. مجموع امتیازهای کسب‌شده از SRFT که در جدول (۲) نشان داده شده است، در تعیین وضعیت ریسک امنیتی دارایی‌ها استفاده می‌گردد. در این جدول، فاکتور ریسک ابزاری برای

3- Security Risk Factor Table

سنجش این موضوع است که آیا یک دارایی نیاز به تحلیل جزئیات آسیب‌پذیری و ارزیابی تهدید دارد یا خیر؟ مطابق با جدول (۳)، چنانچه مجموع نمرات کسب‌شده بیش از ۳۰ گردد تحلیل بیشتر جزئیات درخصوص آسیب‌پذیری و تهدید لازم است [۵].

جدول (۲): فاکتورهای ریسک امنیتی براساس SRFT

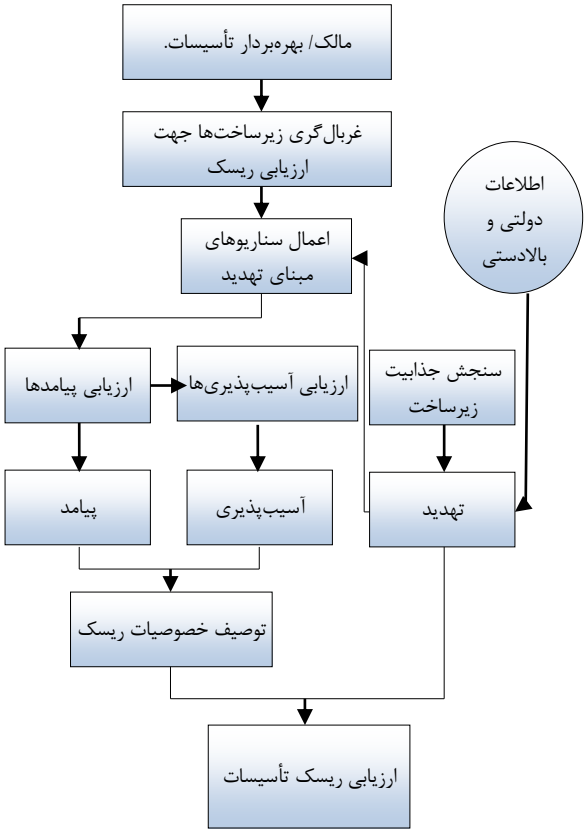
فاکتورهای ریسک	دامنه نمرات ریسک				نمره نهایی
موقعیت	روستایی(۱)	شهری(۲و۳و۴)	تراکم بالا(۵)	-	.....
توانایی دید	عدم دید(۰)	پائین(۱و۲)	متوسط(۳و۴)	بالا(۵)	.....
موجودی	پائین(۱)	متوسط(۲)	بالا (۳و۴)	بسیار بالا (۵)	.....
مالکیت	خصوصی(۱)	عمومی(۲و۳)	-	دولتی (۴و۵)	.....
پیشینه وجود تروریسم در منطقه	عدم وجود(۰)	به ندرت(۱و۲و۳)	-	زیاد (۴و۵)	.....
اقدامات امنیتی موجود	سطح بالا(۱)	معمولی(۲و۳)	-	ضعیف(۴و۵)	.....
کنترل دسترسی	۱	۲،۳	-	۴،۵	.....
پشتیبانی محیطی	۱	۲،۳	-	۴،۵	.....
کاهش اثر مخاطرات	۱	۲،۳	-	۴،۵	.....
روشنایی مطلوب	۱	۲،۳	-	۴،۵	.....
آموزش و آمادگی شخصی	آمادگی خوب۱	آمادگی متوسط ۲،۳	-	ضعیف ۴،۵	.....

جدول (۳): سطح ریسک براساس SRFT

سطح ریسک امنیتی	نمره ریسک واقعی
پائین	<۱۵
متوسط	۱۶-۳۰
بالا	۳۱-۴۵
خیلی بالا	۴۵>

۶-۱-۴- روش RAMCAP [1]

RAMCAP روشی است که چارچوبی برای شناسایی، ارزیابی و مدیریت ریسک برای تجهیزات و دارایی‌های زیرساخت‌های حیاتی در برابر تهدیدات تروریستی ارائه می‌دهد. این روش در پاسخ به پیشنهاد کنفرانس سال ۲۰۰۲ کاخ سفید که در آن بیش از ۱۰۰ مقام ارشد اجرایی از بخش‌های مختلف حضور داشتند و حفاظت از زیرساخت‌های حیاتی ملی را مورد توجه قرار دادند، معرفی گردید. مهم‌ترین اولویت مقام‌های اجرایی تهیه یک روش عینی، اصولی و جامع برای ارزیابی و کاهش ریسک زیرساخت‌ها بود. بعدها این روش برای تأسیسات مختلف از جمله نیروگاه‌های هسته‌ای، مراکز انتقال و ذخیره‌سازی پسمان‌های هسته‌ای، صنایع تولید مواد شیمیایی، پالایشگاه‌های نفت و تأسیسات پتروشیمی، پایانه‌ها و محل‌های بارگیری گاز مایع طبیعی، سدها و سامانه‌های آب و فاضلاب توسعه داده شد. در شکل (۲) فرآیند اجرا در روش RAMCAP آمده است.



شکل (۲): فرآیند گردش داده‌ها در روش RAMCAP

در روش RAMCAP ریسک از برآیند احتمال وقوع تهدید، آسیب‌پذیری و پیامد به‌دست می‌آید (R=T×V×C). ریسک (R)، پتانسیل ایجاد صدمه و خسارت در پی یک وقوع یک تهدید و پیامدهای ناشی از آن است. تهدید (T)، هرگونه نشانه و شرایطی است که پتانسیل ایجاد آسیب و خسارت به دارایی یا تأسیسات را دارا است. در مورد تروریسم، تهدید براساس تجزیه‌وتحلیل قصد و توانایی تروریست برای اجرای اقدامات خصمانه علیه دارایی‌ها، تأسیسات و یا افراد به‌دست می‌آید. آسیب‌پذیری (V)، هرگونه ضعف در طراحی، اجرا و یا فعالیت یک دارایی است که بتواند از سوی دشمن مورد سوء استفاده قرار گیرد. پیامد (C)، نتیجه وقوع یک حادثه از جمله اثرات کوتاه‌مدت، میان‌مدت و بلندمدت و نیز اثرات مستقیم و غیرمستقیم ناشی از آن است و می‌تواند شامل مرگ‌ومیر و جراحت‌های انسانی، خسارت‌های اقتصادی و مالی و تأثیرات زیست‌محیطی باشد. به‌طورکلی روش RAMCAP مشتمل بر هفت گام زیر می‌باشد: [۶]

- توصیف مشخصات دارایی‌ها و انتخاب آن‌ها
- توصیف مشخصات تهدیدات مبتنی بر وضعیت جاری
- تحلیل پیامدها (ملاحظه هزینه‌های مالی، تلفات و آسیب‌ها)

1- Risk Analysis & Management for Critical Asset Protection

- تحلیل آسیب‌پذیری‌ها (تعیین نقاط ضعف موجود در مقابل یک تهدید)
- ارزیابی تهدیدات براساس ارزیابی قابلیت‌ها و نیات دشمن
- ارزیابی ریسک (یک ارزیابی جامع و سیستماتیک از کلیه سناریوهای تهدیدات محتمل در هر دارایی)
- مدیریت ریسک (فرآیند فهم ریسک و تصمیم‌گیری به منظور پیاده‌سازی عملیات کاهش سطح ریسک به یک مقدار قابل قبول)

۶-۱-۵- روش ارزیابی آسیب‌پذیری امنیتی SVA

یکی دیگر از روش‌هایی که با هدف ارزیابی و مدیریت ریسک برای حفاظت از تجهیزات حیاتی صنعت نفت و صنایع وابسته به آن توسعه یافته است و از سوی موسسه API ایالات متحده منتشر گردیده، SVA نام دارد. در این روش به‌طور جامع به ارزیابی تهدیدات امنیتی، آسیب‌پذیری تجهیزات و اجزای صنعت، سطح خطرپذیری امنیتی و ارائه پیشنهادات درخصوص اقدامات بازدارنده و واکنشی در برابر وقوع تهدیدات پرداخته می‌شود. در این سامانه می‌توان دارایی‌ها را هم بصورت کلی و هم بصورت جزئی مورد بررسی قرار داد. اگرچه این روش جهت ارزیابی ریسک توسعه داده شده است اما از آن‌جایی‌که در مورد دارایی‌ها و آسیب‌پذیری‌ها در برابر تهدیدات اهمیت بیشتری قائل شده و اقدامات کاهنده ریسک را نیز در مرتفع‌نمودن نقاط آسیب‌پذیر معرفی می‌کند روش ارزیابی آسیب‌پذیری امنیتی نامیده می‌شود. این روش علاوه‌بر این‌که از انواع منابع نظیر انسانی، مالی، تجهیزاتی و اطلاعاتی به‌طور کافی برخوردار است، از تجربه متخصصین نیز استفاده می‌کند و از دیگر خصوصیات ویژه آن، قابلیت پیش‌بینی و بازخوردگیری است. روش یادشده می‌تواند سطح ریسک هریک از اماکن و تجهیزات محدوده یا صنعت موردنظر را مشخص نماید. این خروجی‌ها که در قالب جداول و نقشه‌های ترکیبی (GIS) نمایش داده می‌شوند، می‌تواند به‌عنوان ابزاری قدرتمند برای پیاده‌سازی طرح‌های پدافند غیرعامل و سامانه مدیریت بحران در اختیار مدیران قرار گیرد.

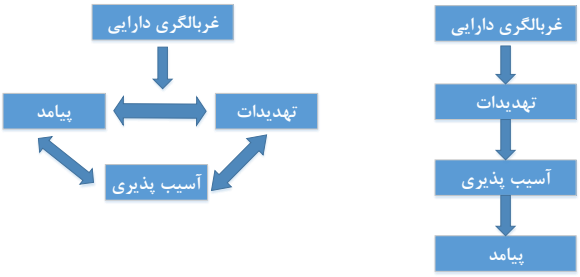
در جدول (۴) روش‌های مختلف ارزیابی ریسک امنیتی با یکدیگر مقایسه شده است. این روش‌ها هریک دارای نقاط قوت و ضعف هستند که برای یک زیرساخت خاص بایستی بهینه‌سازی و تطبیق داده شوند تا نتایج درست‌تری از ارزیابی حاصل شود. در این راستا، روش SVA به نسبت سایر روش‌ها از جامعیت بیشتری برخوردار می‌باشد. با این‌حال، برای زیرساخت‌های هسته‌ای نیاز به اصلاح و تکمیل دارد.

جدول (۴): روش‌های ارزیابی ریسک امنیتی

روش تحلیل ریسک	حوزه ارزیابی ریسک	نوع تحلیل	حوزه مطالعه	سطح اطلاعات مورد نیاز	متخصصین	اجزای روش	ابزارها	قابلیت کاربرد در زیرساخت های هسته ای
FEMA452	امنیتی	کیفی	ساختمان ها و تأسیسات	متوسط	متخصصین مهندسی، معماری	شناسایی دارایی، آسیب پذیری‌ها، پیامد و ریسک	استفاده از جداول راهنمای تهدید، استفاده از ابزارهای تعیین آسیب پذیری، استفاده از جداول راهنمای ریسک	با توجه به اینکه ساختمان و تأسیسات فیزیکی در اولویت ارزیابی قرار دارد استفاده از آن در زیرساخت های هسته‌ای کامل نخواهد بود.
SRFT	امنیتی	کیفی	زیرساخت های فرآیندی	متوسط	تازه کار	تحلیل آسیب‌پذیری و ارزیابی تهدید	استفاده از جدول فاکتور ریسک امنیتی و ماتریس گام به گام	بصورت کلی بوده و استفاده از آن در تأسیسات هسته‌ای اثر بخش نخواهد بود.
RAMCAP	امنیتی	کیفی	کلیه زیر ساخت ها	متوسط	متخصصین حوزه دفاعی، فنی و سیاست گزاری دولتی.	توصیف دارایی‌ها، توصیف تهدیدها، تحلیل پیامدها، تحلیل آسیب‌پذیری، ارزیابی تهدید، ارزیابی و مدیریت ریسک	تدوین جداول دسته بندی تهدید و پیامد، ماتریس دارایی- تهدید، چک لیست محاسبه آسیب پذیری. نرم افزار RAMCAP®	به نسبت FEMA452 از جامعیت کمتری برخوردار بوده و نیاز به ایجاد تغییراتی جهت استفاده درتأسیسات هسته ای دارد.
SVA	امنیتی	کیفی	صنایع نفت و گاز و پتروشیمی	بالا	متخصصین امنیت فیزیکی، امنیت سایبری، مدیریت بحران، متخصص فرآیندی.	توصیف دارایی‌ها، توصیف تهدیدها، تحلیل پیامدها، تحلیل آسیب‌پذیری، ارزیابی تهدید، ارزیابی ریسک، مدیریت ریسک.	ماتریس ارزیابی ریسک، سناریو، چک‌لیست‌های ارزیابی آسیب‌پذیری به تفکیک اجزای زیرساخت و حفاظت فیزیکی، نرم‌افزار SVA pro	این روش قابل استفاده در تأسیسات هسته‌ای است. با این حال از محتوای لازم در این زمینه برخوردار نمی‌باشد. به همین دلیل می‌بایست با روش‌های دیگر ادغام شود.

۷- روش ارزیابی ریسک پیشنهادی

پس از بررسی و مطالعه مدل‌های ریسک ذکرشده، فاکتورهای ارزیابی و شناسایی دارایی، تهدیدات، آسیب‌پذیری و درنهایت، پیامد ناشی از تهدید مورد بررسی قرار گرفته است. با این وجه تمایز که در فرمول ارزیابی ریسک در برخی مدل‌های پیامد و در برخی دیگر ارزش دارایی نادیده گرفته شده است. همچنین، سلسله مراتبی و خطی‌بودن ارزیابی‌ها، ضعف عمده این مدل‌ها به‌شمار می‌آید. مدل کلی پیشنهادی این پژوهش به شکل ذیل می باشد:



شکل (۳): مقایسه مدل‌های ارزیابی ریسک (خطی و شبکه‌ای)

با توجه به مدل ارایه‌شده فوق در مرحله اول دارایی و زیرساخت‌های مهم هر صنعت با استفاده از معیارهای سنجش دارایی، غربالگری شده و به‌عنوان متغییر مستقل جزء ثابت ارزیابی می‌باشد. درواقع، در ارزیابی گام ابتدایی و لازم، شناسایی دارایی‌های مهم است. پس از دارایی‌شناسی هریک از مولفه‌های آسیب‌پذیری و تهدید و پیامد، متناظر با هریک از دارایی‌ها ارزیابی می‌شود. در ادامه به نحوه ارزیابی با استفاده از مدل تحلیل شبکه پرداخته خواهد شد.

۸- کاربرد فرایند تحلیل شبکه‌ای در ارزیابی ریسک

تصمیم‌گیری می‌بایست در یک فضای چندبعدی صورت پذیرد. در چنین شرایطی، روش‌های ارزیابی چندمعیاری با توجه به این‌که در این روش‌ها فرض بر این است که هریک از معیارها محور یا بعد جداگانه‌ای هستند، می‌توانند مورد استفاده قرار گیرند. یکی از روش‌های پرکاربرد در تصمیم‌گیری‌های چندمعیاره فرایند تحلیل شبکه‌ای است. این روش گسترش‌یافته شبکه AHP است. در فرآیند سلسله مراتبی وابستگی‌ها به‌صورت خطی (یعنی از بالا به پایین و یا برعکس) است. حال اگر وابستگی دوطرفه باشد، یعنی وزن شاخص‌ها به گزینه‌ها و وزن گزینه‌ها به شاخص‌ها وابسته باشد، مساله از گونه سلسله مراتبی خارج شده و تشکیل یک شبکه یا سامانه غیرخطی را می‌دهد. [۷] ازجمله مزایای این روش به‌کارگیری معیارهای کمی و کیفی به‌طور همزمان است و نیز می‌تواند ارتباطات پیچیده (وابستگی های متقابل و بازخورد) بین و میان عناصر تصمیم را با به‌کارگیری ساختار شبکه‌ای به‌جای ساختار سلسله مراتبی در نظر بگیرد. تفاوت بین یک "ساختار سلسله مراتبی" و "ساختار شبکه‌ای" در شکل (۳) ارایه شده است. فرآیند تحلیل شبکه‌ای هر موضوع و مسئله‌ای را به مثابه شبکه‌ای از معیارها، زیرمعیارها و گزینه‌ها که با یکدیگر در خوشه‌هایی جمع شده‌اند، در نظر می‌گیرد. تمامی عناصر در یک شبکه می‌توانند به هر شکل دارای ارتباط با یکدیگر باشند. به عبارت دیگر، در یک شبکه، بازخورد و ارتباط متقابل بین و میان خوشه‌ها امکان‌پذیر است [۷].

۸-۱- انتخاب (تعیین الویت) سایت هسته‌ای جهت تهدید

قرار است از بین سه سایت شناسایی‌شده (A,B,C) دارای ضعف و آسیب‌پذیری بالا جهت حمله، انتخاب شود. لذا برای انتخاب سایتی که پتانسیل بیشتری برای تهدید باشد مراحل زیر طی می‌شود:

۸-۱-۱- بررسی مولفه‌های ارزیابی ریسک (معیارها و زیرمعیارها)

در گام اول، فضاها و زیرفضاها و یا مجموعه‌های وابسته زیرساخت و نحوه ارتباط آن‌ها با یکدیگر شناسایی و اولویت‌بندی خواهند شد. پس از انتخاب مراکز حیاتی و حساس شبکه، نوبت به شناخت زیرفضاها و دارایی‌های حیاتی هر مرکز می‌رسد. به‌عنوان مثال، ابتدا سایت‌های هسته‌ای کشور شناسایی شده و در گام بعد نوبت به شناخت زیرساخت‌ها و دارایی‌های مهم هر سایت می‌رسد که با استفاده از شاخص‌های ذیل این دارایی‌ها شناسایی و غربالگری خواهند شد [۹].

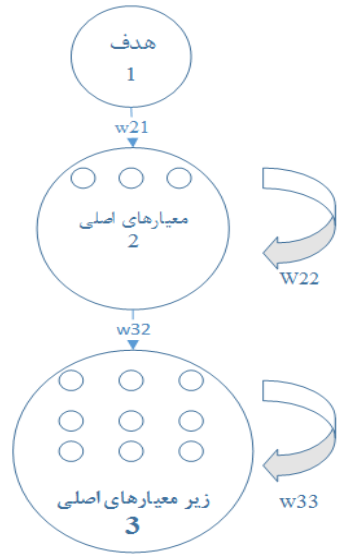
پس از استخراج دارایی‌های مهم در گام نخست، کلیه معیارهای ارزیابی و سنجش‌های لازم که از مطالعات نظری پژوهش حاصل شده است که عبارتنداز: شناسایی تهدیدات، آسیب‌پذیری و پیامد. پس از تعیین و مشخص‌نمودن معیارها و زیرمعیارهای موثر در تعیین سایت مناسب جهت حمله، لازم است ارتباط بین این عوامل (معیارها و زیرمعیارها) نیز مشخص می‌شود. مدل شبکه‌ای برای تعیین سایت مناسب در شکل (۳) ارایه شده است. این شکل نشان می‌دهد که گزینه‌ها به‌طور جداگانه مورد بررسی قرارهای درونی معیارها به یکدیگر نشان می‌دهد. همچنین، زیرمعیارهای اساسی منتج از معیارها که به شرح شکل (۵) معیار و زیرمعیارهای ارزیابی ذیل تشریح می‌گردد:

برخلاف فرآیند تحلیل سلسله مراتبی که ارتباط بین معیارها، زیرمعیارها و گزینه‌ها، سلسله مراتبی و یک سویه است، در فرآیند تحلیل شبکه‌ای، افزون بر ارتباط سلسله مراتبی، در بخش‌هایی از

مدل ممکن است معیارها و زیرمعیارها با یکدیگر ارتباط و وابستگی متقابل داشته باشند. لازم است با توجه به ساختار شبکه‌ای مدل (شکل ۶) ساختار کلی سوپر ماتریس اولیه مشخص می‌شود. با توجه به شکل (۶) که ارتباط و وابستگی‌های بین معیارها و زیرمعیارها را نشان می‌دهد. ساختار سوپرماتریس اولیه به شرح جدول (۵) می‌باشد.

جدول (۵): وابستگی‌های درونی معیارها

معیارها	دارایی	تهدید	آسیب‌پذیری	پیامد
دارایی		√	√	√
تهدید	√		√	√
آسیب‌پذیری	√	√		√
پیامد	√	√	√	



شکل (۶): ارتباط و وابستگی بین معیارهای و زیرمعیارها [۱۰]

برای تعیین ضریب اهمین معیارها و زیر معیارها، با استفاده از جدول (۶) دو به دو آنها را مقایسه می‌کنیم .

جدول (۶): مقیاس ۹ کمیتی saaty

تعریف	امتیاز	تعریف	امتیاز
اهمیت بیشتر	۵	اهمیت مساوی	۱
اهمیت خیلی بیشتر	۷	اندکی بیشتر اهمیت	۳
حالت میانه	۲,۴,۶,۸	اهمیت مطلق	۹

برای دستیابی به الویت های کلی، دریک سامانه با تاثیرات متقابل، بردارهای الویتای داخلی(یعنی Wهای محاسبه شده) درستون‌های مناس یک ماتریس وارد می‌شوند. در نتیجه یک سوپر ماتریس که هر بخش از این ماتریس ارتباط بین دو خوشه دریک سامانه را نشان می‌دهد، بدست می آید. در جدول (۷) W21 برداری است که اثرات هدف برروی معیارها و W32 اثرات معیارها بر روی گزینه‌ها را نشان می‌دهند و W33 ماتریس واحد است

جدول (۷): ساختار سوپر ماتریس اولیه ناموزون

$$\begin{bmatrix} \text{هدف} & \text{اصلی معیار} & \text{زیرمعیار} \\ \cdot & \cdot & \cdot \\ W۲۱ & \text{W۲۲} & \cdot \\ \cdot & W۳۲ & W۳۳ \end{bmatrix}$$

۸-۲- تشکیل ماتریس‌های مقایسه‌ای:

در این گام ماتریس‌های مقایسه‌ای معیارهای اصلی، وابستگی معیارهای اصلی به یکدیگر، زیرمعیارها و وابستگی زیرمعیارها به یکدیگر تشکیل می شود.

۸-۲-۱- مقایسه دودویی معیارهای اصلی

مقایسه دودویی معیارهای اصلی براساس مقیاس ۹ کمیتی Saaty طبق جدول (۷) انجام می‌شود [۱۱]. نتیجه مقایسه دودویی و بردار W21 در ادامه ذکر شده است (جدول ۸). برای افزایش دقت در نتایج از قضاوت گروهی متخصصان جهت امتیازدهی استفاده شده است که بدین منظور روش میانگین هندسی به‌منظور برآیند امتیازات حاصله به‌کار گرفته شده است.

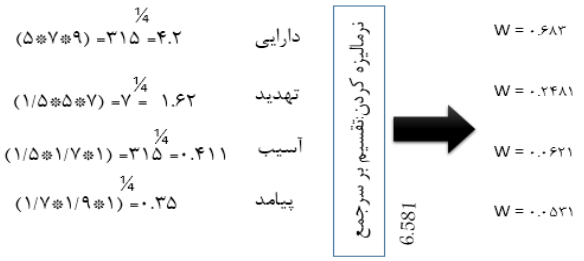
جدول (۸): مقایسه دودویی معیارهای اصلی

معیارها	دارایی	تهدید	آسیب	پیامد
دارایی	۱	۵	۷	۹
تهدید	۱/۵	۱	۵	۷
آسیب	۱/۷	۱/۵	۱	۱
پیامد	۱/۹	۱/۷	۱	۱

به منظور محاسبه ضریب اهمیت معیارها ، روش میانگین هندسی مورد استفاده قرار گرفته است بدین صورت که ابتدا میانگین هندسی ردیف های ماتریس دودویی معیارهای اصلی محاسبه و سپس نرمالیزه می شود.

جدول (۹):بردار ویژه معیارهای اصلی

$$W21=\begin{bmatrix} 0.683 \\ 0.2481 \\ 0.0621 \\ 0.0531 \end{bmatrix}$$



شکل (۷): نحوه محاسبه بردار ویژه اصلی

۸-۳- مقایسه دودویی وابستگی‌های درونی معیارهای اصلی (ماتریس W22)

برای دستیابی به ماتریس W22 و بررسی وابستگی‌های متقابل بین معیارهای اصلی، مقایسه دودویی بین معیارهای اصلی به شرح ذیل انجام می‌شود. همچنین، برای محاسبه ضریب اهمیت هریک از معیارهای اصلی، مقایسه دودویی معیارهای اصلی سه‌گانه دیگر (با کنترل‌کردن معیاره اول یعنی دارایی) در جدول (۱۰) ارائه شده است.

سه ماتریس مقایسه دودویی دیگر، متناظر ماتریس ارائه‌شده در جدول (۱۰)، لازم است تشکیل شده تا بتوان ماتریس مربوط به وابستگی‌های متقابل معیارهای اصلی (W22) را محاسبه کرد.

جدول (۱۰): مقایسه دودویی معیارهای اصلی

W	پیامد	تهدید	آسیب	
۰/۰۳۰۱۶	۱/۹	۱	۱/۷	تهدید
۰/۹۶۹۴	۱/۵	۷	۱	آسیب
۰/۰۰۳۴۱	۱	۹	۵	پیامد

با توجه به وابستگی درونی آن‌ها، با کنترل شاخص دارایی کرد. پس از تشکیل این سه ماتریس و انجام محاسبات لازم، نتایج حاصله در ماتریس W22 (جدول ۱۱) ارائه شده است.

جدول (۱۱): ماتریس W22

پیامد	آسیب	تهدید	دارایی	
۱/۷۴۵۵	۱,۳۵۷۲	۰/۷۵۴۰۵	۰	دارایی
۰/۰۰۰۳۴۹۱	۰/۰۰۰۴۷۸	۰	۰/۰۳۰۱۶	تهدید
۰/۰۱۶۷۵	۰	۰/۰۰۴۳۰۸	۰/۹۶۹۴	آسیب
۰	۰/۰۱۵۳۸	۰/۰۰۳۰۷۷	۰/۰۰۳۴۱	پیامد

۸-۴- مقایسه دودویی زیرمعیارهای از معیارهای اصلی (ماتریس W32)

ضریب اهمیت هریک از زیرمعیارهای مربوط به معیارهای اصلی چهارگانه از طریق مقایسه دودویی آن‌ها به‌دست‌آمده که عناصر ستونی ماتریس W32 را تشکیل خواهند داد. نتیجه مقایسه دودویی زیرمعیارهای مربوط به معیار "ارزش دارایی" و بردار ویژه حاصل از آن در جدول (۱۲) ارائه و نتیجه در ماتریس W32 جدول (۱۳) ارائه شده است.

جدول (۱۲): مقایسه دودویی زیرمعیارهای مربوط به دارایی‌شناسی

بردار ویژه	انحصار	دامنه اثر	عملکردی	سرمایه	
۰/۳۲۴۱	۱/۵	۳	۵	۱	سرمایه
۰/۱۷۴۳	۷	۳/۱	۱	۱/۵	عملکردی
۰/۳۸۴۲	۵	۱	۳	۱/۳	دامنه اثر
۰/۱۱۷۲	۱	۱/۵	۱/۷	۵	انحصار

در این مرحله، ضریب اهمیت هریک از زیرمعیارهای مربوط به معیارهای اصلی چهارگانه از طریق مقایسه دودویی آنها(براساس مقیاس ۹ کمیتی saaty) بدست آمده و این ضرایب اهمیت،عناصر ستونی ماتریس W32 جدول (۱۳) را تشکیل خواهند داد.

جدول(۱۳): ماتریس W32

پیامد	آسیب	تهدید	دارایی	
0	0	0	0.324135	سرمایه ای
0	0	0	0.1743228	عملکردی
0	0	0	0.3842917	دامنه اثر
0	0	0	0.1172506	انحصار و جایگزینی
0	0	0.040179	0	سابقه تهدید
0	0	0.4299172	0	-هزینه -فایده
0	0	1.2570855	0	-توانایی دشمن
0	0	0.117484	0	شدت خسارت
0	0.05206072	0	0	-امکان شناسایی
0	0.0029154	0	0	-ضعف حفاظتی
0	0.15618076	0	0	-امکان دسترسی
0	0.00004628	0	0	-ضعف فرایندی
0	0.00003623	0	0	همجواری
0.91835205	0	0	0	سلامت و امنیت افراد
0.07288506	0	0	0	فشارهای اقتصادی
0.00874621	0	0	0	-فشارهای امنیت ملی
0.00001417	0	0	0	-اثرات روانی
0.00000283	0	0	0	-اثرات اجتماعی

۸-۵- مقایسه دودویی وابستگی‌های درونی زیرمعیارها (ماتریس W33)

با توجه به مطالعات انجام‌شده در این پژوهش زیرمعیارهایی به شرح شکل (۵) استخراج و تبیین گردید که در واقع بیان‌کننده ویژگی‌های چهار معیار اصلی می‌باشد، تاثیر و ارتباط متقابل بین زیرمعیارها توسط کارشناسان خبره تعیین می‌شود. در گام اول مقایسه دودویی هریک از زیرمعیارها که دارای وابستگی متقابل با زیرمعیار موردنظر است، بررسی (جدول ۱۴) و سپس ماتریس W33 (جدول ۱۵)تشکیل می‌شود.

جدول (۱۴): مقایسه دودویی زیرمعیارهای دارای وابستگی متقابل با زیرمعیار ارزش سرمایه‌ای

	عملکردی	دامنه اثر	سایقه تهدید	شدت خسارت	همجواری	سلامت و امنیت افراد	فشارهای اقتصادی	اثرات - روانی		
عملکردی	1.00	3.00	0.14	0.33	5.00	0.20	9.00	0.11	0.76	**0.08**
دامنه اثر	0.33	1.00	0.20	3.00	0.44	9.00	0.33	0.14	0.74	**0.078**
تهدید	7.14	5.00	1.00	5.00	0.33	9.00	3.00	5.00	2.73	**0.29**
خسارت	3.00	0.33	0.20	1.00	1.00	0.20	0.20	5.00	0.54	**0.058**
همجواری	0.20	2.25	3.00	1.00	1.00	3.00	3.00	4.00	2.19	**0.23**
سلامت و	5.00	0.11	0.11	5.00	0.33	1.00	5.00	9.00	0.99	**0.106**
اقتصادی	0.11	3.00	0.33	5.00	0.33	0.20	1.00	3.00	1.00	**0.101**
روانی-	9.00	6.92	0.20	0.20	0.25	0.11	0.33	1.00	0.43	**0.046**

جدول (۱۵): ماتریس W33

0	0.051	0.23	0	0.023	0	0	0.023	0	0	0	0	0.069	0.56	0.0125	0	0.2045	0
0.081	0	0.0362	0	0.254	0	0	0.0036	0	0	0.042	0	0.0564	0	0.2208	0.002	0.023	0.311
0.078	0.002	0	0	0	0.045	0.03	0.01	0	0.021	0	0.205	0.136	0.0012	0.00045	0.26	0.0045	0.06
0	0	0	0	0	0.326	0	0.0023	0	0	0	0.2156	0.002414	0	0.01246	0.415	0.0156	0.003
0.291	0.0658	0	0	0	0.125	0.0145	0	0.02516	0	0.2865	0.236	0.0025	0.0125	0.00256	0.02156	0.0378	0.1456
0	0	0.003	0.07856	0	0	0.04786	0.145	0.0236	0.025654	0.05	0	0.015	0	0.01255	0.1526	0.233	0.213
0	0	0.156	0	0.023	0.078	0	0.0085	0.0156	0	0.05	0.23	0.201	0	0	0	0.0215	0.212
0.058	0.023	0.23136	0.00125	0	0.033	0.121	0	0.001	0.023	0.22	0.002	0.0002	0.0125	0.15	0.136	0.003	0.021321
0	0	0	0	0.0205	0.25	0.0223	0.287	0	0.0232	0.4	0	0	0	0	0	0	0
0	0	0.25	0	0	0.165	0	0.123	0.022	0	0.022	0	0.022	0.002	0.144	0.15	0.1	0.01
0	0.2	0	0	0.33		0.02	0.002	0.029	0.3555	0	0	0.01	0.02	0.021	0.02	0	0
0	0	0.25	0.422	0.14	0	0.101	0.002	0	0	0	0	0	0.092	0	0	0	0
0.234	0	0.059	0.035	0.15	0.045	0.075	0.056	0	0.0242	0.0692	0	0	0.069	0	0	0	0.34
0.106	0	0.315	0	0.002	0	0	0.087	0	0.0125	0.231	0.0316	0.0089	0	0	0	0.02125	0.23
0.107	0.056	0.36	0.0015	0.005	0.021	0	0.125	0	0.265	0.015	0	0	0	0	0.002	0.0856	0.058
0	0.32	0.0674	0.025	0.0023	0.00176	0	0.0541	0	0.0546	0.1	0	0	0	0.012	0	0.31	0.05214
0.046	0.0256	0.096862	0.1639	0.02145	0.0445	0.115	0.0052	0	0.0369	0	0	0	0.2265	0.028103	0.0056	0	0.02115
0	0.002	0.0041	0.044	0.07452	0.0411	0.17	0.124	0	0.133	0	0	0	0.03463	0.084	0.287	0.01	0

جدول(۱۶): ماتریس Eij

A	۰.۷۲	۰.۴۳	۰.۳۵	۰.۲۳	۰.۳۵	۰.۱۴	۰.۴۶	۰.۴۵	۰.۶۴	۰.۴۲	۰.۲۱	۰.۴۶	۰.۵۳	۰.۴۵	۰.۴۵	۰.۴۲	۰.۴۳	۰.۳۳	۰.۴۶
B	۰.۲۳	۰.۳۴	۰.۳۲	۰.۳۶	۰.۴۰	۰.۲۳	۰.۲۳	۰.۳۸	۰.۳۳	۰.۲۳	۰.۴۷	۰.۲۴	۰.۳۶	۰.۳۳	۰.۳۳	۰.۳۴	۰.۳۵	۰.۲۵	۰.۲۴
C	۰.۰۵	۰.۲۳	۰.۳۳	۰.۴۳	۰.۲۵	۰.۶۳	۰.۳۱	۰.۱۷	۰.۰۴	۰.۳۶	۰.۳۲	۰.۳۰	۰.۱۲	۰.۲۳	۰.۲۳	۰.۲۴	۰.۲۳	۰.۴۲	۰.۳۰

۸-۶- مقایسه دودویی گزینه برتر

در این مرحله ارجحیت هریک از گزینه (سایت‌های A B C) در ارتباط با هریک از زیرمعیارها، مورد بررسی و قضاوت کارشناسان قرار می‌گیرد که طبق مقیاس ۹ کمیتی Saaty صورت می‌گیرد و در آن بحث ارجحیت گزینه‌ها مطرح است. در جدول (۱۷)، مقایسه دودویی ارجحیت گزینه‌ها در ارتباط با زیرمعیار "ارزش سرمایه ای" ارائه شده است. برای تعیین میزان ارجحیت گزینه‌ها در ارتباط با سایر زیرمعیارها نیز چنین ماتریس‌هایی باید تشکیل و بردار ویژه آن‌ها محاسبه شود و نتایج آن در ماتریس Eij جدول (۱۶)ارائه شده است.

جدول (۱۷): مقایسه دودویی ارجحیت گزینه‌ها (سایت‌های هسته‌ای) در

ارتباط با زیرمعیار ارزش سرمایه‌ای Eij

گزینه	A	B	C	بردرا ویژه
سایت A	۱	۵	۹	۰/۷۲
سایت B	۱/۵	۱	۷	۰/۲۳
سایت C	۱/۹	۱/۷	۱	۰/۰۵

۸-۷- محاسبه سوپرماتریس حد

جهت محاسبه سوپرماتریس حد مراحل زیر باید محاسبه گردد:

۸-۷-۱- تشکیل سوپرماتریس ناموزون

با توجه به محاسبه تمامی ماتریس‌های ناموزون (W21 W22 W32 W33) می‌توان با جایگزین‌کردن این ماتریس‌ها در سوپرماتریس اولیه (جدول 7) سوپر ماتریس ناموزون را به‌دست آورد.

و نهایتاً می‌بایست سوپرماتریس ناموزون را به سوپرماتریس موزون یعنی ماتریسی که جمع اجزای ستون آن ۱ است، تبدیل شود. بدین منظور، باید سوپرماتریس ناموزون را در ماتریس خوشه‌ای ضرب کرد. ماتریس خوشه‌ای از مقایسه دودویی خوشه‌ها در چارچوب ساختار سوپرماتریس اولیه حاصل می‌شود.

۸-۷-۲- تشکیل سوپرماتریس موزون

برای به‌دست‌آوردن سوپرماتریس موزون، هریک از عناصر خوشه‌های ستونی سوپرماتریس ناموزون در ضریب اهمیت نسبی آن خوشه (از ماتریس خوشه‌ای) باید ضرب شود.

جدول (۱۸): ماتریس خوشه‌ای

زیرمعیارها	معیارهای اصلی	هدف	
۰	۰	۰	هدف
۰	۰/۶۶۷	۱	معیارهای اصلی
۱	۰/۳۳۳	۰	زیرمعیارها

۸-۷-۳- تشکیل سوپرماتریس حد

هدف از به حدرساندن سوپرماتریس موزون این است که تاثیر نسبی درازمدت هریک از عناصر آن در یکدیگر حاصل شود. برای واگرایی ضریب اهمیت هریک از عناصر ماتریس موزون، آن‌را به توان K که یک عدد اختیاری بزرگ است، می‌رسانیم تا این‌که همه عناصر سوپرماتریس همانند هم شوند.[۹]

۹- تعیین سایت هسته‌ای جهت حمله خصمانه

به‌منظور تعیین سایت مناسب جهت انهدام تاسیسات هسته‌ای از رابطه پیشنهادی H Lin [۱۲]به شرح زیر استفاده می‌کنیم:

رابطه (۱): $Di = \sum_{j=1}^{J} wjEij$

که در آن، Di شاخص مطلوبیت سایت i برای حمله، Wj اهمیت نسبی زیرمعیار j و Eij امتیاز سایت i از زیرمعیار j می‌باشد.

مطلوبیت حمله به سه سایت هسته‌ای مدنظر (Di) با استفاده از رابطه فوق‌الذکر محاسبه و نتایج پس از تعیین رتبه سایت‌ها در ردیف آخر جدول (۱۹) ارائه شده است که در آن، سایت A با امتیاز ۰/۴۱۱ مطلوب‌ترین سایت جهت حمله ازنظر دشمن انتخاب می‌شود.

جدول (۱۹): محاسبه شاخص مطلوبیت حمله به سایت‌های هسته‌ای

معیار	زیرمعیار	Wj	Eij			wj Eij		
			سایت A	سایت B	سایت C	سایت A	سایت B	سایت C
ارزش دارایی	سرمایه ای	0.112	0.723	0.227	0.051	0.08097	0.02547	0.006
	عملکردی	0.031	0.433	0.34	0.23	0.01343	0.01054	0.007
	دامنه اثر	0.085	0.345	0.325	0.33	0.02933	0.0276	0.028
	جایگزینی	0.055	0.225	0.356	0.425	0.01238	0.01956	0.023
تهدید	سابقه	0.102	0.35	0.4	0.25	0.0357	0.0408	0.026
	هزـفا	0.106	0.141	0.234	0.625	0.00149	0.00248	0.007
	توانایی	0.103	0.458	0.226	0.31	0.04712	0.02325	0.032
	خسارت	0.041	0.446	0.376	0.17	0.01827	0.01541	0.007
آسیب پذیری	شناسایی	0.061	0.637	0.327	0.04	0.03886	0.01995	0.002
	حفاظتی	0.014	0.423	0.234	0.355	0.00592	0.00328	0.005
	دسترسی	0.016	0.212	0.467	0.323	0.00297	0.00654	0.005
	فرایندی	0.025	0.457	0.237	0.3	0.01143	0.00593	0.008
	همجواری	0.056	0.528	0.358	0.12	0.0298	0.0202	0.007
پیامد	امنیت	0.043	0.453	0.326	0.23	0.01947	0.01401	0.01
	اقتصادی	0.03	0.425	0.34	0.24	0.01274	0.0102	0.007
	امنیت ملی	0.065	0.432	0.345	0.23	0.02811	0.02243	0.015
	روانی	0.012	0.334	0.255	0.42	0.00401	0.00305	0.005
	اجتماعی	0.042	0.461	0.242	0.298	0.01937	0.01016	0.013
	$Di = \sum_{j=1}^{J} wjEij$					0.41136	0.280827	0.21112

۱۰- نتیجه‌گیری

از مهم‌ترین اقدامات پیشگیرانه با رویکرد پدافند غیرعامل، شناخت و تصمیم‌گیری در نحوه شناسایی و اولویت‌بندی راه‌کارها جهت کاهش آسیب‌پذیری زیرساخت‌های مهم، باید دانست. تصمیم‌گیری شامل بیان درست اهداف، تعیین راه‌حل‌های مختلف و ممکن، ارزیابی امکان‌پذیری آنان، ارزیابی عواقب و نتایج ناشی از اجرای هریک از راه‌حل‌ها و بالاخره انتخاب و اجرای آن می‌باشد. کیفیت مدیریت اساساً تابع کیفیت تصمیم‌گیری است زیرا کیفیت طرح و برنامه‌ها، اثربخشی و کارآمدی راه‌بردها و کیفیت نتایجی که از اعمال آن‌ها به‌دست می‌آید همگی تابع کیفیت تصمیماتی است که مدیران و نخبگان اتخاد می‌نماید. در اکثر موارد، تصمیم‌گیری‌ها وقتی مطلوب و مورد رضایت تصمیم گیرنده است که تصمیم‌گیری براساس چندین معیار مورد بررسی قرار گرفته باشد. در روش‌های تصمیم‌گیری چندمعیاره که در این مقاله فرآیند تحلیل شبکه مورد استفاده قرار گرفت، به‌جای استفاده از یک معیار (مدل خطی) سنجش بهینگی از چند معیار سنجش استفاده می‌شود.

در این مقاله، پس از تشریح انواع مدل‌های ارزیابی ریسک مبتنی بر حملات خصمانه، فاکتورهای ارزیابی استخراج گردید. در مدل‌های فوق روش ارزیابی ریسک مبتنی بر مدل خطی است. در واقع، ضعف مدل خطی در این توع تصمیم‌گیری‌ها در این است که اثرات هم‌زمان معیارها را درنظر نمی‌گیرد. به‌عنوان مثال، نخستین گام در مدل‌های ارزیابی ریسک خطی، غربالگری دارایی‌های با ارزش است، درصورتی‌که دارایی با معیارهای مختص به خود سنجیده می‌شود و بسیاری از دارایی‌ها حذف می‌شود. این درحالی است که درصورت بررسی سایر معیارها اعم از پیامد و آسیب‌پذیری، دارایی مورد نظر حذف نشود. به‌عنوان مثال، دارایی مانند پمپ بنزین در نگاه اول با ارزش پایین تلقی و حذف می‌شود درحالی‌که انهدام این دارایی ممکن است دارای پیامدهایی اثرگذار با مقیاس بالا باشد. لذا بررسی هم‌زمان معیارهای ارزیابی ریسک در شناسایی و اولویت‌بندی زیرساخت‌های اساسی و طبیعتاً کاهش آسیب‌پذیری که هدف نهایی پدافند غیرعامل است، ضروری می‌باشد. با توجه به ضرورت ذکرشده در راستای ارزیابی ریسک، مدل فرآیند تحلیل شبکه از یک طرف، این امکان را به ارزیاب می‌دهد که به بررسی دودویی معیارها و زیرمعیارهای ریسک پرداخته و به‌طور هم‌زمان تمامی عوامل تاثیرگذار در ریسک امنیتی را بررسی که منجر به جلوگیری از حذف غیراصولی معیارها خواهد شد. از طرفی دیگر، به‌کارگیری از نخبگان و صاحب‌نظران در تعیین الویت و ارزش اثرگذاری معیارها منجر به افزایش دقت و کارایی ارزیابی ریسک نهایی خواهد شد.

۱۱- مراجع

1. M. Garcia-Melon, J. Ferris-Onate, J. Aznar-Bellver, P. Aragonés-Beltran, and R. Poveda-Bautista, "Farmland appraisal based on the analytic network Process," Journal of Global Optimization, vol. 2, pp. 143-155, 2008.
2. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology#The_OWASP_Risk_Rating_Methodology

۳. زارعی، اسماعیل، در محمدی، علی، ارزیابی ریسک نیمه کمی و کمی در صنایع فرایندی، انتشارات فن آوران، شماره۱۲، ۱۳۹۲.

4. A How-to Guide to Mitigate Potential Terrorist Attacks against Buildings /FEMA 452 /, p. 18, January 2005.

۵. توفیق، فیروز، ارزشیابی چند معیاری در طرح ریزی کالبدی، مجله آبادی، ص. ۴۴، ۱۳۷۲.

۶. پژوهشکده پدافند غیرعامل دانشگاه صنعتی مالک اشتر، ارزیابی ریسک تاسیسات صنعتی، ص. ۶۴، ۱۳۹۲..

۷. مومنی، منصور، شریفی سلیم، علیرضا، مدل ها و نرم افزارهای تصمیم گیری چند شاخصه، انتشارات گنج شایگان، شماره ۹۰، ۱۳۹۴

۸. ذوالقدر، محمد، الگوی ارزیابی ریسک امنیتی و خارجی سامانه های آبرسانی، پایان نامه کارشناسی ارشد، ص. ۱۳۵، ۱۳۹۱.

۹. رزقانی، سیدهادی، و همکاران، تحلیل ریسک اهمیت مراکز حیاتی، حساس و مهم کلانشهر مشهد، فصلنامه مطالعات برنامه ریزی شهری، ص. ۱۲، ۱۳۹۲.

۱۰. زبردست، اسفندیار، کاربرد فرایند تحلیل شبکه، نشریه هنرهای زیبا، ص. ۱۶، ۱۳۸۹.

11. T. L. Saaty and J. M. Alexander, "The Thinking with Models, Mathematical Model in Physical and Social Science, Oxford Pergamon Press, pp.48-155, 1988.
12. Y.-H. Lin, K.-M. Tsai, and W.-J. Shiang, "Research on using ANP to establish a performance assessment model for business intelligence systems," Expert Systems with Application, vol. 36, pp. 4135-4146, 2009.

Risk Assessment of Hostile Attacks Using Analytic Network Process Model

M. Zolghadr, M. J. Gholami*

Abstract

Investigating the factors and identifying the type of potential threats and risks of important assets at the time of incidents are of the key measures in reducing vulnerability with the passive approach. Therefore, in order to develop the most likely scenario to prevent or reduce vulnerability and the consequences, we need to develop comprehensive indicators and risk analysis techniques. In the present models, all stages of risk analysis are linear, while it can be a major weakness in the evaluation process. For example, in the asset screening stage, an asset that does not have a high value in terms of assets is eliminated, but with high potential for large system vulnerabilities. In fact, due to the nature of the linearity of the models, the asset is eliminated in the first stage and prevents evaluation in the next steps (vulnerability assessment). Due to the weakness of linear models for determining the priority of the vulnerability of the three nuclear sites, the network analysis process model has been used. The research method of the present study is based on the purpose of the developmental type. From the nature of the subject, a description of the library resources and the views of the elites to examine the proposed models have been used. Finally, while explaining the indicator, the model of the network analysis process is described in order to evaluate the final risk, which is the most risk related to sites A, B, C.

Key Words: *Indices, risk analysis Assessment methods,Network analysis process*

* Islamic Azad University, Science and Research Branch, Tehran (Mj_gholamikhooeini@yahoo.com)- Writer-in-Charge