دریافت مقاله: ۱۳۹۴/۰۴/۱۳
پذیرش مقاله: ۱۳۹۴/۰۶/۱۹

فصلنامه مدیریت نظامی
شماره ۵۸، سال پانزدهم، تابستان ۱۳۹۴
ص ص ۴۳-۶۹

تحلیل ریسک در سازمان‌های نظامی

(شناسایی و اولویت‌بندی ریسک‌های بحرانی در پایگاه‌های پدافند هوایی)

علیرضا موغلی[۱]، سعید عبدالمنافی[۲]، حسن صالحی[۳]، شهناز محمود صالح[۴]

چکیده

مدیریت ریسک‌ها و مخاطرات یکی از ملزومات اساسی ارتش‌های نوین است. امروزه بدون پیاده‌سازی فرایندهای علمی و منطقی، قادر به شناسایی و رفع مخاطرات در محیط‌های پویا و فناورانه نخواهیم بود. هدف از این تحقیق، شناسایی و اولویت‌بندی مخاطرات اثرگذار بر تداوم عملیات پایگاه‌های راداری، موشکی و شناسایی الکترونیک است. این تحقیق از نوع کاربردی و به شیوهٔ توصیفی-پیمایشی می‌باشد که به روش مقطعی در یک مرکز نظامی صورت گرفته است. حجم نمونه شامل ۴۹ نفر از خبرگان و متخصصان فرماندهی و مدیریت پایگاه‌های پدافندی در استان‌های فارس و بوشهر و خوزستان است. ابزارِ جمع‌آوری داده‌ها، مشتمل بر ۳ پرسشنامه است که بر اساس فن RFMEA طراحی شدند. روش مورد استفاده برای ارزیابی ریسک‌ها، فن ویلیام فاین در ارزیابی ریسک و فن تجزیه و تحلیل حالت خطا و اثر شکست ریسک است. برای تحلیل داده‌ها از روش‌های آماری توصیفی و استنباطی به کمک نرم افزار SPSS19 استفاده گردید. یافته‌ها حاکی از آن است که ریسک‌های حوزهٔ تعمیر و نگهداری و حوزهٔ مدیریت نیروی انسانی، به ترتیب با ضریب اهمیت۲۰ درصد و ۱۵ درصد، بالاترین قابلیت و ریسک‌های حوزهٔ تأمین فیزیکی و ایمنی کار هر یک با ضریب اهمیت ۹ درصد کمترین قابلیت ریسک را در بر می‌گیرند و احتمال وقوع، مهمترین عامل مؤثر بر بحرانی شدن ریسک‌ها می‌باشد. همچنین ۱۰ مؤلفه دارای بیشترین قابلیت ایجاد مخاطره برای تداوم عملیات پایگاه‌های پدافندی نیز شناسایی و اولویت‌بندی گردیدند.

واژه‌های کلیدی: پایگاه‌های پدافند هوایی، شدت پیامد، احتمال وقوع، ضریب تعیین، نمره ریسک.

[۱] استاد مدیریت دولتی، دانشگاه پیام نور
[۲] استادیار مدیریت بازرگانی، دانشگاه پیام نور
[۳] کارشناس ارشد مدیریت دولتی، دانشگاه پیام نور
[۴] کارشناس ارشد مدیریت دولتی، دانشگاه پیام نور

مقدمه

دفاعِ ملّی نیازمند شناخت دقیق و عالمانهٔ محیط راهبردی، تعیین درستِ اهداف و منافع و انتخاب گزینه‌های مناسب و بهنگام برای رسیدن به آن‌هاست (یزدان فام،۱۳۹۱:۶۳). از نیمهٔ دوم قرن نوزدهم، فناوری نظامی پیشرفت چشمگیری داشته است؛ جنگ با ارتش‌های نوین و منسجم شکل می‌گرفت که موجب ایجاد فرصت برای پیاده‌سازی راهبردهای جدید و در نتیجه پیروزی سریع می‌گردید. بنابراین ارتش‌هایی بزرگ و با تحرّک بالا به وجود آمد که دارای پشتیبانی فرماندهی قوی جهت نظارت، کنترل و تصمیم‌گیری بودند. نیاز اولیه و اساسی این ارتش‌ها در زمان صلح و جنگ، اطلاعات دربارهٔ خودشان و نیروهای خارجی است؛ زیرا این اطلاعات در صحنهٔ نبرد نقش اساسی دارند (واحدی و زارعی،۱۳۸۶:۸۰). ارتش به مثابه اصلی‌ترین سازمان نظامی موظف است کشور را از خطرات و تهدیدات خارجی حفظ نموده و همواره مدافع امنیّت و تمامیت ارضی کشور باشد (ساکی‌زاده و جهانگیرزاده،۱۳۸۷:۱۳۳). از سوی دیگر آینده با عدم قطعیّت و ابهام همراه است، به همین دلیل همواره مخاطره و ریسک وجود دارد. فرایند رایج در طراحی ساختار و سازماندهی نظامی به‌منظور مقابله با تهدیدات پیش‌بینی نشده محیط، بسیار شکننده است و در عمل پیاده‌سازی تحولات ساختاری را به مخاطره می‌اندازد؛ حتی ممکن است منجر به شکست شود. در چنین شرایطی ضمن از دست دادن زمان و صرف هزینهٔ زیاد، سازمان کارایی و اثربخشی لازم را ندارد و کشور را دچارِ آثار سوء دفاعی- امنیّتی می‌کند (آقامحمدی-۱۳۹۰-۶۵). یکی از چالش‌های مدیریت این است که چه مقدار عدم اطمینان را تحمّل نماید؟ از اساسی‌ترین راهکارها برای حلِ مسئله عدم قطعیت، ارزیابی، تحلیل و مدیریت ریسک است. میزان تمرکز بر تحلیل ریسک، به عنوان یکی از مراحل اساسی فرایند مدیریت ریسک، به‌طور مستقیم به درجه پیچیدگی سازمان و میزان تعامل آن با محیط پیرامونی وابسته است؛ اما احتمال ضرر و زیان وارده ناشی از ریسک‌ها و مخاطرات همیشه با ارزیابی و تحلیل ریسک قابل کاهش است. در این میان سازمان‌های نظامی باید بتوانند به‌طور منطقی و روشمند مخاطرات بالقوه را شناسایی و تحلیل نموده، برای مدیریت مناسب آن‌ها در شرایطِ اطمینان اقدام کرده و از تصمیم‌گیری‌های ذهنی و تقریبی پرهیز نمایند. در تحقیق پیش رو، تحلیل و ارزیابی روشمند و علمی ریسک‌ها و مخاطرات در یک محیط نظامی مورد مطالعه قرار گرفته است.

بیان ضرورت و اهمیت مسئله

بعضی از مدیران با اتخاذِ سیاست گریز از ریسک، نسبت به کارهای متهوّرانه موضع‌گیری می‌کنند و فرصت‌های رشد را از دست می‌دهند؛ از طرفی برخی از مدیران با بروز رفتارهای هیجانی و اتخاذ تصمیمات پُر خطر، خسارات جبران‌ناپذیری را به سازمان وارد می‌کنند (مهدی، حشمتی، کلهر و بازیاری، ۱۲:۱۳۹۳). سامانه‌های فرماندهی و کنترل همچون C3I[1]، C4I[2]، C4ISR[3]، WWMCCS[4]، GCCS[5] و... به عنوان بستر اساسی مدیریت و رهبری در سازمان‌های نظامی به‌کار گرفته می‌شوند. تغییرات روزافزون محیط‌های عملیاتی، باعث افت شدید کارایی این سامانه‌های سنتی شده است (حقیری و ستاری‌خواه، ۱۶۹:۱۳۸۴). یکی از مباحثی که کمتر به صورت علمی در سازمان‌های دولتی و نظامی به‌کارگرفته شده مدیریت ریسک است. در اجرای فرایند مدیریت ریسک دو مبحث بسیار مهم است: اول اینکه ریسک‌های بحرانی که اثر زیادی بر تداوم عملیات می‌گذارند شناسایی شوند؛ چرا که تحلیل تمام ریسک‌ها، زمان‌بر بوده و کارایی لازم را ندارد؛ دوم اینکه بعد از شناسایی ریسک‌های بحرانی و تحلیل آن‌ها، واکنش به ریسک ضرورت می‌یابد؛ چون زمانی مدیریت ریسک کارایی خواهد داشت که به محض وقوعِ ریسک، بتوان تأثیر آن را حذف یا کاهش داد. پایگاه‌های راداری، شناسایی الکترونیک و موشکی پدافند به لحاظ نقش اخطار اولیه، کشف و شناسایی اهداف و تهدیدات فرا سرزمینی، دفع و خنثی‌سازی تجاوزات و حملات نیروهای بیگانه، نقشی راهبردی در دفاع از آسمان و امنیّت کشور ایفا می‌نمایند. از یک سو این پایگاه‌های اغلب در محیط‌های کوهستانی و در ارتفاعات مرزی مستقر شده و در استفاده از منابع انرژی سراسری محدودیت دارند؛ بنابراین به دلیل بُعد مسافت با محیط‌های شهری و اداری، در دسترسی به خدمات ارتباطی امن، پشتیبانی و اورژانس نیز با مشکلات و هدر رفت.

زمان مواجه‌اند؛ از سوی دیگر اهمیت راهبردی این پایگاه‌ها در تهیهٔ اطلاعات حیاتی نظامی و تأمین امنیّت کشور، حتی چند ثانیه اختلال در عملیات این مراکز را نیز غیرموجّه می‌داند. به عبارت دیگر یکی از دغدغه‌های اصلی در این پایگاه‌ها مدیریت ریسک‌ها و مخاطراتی است که

[1] Command, Control, Communication & Intelligence
[2] Command, Control, Communication, Computer & Intelligence
[3] Command, Control, Communication, Computer, Intelligence, Surveillance & Reconaissance
[4] World Wide Military Command & Control System
[5] Global Command & Control Syste

می‌توانند موجب تعطیلی عملیات، خاموشی دستگاه‌ها و تجهیزات راداری، توقف در رهگیری اطلاعات و اختلال در عملکرد سامانه‌های راداری و موشکی حتی در مقیاس ثانیه شوند. در این تحقیق نخست سعی شده مفاهیم و مراحل مدیریت ریسک بررسی و سپس به صورت موردی فرایند مدیریت ریسک‌های مؤثر بر تداوم و توقف عملیات در یک پایگاهِ پدافندی برای شناسایی و دسته‌بندی حوزه‌های مختلف ریسک، ارزیابی و اولویت‌بندی ریسک‌ها و روش مواجهه با آن‌ها بررسی گردد. با توجه به مطالب یاد شده، سؤالِ اصلی تحقیق این است:

- اولویت‌بندی ریسک‌های مؤثر بر توقف عملیات در یک پایگاه پدافندی کدامند؟

سوالات فرعی تحقیق

۱- مهمترین عامل در بحرانی شدن ریسک‌های موجود در یک پایگاه پدافندی کدامند؟

۲- ریسک‌های بحرانی کدامند؟

مبانی نظری تحقیق

۱- تعریف مدیریت ریسک: مدیریت ریسک شامل قسمتی از فرایندهای مدیریتی است که مدیران را قادر می‌سازد تا به صورت آگاهانه تصمیماتی در رابطه با مخاطرات اتخاذ نمایند. (بورس اوراق بهادار، بی‌تا:۲۱). «یک فرایند متمرکز که طی چرخهٔ عمر سیستم تکامل می‌یابد و عبارتست از: نوعی روش‌شناسی سازمان‌یافته برای شناسایی و اندازه‌گیری مستمرِ عوامل ناشناس، توسعهٔ راهکارهای تخفیفی[1]، گزینش، برنامه‌ریزی و اجرای مناسب تخفیف‌دهنده‌های ریسک و رهگیری عملکردها برای اطمینان از موفقیت در تضعیف ریسک» (وزارت دفاع آمریکا،۳:۲۰۰۶)[2]. در تعریفی کاربردی و کامل‌تر مدیریت ریسک عبارتست از: فرایند شناسایی، تحلیل و گزارش مخاطرات و تصمیم‌گیری در مورد پذیرش، اجتناب، انتقال و یا کنترل آن در یک سطحِ قابل قبول با توجه به هزینه‌ها و منابع موجود (وزارت امنیّت داخلی آمریکا،۷:۲۰۱۱)[3]. چنانچه مدیریت بتواند طی یک فرایند منطقی اطلاعات مناسب و کافی را از شرایط درونی و پیرامونی سازمان خود جمع‌آوری و بر مبنای آن اقدام نماید، خواهد توانست ضعف‌های درون سازمانی را به قوت و تهدیدات بیرون سازمانی را به فرصت تبدیل نماید؛ با

[1] Mitigation Options
[2] United State of America - Department Of Defence
[3] United State of America - Homeland Security

قطعیّت بیشتری رویدادهای منفی را از مسیر حرکت سازمان منحرف کرده و بر احتمال وقوع رویدادهای مثبت بیافزاید.

۲- فرایند مدیریت ریسک: فرایند مدیریت ریسک عبارت است از: ۱- تعریف چارچوب اهداف ۲- شناسایی ریسک بالقوه ۳- ارزیابی و تحلیل ریسک ۴- توسعهٔ راه حل‌ها و پیشنهادها ۵- تصمیم‌گیری و اجرا ۶- ارزیابی و نظارت ۷- ارتباطات (وزارت امنیّت داخلی آمریکا، ۱۵:۲۰۱۱). از نظر چاپمن و وارد[1] مدیریت ریسک فرایندی ۹ مرحله‌ای دارد: ۱- شناسایی جنبه‌های اصلی و اهداف مدیریت ریسک؛ ۲- تمرکز بر یک رویکرد راهبردی در مدیریت ریسک؛ ۳ـ شناسایی زمان بروز ریسک‌ها؛ ۴- تخمین ریسک‌ها و بررسی رابطهٔ میان آن‌ها؛ ۵- تخصیص مالکیت ریسک و ارائه پاسخ مناسب؛ ۶- تخمین میزان ابهام و عدم اطمینان؛ ۷-تخمین اهمیت رابطهٔ میان ریسک‌های مختلف؛ ۸- طراحی پاسخ‌ها و نظارت بر وضعیت ریسک؛ ۹- کنترل مراحل اجرا (عالم تبریز و حمزه‌ای، ۴:۱۳۹۰). استاندارد PMBOK[2] مدیریت ریسک را یک فرایند ۶ مرحله‌ای در نظر می‌گیرد: ۱- برنامه‌ریزی ریسک ۲- شناسایی ریسک ۳- تحلیل کیفی ریسک ۴- تحلیل کمی ریسک ۵- برنامه‌ریزی برای پاسخ به ریسک ۶- کنترل و نظارت ریسک (همان: ۴ و ۵). همچنین استاندارد ۴۳۶۰ استرالیا- نیوزیلند[3] که در سال ۲۰۰۴ به عنوان استاندارد مرجعِ مدیریت ریسک در زیرمجموعه استانداردهای جهانی سلامت، ایمنی و محیط زیست (HSE[4]) پذیرفته و توصیه شده است، فرایند مدیریت ریسک را در ۷ مرحله تبیین می‌کند: ۱- تعریف اهداف ۲- تشخیص ریسک ۳- تحلیل ریسک ٤- ارزیابی ریسک ٥-مشاوره و ارتباطات ٦- اقدام ۷- نظارت و بازرسی (استاندارد HSE، بی‌تا:۹).

الگوی فرایند مدیریت ریسک پیشنهادی وزارت دفاع آمریکا نیز شامل یک چرخهٔ پنج مرحله‌ای است: ۱- شناسایی ریسک ۲- تحلیل ریسک ۳- برنامه‌ریزی تضعیف ریسک ۴- اجرای برنامهٔ تضعیف ۵- رهگیری و نظارت (وزارت دفاع آمریکا،۴:۲۰۰۶).

در الگوهای مختلف که توسط محققان و مراجع متفاوت ارائه شده‌اند، گاه چند گام در هم ادغام شده و گاه نیز یک گام، خود به چند گام مجزا از هم تفکیک شده‌اند. بنابراین در یک

[1] Chopman & Ward
[2] Project Management Body of Knowledge
[3] Standard (AS/NZS 4360: 2004)
[4] Health , Safty & Environment

جمع‌بندی توسط محقق از الگوهای بالا، الگوی کلی فرایندِ مدیریت ریسک به صورت زیر ارائه و در ادامه هر گام به تشریح بیان می‌شود:

الف- تبیین اهداف مدیریت ریسک

ب- شناسایی ریسک

ج- ارزیابی و تحلیل ریسک

د- تعریف راهکارها و راه حل‌ها

هـ- نظارت و تجدیدنظر

الف) تبیین اهداف مدیریت ریسک

مطالعات مختلف این گام را با عناوینی همچون؛ تعریف چارچوب اهداف، برنامه‌ریزی ریسک، و یا تعریف اهداف ذکر نموده‌اند. اهداف متنوعی برای مدیریت ریسک ذکر شده‌اند. وزارت امنیّت داخلی آمریکا مدیریت ریسک را موجب تکامل و ارتقای برنامه‌ریزی عملیاتی و راهبردی، توسعهٔ سیاست‌ها و راهبردها، بودجه‌بندی، ارزیابی و ارزشیابی عملکرد و فرایندهای گزارش‌دهی عنوان می‌کند (وزارت امنیّت داخلی آمریکا،۸:۲۰۱۱). از مَنظر رویکرد سیستمی به سازمان نیز می‌توان مدیریت ریسک را بر مبنای دو گام مرتبط هدف‌گذاری نمود: ۱- مدیریت پیشگیرانه قبل از وقوع حادثه ۲- مدیریت تصمیم اشتباه بعد از وقوع حادثه. مدیریت پیشگیرانه قبل از حادثه، بر مبنای تعریف برنامه‌هایی برای استقرار سیستم ایمنی، پیشگیری، حذف علل ریشه‌ای مخاطرات و ایجاد سطح قابل قبولی از نگرانی، اضطراب و اطمینان خاطر، برنامه‌ریزی می‌شود و مدیریت تصمیم اشتباه بعد از حادثه، باید به تعیین برنامه‌هایی برای حفظ بقاء، خروج از بحران، تثبیت مجدد، بازگشت به روند عادی فعالیت و رشد توجه نماید. مهمترین هدف مدیریت ریسک، کمک به سازمان در مدیریت بهتر ریسک‌های مربوط به مأموریتش است. این روش، مدیران را یاری می‌کند تا بتوانند هزینه‌های عملیاتی و اقتصادی خود را تعدیل نمایند و بهترین تصمیمات را اتخاذ کنند (پورصادق، فرشچی و موحدی صفت،۴:۱۳۹۲). سایر اهداف و کارکردهای مورد انتظار از مدیریت ریسک عبارتند از: الف- پیشگیری مقدماتی شامل حذف عوامل مخاطره‌آمیز در سازمان و ایمن‌سازی نسبت به آن‌ها؛ ب- پیشگیری ثانویه شامل تشخیص به موقع ریسک و مدیریت آن با هدف جلوگیری از اخلال در عملیات جاری و آتی

سازمان؛ ج- پیشگیری نهایی شامل اصلاح و بازتوانی برای بازگشت سازمان به روند عادی و ادامهٔ فعالیت‌ها.

ب) شناسایی ریسک

ریسک عبارتست از: مخاطره، تهدید، رویداد، فرد، سازمان یا فعلی طبیعی یا مصنوعی که شامل آسیب جانی، مالی، اطلاعاتی، امنیّتی، کارکردی یا محیطی برای فرد، سازمان یا جامعه باشد (وزارت امنیّت داخلی آمریکا،۱۳:۲۰۱۱). ریسک عبارتست از: احتمال انحراف در یک برآورد. وزات دفاع آمریکا ریسک را به میزان عدم اطمینان آتی در نیل به اهداف و مقاصد برنامه‌های اجرایی، در محدودهٔ هزینه، زمان‌بندی و چارچوب عملکرد تعیین شده تعبیر می‌کند (وزارت دفاع آمریکا،۳۳:۲۰۰۶).

شناسایی ریسک فعالیتی است که طی آن همهٔ ارکان برنامه‌ها بررسی می‌شوند تا ریشه رویدادهای آینده شناسایی و مستندسازی شده و مراحلی برای مدیریت مؤثر آن‌ها طراحی شود. این کار باید تا حد امکان از ابتدای برنامه‌ها و حتی قبل از طراحی برنامه‌ها شروع شده و در طول اجرای برنامه‌های سازمانی به‌طور مستمر ادامه یافته و بازبینی شود (وزارت دفاع آمریکا،۳۳:۲۰۰۶).

ج) ارزیابی و تحلیل ریسک

هر مخاطره دارای سه مؤلفه اساسی است: ۱- علت ریشه‌ای ۲-برآورد فعلی ۳- پیامد آتی. علل ریشه‌ای که هنوز شکل نگرفته و اگر به موقع حذف یا تصحیح شود از ایجاد یک پیامد سنگین جلوگیری خواهد شد. برآورد فعلی در واقع پیش‌بینی نسبت به چیزی است که در آینده اتفاق خواهد افتاد و پیامد آتی که نتیجهٔ وقوع ریسک در واقعیت است. علل ریشه‌ای مهمترین بُعد ریسک است؛ از این رو مخاطرات باید مورد بررسی ریشه‌ای و ماهیتی قرار بگیرند (وزارت دفاع آمریکا،۱:۲۰۰۶). وزارت امنیّت داخلی آمریکا در رویکرد فراگیر به مدیریت ریسک، انواع ریسک‌ها را در سه گروه کلی ریسک‌های راهبردی، عملیاتی و سازمانی جای می‌دهد. ریسک‌های راهبردی تهدیدی برای توانایی سازمان در نیل به راهبردهایش به‌شمار می‌روند که بر فلسفهٔ وجودی، شهرت و قابلیت پیش‌بینی روندهای بلندمدت سازمان تأثیر جدی می‌گذارند. ریسک‌های عملیاتی بر کارکنان، مواد، تجهیزات، زمان، اطلاعات، فناوری و نیل به اهداف عملیاتی تأثیر گذارند. ریسک‌های سازمانی که کمتر قابل لمس و مشاهده هستند، از درون

سازمان نشئت می‌گیرند و توانایی سازمان را در سازماندهی، جذب نیرو، آموزش و پشتیبانی متأثر می‌نمایند (وزارت امنیّت داخلی آمریکا،۱۴:۲۰۱۱). فنون متنوعی برای ارزیابی و تحلیل ریسک استفاده می‌شوند که در دو دستهٔ کلی جای می‌گیرند: فنون تحلیل کیفی و فنون تحلیل کمی. در تحلیل کیفی ریسک، با توجه به درجه‌بندی ریسک‌ها می‌توان تمام ریسک‌ها را در نظر گرفت یا بخشی از آن‌ها را، که اولویت کمتری دارند، حذف نمود. در تحلیل کمی ارتباط بین ریسک‌ها با تداوم عملیات در نظرگرفته می‌شود و مشخص می‌نماید که استمرار عملیات با توجه به هر ریسک بحرانی چه تغییری می‌کند. نتیجهٔ ارزریابی و تحلیل ریسک عبارتست از: اولویت‌بندی ریسک‌ها، تشخیص ریسک‌های بحرانی و تعیین عوامل شدت تأثیر، احتمال وقوع، ضریب تعیین[1] و نمره هر ریسک.

ضریب تعیین یا ضریب کشف عبارتست از: توانایی کشف و ردیابی یک ریسک به همراه فرصت کافی برای برنامه‌ریزی اقتضایی به منظور پاسخگویی به ریسک.

د) تعریف راهکارها و راه‌حل‌ها: فعالیت شناسایی، ارزیابی و انتخاب ابزارها، راهکارها و راهبردهایی که ریسک‌ها را با توجه به محدودیت‌ها و مقاصد موجود، در سطحی قابل قبول نگاه می‌دارد (وزارت دفاع آمریکا،۱۸:۲۰۰۶). وزارت دفاع آمریکا در سال ۲۰۰۶ چهار راهبرد عمده را برای تصمیم‌گیری در مورد نحوهٔ مواجهه با ریسک‌ها ارائه می‌دهد: ۱- پذیرش ۲- اجتناب ۳- کنترل ۴- انتقال (وزارت دفاع آمریکا،۱۸:۲۰۰۶):

۱- پذیرش: تصمیمی صریح یا ضمنی مبنی بر اینکه در برابر ریسک مورد نظر هیچ واکنش مؤثری صورت نگیرد.

۲- اجتناب: تصمیم یا راهکاری که سازمان را از رویارویی و تأثیرپذیری از ریسک دور و از آن بر حذر می‌دارد.

۳- کنترل: فعالیت‌هایی برای کاهشِ توان آسیب ریسک و یا نگهداری ریسک در یک سطحِ قابل قبول.

۴- انتقال: اتخاذ راهبردهایی برای انتقال تمام یا بخشی از پیامدهای ریسک به شخص، سازمان، سیستم و یا شبکه‌ای دیگر، مثل راهبرد ایجاد پوشش‌های بیمه‌ای.

[1] Detection Value or Earned Value

در این مرحله روش‌ها و هزینه‌های حذف خطر هر یک از ریسک‌های بحرانی محاسبه و با میزان پیامد و نمرهٔ ریسک مقایسه شده و با توجه به توجیه اقتصادی، امنیّتی، ایمنی، فرهنگی و اجتماعی یکی از راهبردهای مواجهه با ریسک انتخاب می‌گردد.

ه) نظارت و تجدید نظر: هدف از نظارت بر اجرای راهکارهای مدیریت ریسک، کسب تجربه و اطلاعات کافی دربارهٔ ریسک‌های آتی است تا بتوان دربارهٔ علل ریشه‌ای ریسک‌ها قضاوت و تصمیم‌گیری نمود (وزارت دفاع آمریکا،۲۰۰۶:۳۳). نظارت عبارتست از فرایند ردیابی، ارزیابی و اندازه‌گیری نظام‌مند اقدامات مقابله با ریسک، مطابق با استانداردهای تعیین شده، طی فرایندهای توسعه و بهبود راهکارها (وزارت دفاع آمریکا،۲۰۰۶:۳۳). باید توجه داشت که ریسک‌ها طی زمان و در مواجهه با تحولات محیطی، تغییر ماهیّت داده، تبدیل شده و جابه‌جا می‌شوند و می‌توانند در جای دیگر و با شکل و میزان تأثیر متفاوت‌تری ظاهر شوند. ریسک‌های جدید، به شکل دائم شکل می‌گیرند و سازمان را تهدید می‌کنند؛ از این رو همواره نظارت و پایش مستمر در سازمان و محیط پیرامونی سازمان برای غافلگیر نشدن در مواجهه با مخاطرات لازم است و هوشیاری و نکته‌سنجی مدیران و فرماندهان را طلب می‌کند.

- فن تجزیه و تحلیل حالت خطا و اثر شکست ریسک[1]:

این فن یکی از رایج‌ترین فنون تحلیل ریسک و پیش‌بینی تأثیر آن بر اهداف ریسک است که ابتدا در صنایع هواپیماسازی و سپس به‌طور گسترده در سایر صنایع به‌کارگرفته شد؛ هدف آن شناسایی و رتبه‌بندی نقایص و معایب احتمالی در فرایندهاست. سانتوس و همکارانش[2] در ۲۰۰۸ این فن را با استاندارد PMBOK ادغام نموده و در مدیریت ریسک پروژه به‌کار گرفتند. همچنین آندری و میگوئل[3] از این فن

برای مدیریت ریسک در توسعهٔ محصولات جدید استفاده نمودند. عالم تبریز و حمزه‌ای نیز طی تحقیقی در سال ۱۳۹۰ با تلفیق مدیریت ریسک استاندارد و فن RFMEA به ارزیابی و تحلیل ریسک‌های پروژهٔ توسعه میدان نفتی آزادگان پرداختند. در این فن به‌منظور رتبه‌بندی ریسک‌ها، از سه مقیاس احتمال وقوع ریسک، شدت اثر ریسک و ضریب کشف ریسک استفاده می‌شود که می‌تواند تحلیل ریسک را با دقت بالایی انجام دهد. در این فن حاصلضرب دو مقدار

[1] RFMEA
[2] Dos Santos, Flavie Roberto Souza, Cabral Sandra
[3] Segismundo, Andre, Miguel, P.A.C

احتمال وقوع و شدت اثر ریسک، ضریبی را با عنوان نمرهٔ ریسک پدید می‌آورد. با ضرب کردن مقدار ضریب کشف در نمرهٔ ریسک، مقدار جدیدی تحت عنوان RPN [1] به دست می‌آید و هر ریسکی که RPN بزرگتری داشته باشد از اولویت بالاتری برخوردار خواهد بود.

روش تحقیق

این تحقیق از نظر هدف کاربردی و از نظر نحوهٔ گردآوری داده‌ها توصیفی-پیمایشی است. مورد مطالعه (با رعایت طبقه‌بندی) یکی از پایگاه‌های پدافندی ارتش در حوزهٔ جنوب کشور است. جامعهٔ آماری شامل فرماندهان صف و ستاد، خبرگان و متخصصان مرتبط با عملیات پایگاه‌های شناسایی، راداری و موشکی پدافند ارتش است. حجم نمونه با استفاده از جدول مورگان و فرمول کوکران ۴۸ نفر تعیین گردید. طی سه مرحله و هر بار۵۲ پرسشنامه به روش تصادفی بین جامعهٔ آماری توزیع و در نهایت ۴۹ نفر، پرسشنامه‌های تکمیل شده را برگشت دادند. در مجموع، ۱۶۲ سوال طی سه پرسشنامه ۵۴ سوالی بر مبنای طیف ۵ نقطه‌ای لیکرت به هر یک از افراد نمونه ارائه گردید.

ابزار پژوهش: در مرحلهٔ شناسایی ریسک‌های محتمل با روش مطالعات میدانی و کتابخانه‌ای، مراجعه به متون و سوابق و مصاحبه با کارکنان و فرماندهان، ساختار شکست کار در پایگاه تا سومین سطح آن شکسته شد و در مجموع ۸ گروه اصلی با ۵۸ ریسک زیرگروه مرتبط با یک پایگاه نظامی پدافندی شناسایی و به ۱۶ نفر از خبرگان و متخصصان، ارائه گردید. طبق نظر خبرگان، ۴ مخاطره فاقد موضوعیت و قابل اغماض تشخیص داده شدند و ۵۴ مخاطره به‌طور اجماع برای بررسی‌های بیشتر باقی ماندند و مخاطرهٔ جدیدی پیشنهاد نگردید: این ۵۴ ریسک در ۸ گروه اصلی به شرح ذیل قرار گرفتند: گروه مدیریت نیروی انسانی با ۶ ریسک، عوامل بهداشتی با ۶ ریسک، ایمنی کار با ۷ ریسک، پشتیبانی و تدارکات با ۷ ریسک، امنیّت اطلاعات با ۷ ریسک، حفاظت فیزیکی با ۷ ریسک، تعمیر و نگهداری با ۷ ریسک و عملیات نیز با ۷ ریسک.

در این تحقیق از سه پرسشنامهٔ محقق ساخته استفاده گردید.

[1] Risk Priority Number

- در پرسشنامه اول از شرکت‌کنندگان خواسته شد تا شدتِ پیامد هر یک از این ۵۴ ریسک را بر ایجاد اختلال در تداوم فعالیت و مأموریت اصلی پایگاه مشخص نمایند:

جدول ۱: مبنای طیف لیکرت برای پرسشنامه شدت پیامد ریسک

طیف لیکرت	شدت پیامد
۵	توقف کامل و اختلال بلندمدت در مأموریت اصلی پایگاه
۴	اختلال موقت در مأموریت و عملیات اصلی پایگاه
۳	اختلال اساسی در فعالیت‌های فرعی و پشتیبانی
۲	اختلال موقت و جزئی در فعالیت‌های فرعی
۱	عدم اختلال در عملیات عادی و معمول

- در پرسشنامه دوم خواسته شد تا احتمال وقوع هر یک از ۵۴ ریسک را تعیین نمایند:

جدول ۲: مبنای طیف لیکرت برای پرسشنامه احتمال وقوع ریسک

طیف لیکرت	احتمال وقوع
۵	یک تا چند بار در روز - بسیار محتمل
۴	یک تا چند باردر هفته
۳	یک تا چند بار در ماه
۲	یک تا چند بار طی سال
۱	بسیار نامحتمل - هرگز یا یکبار طی چند سال اخیر

- در پرسشنامه سوم ضریب تعیین ریسک گویه‌های۵۴ گانه مدنظر قرار داشت:

جدول ۳: مبنای طیف لیکرت برای پرسشنامه ضریب کشف ریسک

طیف لیکرت	ضریب تعیین
۵	روش کشفی برای ریسک وجود ندارد.
۴	روش کشف ریسک یا زمان پاسخ به ریسک نامشخص و نامطمئن است.
۳	روش کشف ریسک اثربخشی متوسطی دارد.
۲	روش کشف ریسک اثربخشی بالایی دارد.
۱	روش کشف کاملا مشخص و ممکن و زمان برای پاسخگویی کافیست

برای بررسی روایی پرسشنامه‌ها به اعضای خبرگان ارائه شدند و هیچ مولفه‌ای حذف یا پیشنهاد نگردید. برای بررسی پایایی پرسشنامه‌ها، آلفای کرونباخ مربوط به هر پرسشنامه محاسبه شد. برای پرسشنامه اول ۰/۹۴، پرسشنامه دوم ۰/۹۵ و برای پرسشنامه سوم ۰/۸۸ به دست آمد که بیانگر پایایی مناسبی است؛ از این رو روایی و پایایی پرسشنامه‌ها تأیید گردید.

روش تحلیل داده‌ها توصیفی، استنباطی و در مرحلهٔ ارزیابی و تحلیل ریسک از فن RFMEA *و فن ویلیام فاین* در آنالیز ریسک استفاده شد. بر این اساس نمرهٔ ریسک برای هر یک از ریسک‌ها به صورت رابطهٔ زیر محاسبه می‌شود:

نمرهٔ ریسکR = شدت پیامد ریسکX × احتمال وقوع ریسکY

از ضرب کردن نمره ریسک و ضریب تعیین، مقدار جدیدی با عنوان RPN به دست می‌آید.

$$Z \times Z = R \times Y \times RPN = X$$

هر ریسکی که RPN بزرگتری داشته باشد از قابلیت ریسک بالاتری برخوردار است.

یافته‌های پژوهش

بعد از استفاده از ساختار شکست ریسک، فهرست ریسک‌های ۵۴گانه با استفاده از نظر خبرگان طی سه مرحله و در سه پرسشنامه مجزا تهیه و به اعضای نمونهٔ آماری ارائه گردید تا سه مقدار احتمال وقوع، شدت تأثیر و ضریب کشف ریسک برای تمامی ریسک‌ها به دست آید. برای بررسی نرمال بودن نتایج از آزمون کولموگروف-اسمیرنف[1] استفاده شد. براساس نتایج آزمون همه متغیرهای تحقیق نرمال هستند. همچنین برای بررسی وضعیت شدت پیامد، احتمال وقوع و ضریب تعیین ریسک‌ها آزمون میانگین یک جامعه آماری[2] استفاده شد.

سوال اصلی تحقیق: اولویت‌بندی ریسک‌های مؤثر بر توقف عملیات پایگاه‌های پدافندی کدامند؟

[1] Kolmogorov-Smirnov test
[2] One sample T test

جدول۴: محاسبه RPN با استفاده از میانگین امتیازات حاصل از هر ۳ پرسشنامه

ردیف	حوزه	ریسک	شدت ریسک	احتمال وقوع	نمره ریسک R	ضریب تعیین	RPN
۱	تعمیر و نگهداری	خاموش کردن سامانه‌های عملیات جهت پیشگیری از صدمهٔ رعدوبرق	۴/۹۱	۳/۸۶	۱۸/۹۵	۳/۹	۷۳/۹
۲	تعمیر و نگهداری	قطع کلیه خطوط ارتباطی بی‌سیم و تلفنی	۴/۱۸	۳/۹۶	۱۶/۵۵	۴/۳	۷۱/۲
۳	نیروی انسانی	کمبود نیروی متخصص عملیاتی	۴/۱	۳/۹۸	۱۶/۳۱	۳/۷	۶۰/۴
۴	عملیات	اشتباه در کشف و شناسایی اهداف متخاصم پروازی	۴/۰۲	۳/۹۸	۱۵/۹۹	۲/۶	۴۱/۶
۵	تعمیر و نگهداری	قطع برق سراسری و برق نیروگاه داخلی به‌طور همزمان	۴/۸۷	۲/۰۵	۱۰	۴	۴۰
۶	نیروی انسانی	کمبود نیروی متخصص تعمیر و نگهداری	۳/۹۳	۳	۱۱/۷۹	۳/۳	۳۸/۹
۷	امنیّت اطلاعات	افشای اطلاعات طبقه‌بندی از طریق ماهواره‌های جاسوسی و عکسبرداری	۳	۴	۱۲	۳/۲	۳۸/۴
۸	امنیّت اطلاعات	افشای اطلاعات طبقه‌بندی شده از طریق مکالمات بی‌سیم و تلفنی	۲/۹۷	۴	۱۱/۸۸	۳/۲	۳۸
۹	عوامل بهداشتی	عدم دسترسی به فوریت‌های پزشکی	۲/۹۱	۴/۰۸	۱۱/۸۷	۲/۹	۳۴/۴
۱۰	تعمیر و نگهداری	خرابی دستگاه‌ها و تجهیزات سامانه‌های راداری عملیات	۳/۹۷	۲/۸۶	۱۱/۳۵	۳	۳۴/۱
۱۱	امنیّت اطلاعات	افشای اطلاعات طبقه‌بندی از طریق دستگاهای دورنگار بدون رمزکننده	۳/۰۲	۳/۰۸	۹/۳	۳/۵	۳۲/۵
۱۲	پشتیبانی	کمبود تجهیزات و قطعات یدکی حسّاس و مورد نیاز عملیات	۳/۹۱	۲/۰۴	۷/۹۷	۳/۸	۳۰/۳
۱۳	عملیات	تأخیر در اعلام خطر به پایگاه‌های موشکی و مبادی بالادستی	۴/۸۳	۱/۹۸	۹/۵۶	۳/۱	۲۹/۶
۱۴	عوامل بهداشتی	شیوع بیماری‌های واگیردار	۳	۲/۸۸	۸/۶۴	۳/۴	۲۹/۴

۱۵	نیروی انسانی	کمبود نیروی پاسداری	۳/۰۴	۳	۹/۱۲	۳/۲	۲۹/۲
۱۶	حفاظت فیزیکی	کمبود پُست‌های پاسداری و بازرسی	۳/۰۲	۳/۸۶	۱۱/۶۵	۲/۵	۲۹/۱
۱۷	عملیات	اشتباه در تجزیه و تحلیل اطلاعات رهگیری شده	۳/۹۷	۲/۰۶	۸/۱۷	۳/۴	۲۷/۸
۱۸	حفاظت فیزیکی	فرسودگی و نقصِ تجهیزات سیستم حفاظت پیرامونی	۲/۹۳	۳/۰۶	۸/۹۶	۳/۰۵	۲۷/۳
۱۹	امنیّت اطلاعات	سرقت اطلاعات طبقه‌بندی از طریق نفوذ به شبکهٔ رایانه‌ای	۲/۹۷	۲/۱	۶/۲۳	۴/۳	۲۶/۸
۲۰	تعمیر و نگهداری	غیرعملیاتی شدن سامانه‌های اعلام خطر عملیات	۴	۲/۱۶	۸/۶۴	۳/۱	۲۶/۷
۲۱	امنیّت اطلاعات	از بین رفتن اطلاعات طبقه‌بندی به دلیل سیستم بایگانی و مدیریت نامناسب اطلاعات	۳	۲/۰۴	۶/۱۲	۴/۲	۲۵/۷
۲۲	ایمنی کار	آتش‌سوزی گسترده	۴/۸۹	۱/۰۸	۵/۲۸	۴/۷	۲۴/۸
۲۳	نیروی انسانی	کمبود کادر بهداری	۳/۰۴	۳/۰۲	۹/۱۸	۲/۷	۲۴/۸
۲۴	ایمنی کار	نبود یا سالم نبودن تجهیزات اطفای حریق	۴/۰۶	۱/۹۸	۸/۰۳	۳	۲۴/۱
۲۵	تعمیر و نگهداری	غیرعملیاتی شدن سامانه ارتباط راداری و رادیویی با اهداف پروازی	۳/۹۷	۲	۷/۹۴	۳	۲۳/۸
۲۶	پشتیبانی	انسداد جادهٔ دسترسی بر اثر ریزش کوه	۲/۹۷	۱/۹	۵/۶۴	۴/۲	۲۳/۷
۲۷	عملیات	مهارت پایین کاربران در اعلام هشدار اولیه	۴	۱/۹	۷/۶	۳	۲۲/۸
۲۸	ایمنی کار	انفجار در زاغه مهمات	۴/۲	۱/۱۲	۴/۷	۴/۸	۲۲/۶
۲۹	تعمیر و نگهداری	خرابی سیستم خنک‌کننده دستگاه‌ها و تجهیزات حسّاس عملیات	۴/۱۴	۱/۸۲	۷/۵۳	۳	۲۲/۶
۳۰	پشتیبانی	عدم دسترسی به دلیل کولاک و آب و هوای کوهستانی	۲/۹۷	۲/۰۲	۵/۹۹	۳/۷	۲۲/۲

۳۱	حفاظت فیزیکی	ورود غیرمجاز به پایگاه	۳	۱/۹۸	۵/۹۴	۳/۷	۲۲
۳۲	امنیّت اطلاعات	دسترسی غیر مجاز به مخزن اسناد طبقه‌بندی شده	۲/۸۳	۲/۰۴	۵/۷۷	۳/۸	۲۱/۹
۳۳	عوامل بهداشتی	مسمومیت غذایی عمومی غیر عمدی	۳/۸۹	۲	۷/۷۸	۲/۸	۲۱/۸
۳۴	عوامل بهداشتی	آلودگی باکتریایی مخازن آب آشامیدنی	۳/۰۲	۱/۹۸	۵/۹۷	۳/۴	۲۰/۳
۳۵	عملیات	تأخیر در انجام هماهنگی با پایگاه‌های همجوار	۳/۰۶	۲/۱	۶/۴۲	۳/۱۵	۲۰/۲
۳۶	پشتیبانی	تخریب جاده دسترسی به‌علت بارش باران‌های کوهستانی	۲/۱۲	۱/۹۴	۴/۱۱	۴/۹	۲۰/۱
۳۷	عملیات	سرعتِ عمل پایین اپراتور در ثبت و مستندسازی فرایندهای عملیاتی	۳/۰۴	۲	۶/۰۸	۳/۳	۲۰
۳۸	ایمنی کار	برق گرفتگی کارکنان حین انجام کار	۳/۰۴	۲/۱۲	۶/۴۴	۳	۱۹/۳
۳۹	نیروی انسانی	کمبود نیروی پشتیبانی	۲	۳	۶	۳/۲	۱۹/۲
۴۰	پشتیبانی	اتمام ذخیرهٔ سوخت نیروگاه برق داخلی	۳	۲/۱	۶/۳	۳	۱۸/۹
۴۱	عملیات	اشتباه در انتقال اطلاعات پردازش شده به پایگاه‌های موشکی و مبادی بالادستی	۳/۹۳	۱/۹	۷/۴۶	۲/۵	۱۸/۶
۴۲	امنیّت اطلاعات	افشای اطلاعات طبقه‌بندی به‌دلیل امحای ناقص و نامناسب اطلاعات	۳/۰۴	۲	۶/۰۸	۳	۱۸/۲
۴۳	حفاظت فیزیکی	عدم پشتیبانی از سوی یگان‌های همجوار به‌دلیل بعد مسافت	۳	۲	۶	۳	۱۸
۴۴	عوامل بهداشتی	گزش جانوران موذی سمی	۲/۰۴	۱/۹۶	۳/۹۹	۴/۴	۱۷/۶
۴۵	ایمنی کار	مجهز نبودن ساختمان‌ها و تاسیسات به سامانه‌های اعلام خطر	۲/۰۶	۱/۹۸	۴/۰۷	۴	۱۶/۳
۴۶	نیروی انسانی	کمبود نیروی خدماتی	۲/۰۴	۳/۰۲	۶/۱۶	۲/۵	۱۵/۴

۴۷	پشتیبانی	کمبودِ وسائل نقلیه و ماشین آلات	۲/۱۲	۲/۹۸	۶/۳۱	۲/۴	۱۵/۱
۴۸	حفاظت فیزیکی	کمبود اسلحه و مهمات پاسداری	۳	۲/۱۴	۶/۴۲	۲/۲	۱۴/۱
۴۹	عوامل بهداشتی	از کارافتادن سیستم سردخانهٔ مواد غذایی فاسدشدنی	۲/۰۲	۲/۰۴	۴/۱۲	۳/۳	۱۳/۶
۵۰	حفاظت فیزیکی	سرقت اسلحه و مهمات	۳	۲/۰۲	۶/۰۶	۲/۲	۱۳/۳
۵۱	ایمنی کار	نبود تجهیزات مقابله با تک هسته‌ای، میکروبی، شیمیایی	۲/۰۸	۲/۰۴	۴/۲۴	۳	۱۲/۷
۵۲	ایمنی کار	غیرکالیبره شدن تشعشعات راداری	۲/۱۶	۱/۲۴	۲/۶۷	۴/۵	۱۲/۱
۵۳	پشتیبانی	اتمام ذخیره آب و مواد غذایی	۱/۹۵	۳	۵/۸۵	۲/۰۵	۱۲
۵۴	حفاظت فیزیکی	سرقت اموال منقول و غیر منقول	۳	۱/۱۸	۳/۵۴	۲/۸	۱۰

مطابق با فن ویلیام فاین و RFMEA از میانگین امتیازات استفاده گردید و نتایج حاصل از آزمون میانگین نمونهٔ آماری برای هر یک از حوزه‌های هشت‌گانهٔ پرسشنامه بعد از وزن‌دهی به نسبت تعداد مؤلفه‌های هر عامل محاسبه گردید:

نتایج مربوط به پرسشنامه اول(شدت ریسک) بیانگر آن است که ۳۷ ریسک دارای شدت پیامد بالا و ۲ ریسک دارای شدت پیامد پایین و ۱۵ریسک دارای شدت پیامد متوسط هستند. قابلیت رتبه‌بندی مؤلفه‌ها از طریق آزمون فریدمن[1] مورد بررسی قرار گرفت. بر این اساس، آماره کای اسکوئر برابر ۲۲۲۵/۲ با درجهٔ آزادی ۵۳ و سطح معناداری۰/۰۰۰ به دست آمد؛ بنابراین اولویت‌بندی‌های حاصل بر اساس میانگین رتبه‌ای فریدمن به‌طور کامل با اولویت‌بندی مؤلفه‌ها براساس میانگین امتیازات هماهنگ و منطبق بود. یافته‌ها حاکی است در زمینهٔ *شدتِ ریسک*، گروه تعمیر و نگهداری با ضریب اولویت ۱۷ درصد بیشترین میانگین را دارد و کمترین ضریب اهمیت شدت ریسک مربوط به گروه پشتیبانی با ضریب ۱۰ درصد است. بر این اساس می‌توان نتیجه گرفت که ریسک‌های زیرگروه حوزهٔ تعمیر و نگهداری، در صورت وقوع بیشترین شدت اثر منفی را بر تداوم عملیات و مأموریت پایگاه دارند و ریسک‌های مرتبط با تدارکات کمتر از

[1] Friedman test

سایر حوزه‌ها اثر مخرب و منفی برجای می‌گذارند. سایر ضرایب اهمیت عبارتند از: گروه عملیات ۱۵درصد، ایمنی کار۱۲درصد، نیروی انسانی۱۲درصد، حفاظت فیزیکی۱۲ درصد، امنیّت اطلاعات۱۱ درصد و عوامل بهداشتی۱۱ درصد.

نتایج مربوط به پرسشنامه دوم (احتمال وقوع ریسک) حاکی از آن است که ۱۶ مخاطره دارای احتمال وقوع بالا، ۲۰ مخاطره دارای احتمال وقوع پایین و ۱۸ مخاطره دارای احتمال وقوع متوسط می‌باشند. قابلیت رتبه‌بندی مؤلفه‌ها از طریق آزمون فریدمن مورد بررسی قرار گرفت. بر این اساس آماره کای اسکوئر برابر ۲۰۳۹/۵ با درجهٔ آزادی ۵۳ و سطح معناداری۰/۰۰۰ به دست آمد؛ بنابراین اولویت‌بندی‌ها بر اساس میانگین رتبه‌ای فریدمن به‌طور کامل با اولویت‌بندی مؤلفه‌ها بر اساس میانگین امتیازات هماهنگ و منطبق بود. در زمینهٔ احتمال وقوع ریسک، بیشترین احتمال وقوع ریسک‌ها متعلق به گروه نیروی انسانی با ضریب اهمیت ۱۶ درصد و کمترین احتمال وقوع متعلق به گروه ایمنی با ضریب اهمیت۸ درصد است؛ به عبارتی ریسک‌های حوزهٔ نیروی انسانی از سایر ریسک‌ها تکرارپذیرترند، اما در حوزهٔ ایمنی کار احتمال وقوع ریسک‌ها کمتر از سایر حوزه‌ها است. سایر ضرایب اولویت عبارتند از: گروه امنیّت اطلاعات۱۴درصد، تعمیر و نگهداری۱۴درصد، عوامل بهداشتی۱۳ درصد، حفاظت فیزیکی۱۲ درصد، پشتیبانی۱۲ درصد، عملیات۱۱ درصد.

نتایج حاصل از پرسشنامهٔ سوم (ضریب تعیین ریسک) بیانگر این است که تعداد ۳۲ مخاطره دارای ضریب تعیین بالا، ۲۲ مخاطره نیز دارای ضریب تعیین متوسط و هیچ مخاطره‌ای دارای ضریب تعیین پایین نیست. بیان این نکته ضروری است که هر چقدر ضریب تعیین یک مؤلفه بالاتر باشد، شناسایی و پاسخگویی مناسب به ریسک دشوارتر و غیرممکن‌تر خواهد بود. قابلیت رتبه‌بندی مؤلفه‌ها از طریق آزمون فریدمن مورد بررسی قرار گرفت. بر این اساس، آماره کای اسکوئر برابر ۲۲۳۲/۵ با درجهٔ آزادی ۵۳ و سطح معناداری۰/۰۰۰ به دست آمد؛ بنابراین اولویت‌بندی بر اساس میانگین رتبه‌ای فریدمن در این پرسشنامه نیز با اولویت‌بندی مؤلفه‌ها بر اساس میانگین امتیازات هماهنگ بود. از نظر اولویت‌بندی ضریب تعیین ریسک، بالاترین ضرایب مربوط به گروه امنیّت اطلاعات با ضریب۱۴ درصد و کمترین ضرایب مربوط به حفاظت فیزیکی با ۱۱ درصد می‌باشد. به عبارت دیگر کشف و شناسایی ریسک‌های حوزهٔ امنیّت اطلاعات دشوارتر از سایر حوزه‌ها بوده و زمان عامل مهمی در ارائه پاسخ مناسب به آن‌هاست؛ در حالی که ریسک‌های حوزهٔ حفاظت فیزیکی روش کشف و شناسایی مؤثرتر و

ساده‌تری داشته و زمان کافی برای ارائه پاسخ مقتضی به آن‌ها نیز در دسترس می‌باشد. سایر ضرایب عبارتند از: گروه پشتیبانی۱۳ درصد، تعمیر و نگهداری۱۳ درصد، عوامل بهداشتی۱۳ درصد، ایمنی کار۱۲ درصد، نیروی انسانی۱۲ درصد، عملیات۱۲ درصد.

نمرهٔ ریسکR از ادغام ضرایب مربوط به شدت ریسک و احتمال وقوع ریسک به دست می‌آید. بعد از ادغام ضرایب مربوط و مشخص شدن نمرهٔ هر ریسک، اولویت‌بندی عوامل هشت‌گانه بر اساس نمرهٔ ریسک به دست آمد: بر این اساس گروه تعمیر و نگهداری با ضریب ۱۸ درصد دارای بالاترین قابلیت ریسک و گروه ایمنی با ضریب ۸ درصد کمترین قابلیت ریسک را دارا هستند. سایر ضرایب عبارتند از: گروه نیروی انسانی۱۵ درصد، عملیات ۱۴ درصد، امنیّت اطلاعات ۱۳ درصد، عوامل بهداشتی۱۱ درصد، حفاظت فیزیکی۱۱ درصد، پشتیبانی۹ درصد.

در نهایت از نظر RPN در سطح عوامل هشت‌گانه ریسک‌های پایگاه‌های پدافند این نتیجه استنباط می‌شود که گروه تعمیر و نگهداری با ضریب اولویت ۲۰ درصد بحران‌سازترین حوزه در تداوم عملیات پایگاه‌های پدافندی است؛ سپس گروه مدیریت نیروی انسانی با ضریب ۱۵ درصد و امنیّت اطلاعات با ضریب۱۴ درصد قرار دارند. گروه عملیات۱۲ درصد، عوامل بهداشتی ۱۱درصد و پشتیبانی ۱۰ درصد در حد متوسط و گروه حفاظت فیزیکی و ایمنی کار هر کدام با ضریب اولویت ۹ درصد کم بحران‌ترین ریسک‌ها را در خود جای داده‌اند:

جدول۵: اولویت‌بندی ریسک گروه‌ها برحسب RPN ریسک

گروه‌ها	RPN	تعداد گویه	ضریب اولویت
تعمیر و نگهداری	۴۱/۷۳	۷	۰/۲۰
نیروی انسانی	۳۱/۳۱	۶	۰/۱۵
امنیّت اطلاعات	۲۸/۸۱	۷	۰/۱۴
عملیات	۲۵/۸۳	۷	۰/۱۲
عوامل بهداشتی	۲۲/۸۵	۶	۰/۱۱
پشتیبانی	۲۰/۳۴	۷	۰/۱۰
حفاظت فیزیکی	۱۹/۱۲	۷	۰/۰۹
ایمنی کار	۱۸/۸۵	۷	۰/۰۹

سؤال فرعی۱: مهمترین عامل بحرانی شدن ریسک‌های موجود در پایگاه پدافند کدامند؟

فرضیه۱: شدت ریسک رابطه معناداری با RPN دارد.

ضریب همبستگی پیرسون بین RPN و شدت تأثیر ریسک برابر با ۰/۵۸۱ و سطح معناداری ۰/۰۰۰ است؛ از این رو فرضیهٔ مورد تأیید قرار گرفت. نتایج نشان می‌دهد افزایش شدت تأثیر ریسک‌ها رابطهٔ معنادار مثبتی با افزایش قابلیت مخاطره آفرینی دارد.

جدول ۶: ضریب همبستگی پیرسون بین RPN و شدت پیامد ریسک

	RPN	معناداری
شدت پیامدX	۰/۵۸۱	۰/۰۰۰

فرضیه۲: احتمال وقوع رابطهٔ معناداری با RPN دارد.

ضریب همبستگی پیرسون بین RPN و احتمال وقوع ریسک برابربا ۰/۶۵۸و سطح معناداری ۰/۰۰۰ است. از این رو فرضیه مذکور مورد تأیید قرار گرفت. افزایش در احتمال وقوع موجب افزایش معنادار مثبت در قابلیت مخاطره آفرینی می‌شود.

جدول۷: ضریب همبستگی پیرسون بین RPN و احتمال وقوع ریسک

	RPN	معناداری
احتمال وقوعY	۰/۶۵۸	۰/۰۰۰

فرضیه۳: ضریب تعیین رابطه معناداری با RPN دارد.

ضریب همبستگی پیرسون بین RPN و ضریب تعیین برابر ۰/۲۵۳ و سطح معناداری برابر ۰/۰۶۴ است. بنابراین فرضیه مذکور تأیید نشد؛ به عبارت دیگر تغییرات ضریب تعیین ریسک‌ها موجب تغییرات معناداری در مقدار قابلیت مخاطره آفرینی نمی‌شود.

جدول۸: ضریب همبستگی پیرسون بین RPN و ضریب تعیین ریسک

	RPN	معناداری
ضریب تعیینZ	۰/۲۵۳	۰/۰۶۴

در نتیجه RPN با احتمال وقوع بالاترین همبستگی و با درجهٔ ریسک نیز همبستگی بالایی دارد ولی با ضریب تعیین همبستگی معناداری ندارد.

تحلیل رگرسیون چندگانه: بر اساس تحلیل رگرسیون صورت گرفته مشاهده می‌شود که احتمال وقوع بیشترین تأثیر را بر بحرانی شدن ریسک دارد. در واقع یک واحد کاهش در احتمال وقوع ریسک باعث کاهشی به اندازه ۰/۷۷۷ واحد در RPN ریسک می‌شود:

جدول ۹: تحلیل رگرسیون چندگانه

متغیر	B	خطای معیار	BETA	T	سطح معناداری
شدت تأثیر	۸/۵۲۱	۰/۶۱۲	۰/۵۳۸	۱۳/۹۱۲	۰/۰۰۰
احتمال وقوع	۱۲/۴۸۵	۰/۶۴۲	۰/۷۷۷	۱۹/۴۳۷	۰/۰۰۰
ضریب تعیین	۷/۷۱۷	۰/۷۶۵	۰/۴۰۶	۱۰/۰۹۳	۰/۰۰۰

سوال فرعی ۲: ریسک‌های بحرانی کدامند؟

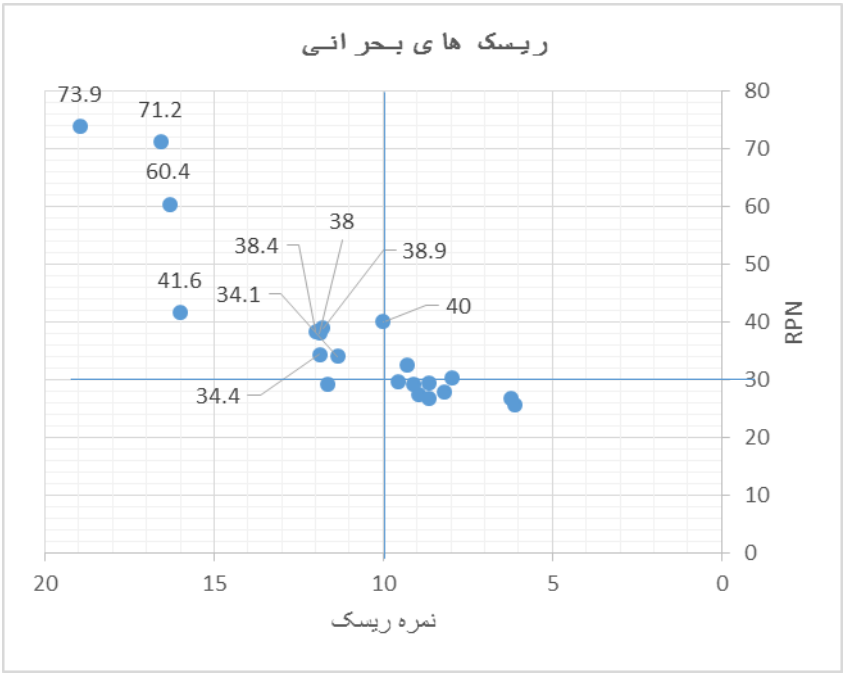
مقادیر RPN و نمرهٔ ریسک برای ریسک‌های بحرانی در جدول ذیل آورده شده است. بر این اساس ۱۰ ریسک که نمرهٔ ریسک آن‌ها بیشتر از ۱۰ و RPN آن‌ها بیشتر از ۳۰ است به عنوان ریسک‌های بحرانی انتخاب شده‌اند:

جدول۱۰: ریسک‌های بحرانی

ردیف	حوزه	ریسک بحرانی	RPN
۱	تعمیر و نگهداری	خاموش کردن سامانه‌های عملیاتی جهت جلوگیری از آسیب رعد و برق	۷۳/۹
۲	تعمیر و نگهداری	قطع کلیه خطوط ارتباطی بی‌سیم و تلفنی	۷۱/۲
۳	نیروی انسانی	کمبود نیروی متخصص عملیاتی	۶۰/۴
۴	عملیات	اشتباه در کشف و شناسایی اهداف متخاصم پروازی	۴۱/۶
۵	تعمیر و نگهداری	قطع برق سراسری و برق نیروگاه داخلی به‌طور همزمان	۴۰
۶	نیروی انسانی	کمبود نیروی متخصص تعمیر و نگهداری	۳۸/۹

ردیف	حوزه	ریسک بحرانی	RPN
۷	امنیّت اطلاعات	افشای اطلاعات طبقه‌بندی از طریق ماهواره‌های جاسوسی و عکسبرداری	۳۸/۴
۸	امنیّت اطلاعات	افشای اطلاعات طبقه‌بندی شده از طریق مکالمات بی‌سیم و تلفنی	۳۸
۹	عوامل بهداشتی	عدم دسترسی به فوریت‌های پزشکی	۳۴/۴
۱۰	تعمیر و نگهداری	خرابی دستگاه‌ها و تجهیزات سامانه‌های راداری عملیات	۳۴/۱

از این ده ریسک بحرانی، تعداد ۴ مورد مربوط به عامل تعمیر و نگهداری و ۲ مورد مربوط به نیروی انسانی هستند. دو مورد متعلق به حوزهٔ اطلاعاتی، یک مورد از حوزهٔ عملیات و یک مورد نیز از حوزهٔ عوامل بهداشتی هستند.



نمودار۱ : ریسک‌های بحرانی

بحث و تحلیل

۱- مهمترین ریسک در زمینه توقف عملیات، خاموشی‌های مکرر سامانه‌ها با هدف جلوگیری از آسیب رعد و برق به آن‌ها با RPN=۷۴ است. پایگاه‌های یاد شده به دلیل نوع عملکرد عموما در ارتفاعات کوهستانی مستقرند و در شرایط آب و هوایی ناپایداری قرار دارند و در تمام ماه‌ها پی‌درپی با پدیدهٔ رعدوبرق مواجه‌اند؛ برای جلوگیری از آسیب به تجهیزات حسّاس ناچار به خاموش کردن سامانه‌های الکترونیک و جداسازی آن‌ها از آنتن‌های گیرنده و فرستنده می‌شوند. در همین راستا بروز صاعقه‌های مکرر موجب آسیب سامانه‌های حسّاس مخابراتی و تجهیزات درون ماکس‌های ارتباطی نیز می‌شوند و این مسئله به همراه نوسانات جوی، تشعشعات راداری و کیهانی، تداخل امواج و... می‌تواند باعث قطع مکرر خطوط ارتباطی و بی‌سیم شده، جریان اطلاعاتی و عملیات عادی پایگاه را مختل نماید (دومین ریسک بحرانی با RPN=۷۱).

۲- براساس نتایج تحقیق، کمبود نیروی متخصص عملیاتی با RPN=۶۰ و کمبود نیروی متخصص تعمیر و نگهداری با RPN=۳۹ به ترتیب سومین و ششمین مخاطرهٔ بحران‌ساز در تداوم فعالیت پایگاه‌های پدافندی‌اند. با توجه به تفکیک پدافند از نیروی هوایی و تشکیل قرارگاه پدافند هوایی، به عنوان یک نیروی نوپا، مستقل و متمرکز در کنار نیروهای سه‌گانه طی چند سال اخیر، این نیرو هنوز در حال تعریف و تثبیت نظام مدیریتی، اداری و عملیاتی است و بالطبع در زمینهٔ مدیریت منابع انسانی نیز در حال آزمون و خطا بر روی سیاست‌های تعدیل نیرو، کاهش سِمت‌های شغلی، حرکت به سوی سبک‌سازی و حرفه‌ای‌گرایی است. کاهش سِمت‌های سازمانی در همه واحدها و تخصص‌ها با نسبت مشابه و بدون مطالعات نیازسنجی قطعا موجب بروز نابسامانی در تأمین نیروی انسانی به خصوص در تخصص‌های حسّاس می‌شود.

۳- اشتباه در کشف و شناسایی اهداف متخاصم پروازی با RPN=۴۲، افشای اطلاعات طبقه‌بندی شده از طریق مکالمات بی‌سیم و تلفنی و افشای اطلاعات طبقه‌بندی از طریق ماهواره‌های جاسوسی و عکسبرداری هرکدام با RPN=۳۸ به ترتیب به عنوان چهارمین، هفتمین و هشتمین مؤلفه بحران‌ساز در پایگاه‌های پدافند، بیانگر لزوم توجه کافی به انگیزش و آموزش بدو خدمت کارکنان جدیدالورود و تداوم آموزش حین خدمت کارکنان قدیمی در کنار بهره‌برداری از فرصت‌های علمی و تحقیقاتی جهت طراحی، ساخت، خرید و بروزرسانی

سامانه‌های راداری همگام با تغییرات سریع فناوری در دنیا هستند. امروزه جِسگرهای فوق‌العاده ظریف سامانه‌های جاسوسی ماهواره‌ای و پروازهای شناسایی، نه فقط بر مبنای دید چشمی بلکه بر اساس کوچک‌ترین میزان انتشار شیمیایی، حرارتی، ارتعاشی، امواج الکتریکی، الکترونیکی، صوتی، رادیویی، رادیو اکتیو، مغناطیسی و ... از تاسیسات کشور هدف قادر به کشف و شناسایی مکان‌های حسّاس غیرنظامی و نظامی، استعداد نیروها، تجهیزات، تسلیحات، نوع فعالیت‌ها، نحوهٔ ترددها، ارزیابی عملکردها و قابلیت‌ها از فواصل دور و بدون نیاز به برخورد نزدیک هستند.

۴- با توجه به مسافت و هزینهٔ بالای تأمین برق از شبکه برق سراسری و مشکلات تعمیر و نگهداری مربوط به آن، پایگاه‌های پدافندی در تأمین برق اغلب به صورت خودکفا عمل نموده و از شبکه برق سراسری به عنوان سیستم پشتیبان استفاده می‌کنند. با این‌حال قطع همزمان برق سراسری و برق نیروگاه داخلی، در عین احتمال وقوع کم، به عنوان پنجمین ریسک بحرانی با RPN=۴۰ نشان‌دهنده میزان شدت پیامد بالای این مؤلفه بر خاموشی‌های ناخواسته در سامانه‌های پدافند است.

۵- دسترسی نداشتن به فوریت‌های پزشکی با RPN=۳۴/۴ به عنوان نهمین ریسک بحرانی پایگاه‌های پدافند ناشی از فاصله زیاد با مراکز درمانی و بیانگر کمبود تجهیزات اولیه اورژانسی در محل است. بی‌توجهی به این امر موجب به خطر افتادن جان کارکنان می‌شود که بزرگ‌ترین سرمایهٔ یک سازمان نظامی بشمار می‌روند.

۶- طبق نتایج تحقیق خرابی دستگاه‌ها و تجهیزات سامانه‌های راداری عملیات با RPN=۳۴ آخرین ریسک بحرانی است که در صورت وقوع می‌تواند موجب توقف رهگیری و اختلال در شناسایی اهداف متخاصم گردد.

نتیجه‌گیری

این تحقیق با هدف شناسایی و اولویت‌بندی ریسک‌های مؤثر بر تداوم عملیات در پایگاه‌های پدافند صورت گرفت. اهمیت راهبردی سامانه‌های راداری و شناسایی الکترونیک بر رصد لحظه به لحظه، هوشیاری شبانه‌روزی، تحلیل به موقع و دقیق اطلاعات، هماهنگی منسجم و اقدام پیش‌دستانه برای حفظ تمامیت ارضی، حریم هوایی و گسترهٔ آبی استوار است. باید ریسک‌ها و مخاطراتی که در مورد تداوم عملیات این پایگاه‌ها مدنظر قرار می‌گیرند با مقیاس ثانیه سنجش شوند. توقف عملیات و خاموشی سامانه‌های راداری در این پایگاه‌ها حتی برای چند ثانیه

می‌تواند موجب بی‌دفاع ماندن بخشِ وسیعی از مرزهای کشور در مقابل نفوذ، تجسس و یا حملات احتمالی نیروهای متخاصم، به خصوص تهدیدات پر سرعت پروازی شود. در این تحقیق ۵۴ ریسک که دارای تأثیر بالقوه بر استمرار و توقف فعالیت‌ها بودند با استفاده از فن RFMEA و فن ویلیام فاین مورد شناسایی، ارزیابی و اولویت‌بندی قرار گرفتند و۱۰ریسک دارای قابلیت بالاتر مشخص شدند. همچنین مشخص گردید که احتمال وقوع ریسک با ضریب همبستگی۰,۶۵ بیشترین اثر را در بحرانی شدن ریسک‌ها و ضریب تعیین با ضریب همبستگی ۰,۲۵۳ کمترین تأثیر را دارد. این مسئله بیانگر این موضوع است که ریسک‌های مطرح در پایگاه‌های پدافندی، نه به‌خاطر ناتوانی در کشف و کمبود زمان پاسخ دهی به آن‌ها، بلکه بیشتر به دلیل عدم اهتمام برای رفع آن‌ها به وضعیت بحران می‌رسند. به عبارت دیگر علی‌رغم اینکه ریسک‌ها به آسانی کشف می‌شوند و موقعیت رفع آن‌ها نیز فراهم می‌باشد، امّا اغلب به دلیل بی‌توجهی به رفع آن‌ها، به‌طور مکرر رخ داده و به مرز بحران‌سازی می‌رسند. این مسئله را می‌توان در بالا بودن ضریب همبستگی احتمال وقوع و RPN مشاهده نمود.

پیشنهادها

برای یافتن راهبردهای پاسخ، با کمک نظر خبرگان پیشنهادهای ممکن مربوط به هر ریسک بحرانی تعیین شد تا بتوان برای رفع یا کاهش آن‌ها اقدام نمود.

الف: انجام تحقیقات علمی و استفاده از ظرفیت‌های فنی و مهندسی موجود، برای مقابله با ریسک‌های گروه تعمیر و نگهداری و کاهش چشمگیر تعطیلی عملیات از طریق: ۱- بِروزرسانی سامانه‌های برقگیر؛ ۲- تهیه و نصب روکش‌ها و ریدوم‌های(RADOME) محافظ در برابر صاعقه؛ ۳- استقرار سامانه‌های برق اضطراری و upsها؛ ۴- انجام بازرسی‌های دوره‌ای از سامانه‌ها و برطرف‌سازی عیوب آن‌ها قبل از توقف اساسی کار؛ ۵- سرویس منظم ژنراتورهای برق؛ ۶- پیش‌بینی ژنراتورهای جایگزین؛ ۷- هماهنگی با ادارات برق منطقه‌ای در مورد اطلاع‌رسانی قبل از قطع برق و کاهش میزان خاموشی‌ها؛ ۸- ایجاد ذخیرهٔ کافی از قطعات یدکی و ۹- تأمین نیروی انسانی متخصص تعمیر و نگهداری.

ب- پیشنهادها برای مقابله با ریسک‌های گروه نیروی انسانی با هدف کاستن از میزان ترک خدمت، نارضایتی شغلی و غیبت کارکنان: ۱- توجه به تأمین نیروهای صف در پایگاه‌های راداری و سیگنت با انجام مطالعات نیازسنجی؛ ۲- تأمین نیازهای زیستی و رفاهی و ایجاد امکان ارتقای شغلی؛ ۳- تحقّق عادلانهٔ مزایا و فوق العاده‌ها و کاهش تبعات سختی کار.

ج- در گروه امنیّت اطلاعات پیشنهاد می‌شود: ۱- امنیت شبکهٔ ارتباطات تأمین شود؛ ۲- دستگاه‌های رمزکننده اطلاعات طبقه‌بندی شود؛ ۳- روش‌های قدیمی استتار و اخفا مورد بازبینی قرار گیرد و ۴- تجهیزات نوین، شناسایی و به‌کارگرفته شوند.

د- در گروه عوامل بهداشتی پیشنهاد می‌شود: ۱- فرماندهان پایگاه نسبت به تأمین کادر پزشکی و آمبولانس مجهز به تجهیزات اورژانس اقدام کنند؛ ۲- فرماندهان پایگاه دستورالعمل‌های مشخصی را برای مواقع اضطرار تهیه کنند تا در مواقع اضطراری از اتلافِ زمان جلوگیری شود.

فهرست منابع

۱- آقامحمدی، داوود، (۱۳۹۰)، «عوامل مؤثر بر چابکسازی سازمان‌های نظامی کشور با نگرش به تهدیدات آینده»، فصلنامه مطالعات دفاعی استراتژیک، سال۱۱، شماره۴۴، تابستان۹۰، ص۶۳ تا۸۸.

۲- بورس اوراق بهادار تهران، (بی‌تا)، چارچوب مدیریت ریسک بورس اوراق بهادار تهران(tse) مدیریت ریسک، چارچوب یکپارچه، جلد اول، بی‌جا.

۳- پورصادق، ناصر؛ فرشچی، سیدمحمدرضا؛ موحدی صفت، محمدرضا، (۱۳۹۲)، «مدیریت ریسک در محیط‌های نظامی و ارائه یک الگوی ارزیابی مبتنی بر نظریه بازی‌ها»، فصلنامه مدیریت نظامی، سال سیزدهم، شماره ۱، پاییز ۹۲، ص ۱ تا ۴۴.

۴- حقیری، علی اصغر؛ ستاریخواه، علی، (۱۳۸۴)، «سامانهٔ فرماندهی و کنترل به عنوان عامل برترساز در نیروهای مسلح»، فصلنامه مطالعات دفاعی استراتژیک دانشگاه عالی دفاع ملی، شماره۲۳-۲۴، ص ۱۶۳ تا ۱۸۸.

۵- ساکی‌زاده، مراد؛ جهانگیرزاده، منصور، (۱۳۸۷)، «بررسی جامعه‌شناختی ویژگی‌های فرماندهان و تأثیر آن بر توانمندی ارتش»، فصلنامه مدیریت نظامی، شماره ۳۰، ص ۱۲۹ تا ۱۵۰.

۶- عالم تبریز، اکبر؛ حمزه‌ای، احسان، (۱۳۹۰)، «ارزیابی و تحلیل ریسک‌های پروژه با استفاده از رویکرد تلفیقی مدیریت ریسک استاندارد PMBOK و فن RFMEA»، فصلنامه مطالعات مدیریت صنعتی، سال نهم، شماره۲۳، زمستان ۱۳۹۰، ص ۱ تا ۱۹.

۷- مهدی، محمد؛ حشمتی، محمد رسول؛ کلهر، اصغر؛ بازیاری، حسین، (۱۳۹۳)، «بررسی میزان ریسک‌پذیری مالی افسران دانشگاه افسری امام علی(ع)»، فصلنامه مدیریت نظامی، شماره ۵۵، سال چهاردهم، پاییز ۹۳، ص ۱ تا ۲۰.

۸- واحدی، مرتضی؛ زارعی، علی اصغر، (۱۳۸۵)، «اطلاعات نظامی در عصر جهانی شدن»، ماهنامه نگرش راهبردی، شماره ۷۷-۷۸، ص ۷۳ تا ۱۱۰.

۹- یزدان فام، محمد، (۱۳۹۱)، «راهبرد دفاع ملی، درس‌هایی از پایان جنگ تحمیلی»، فصلنامه مطالعات راهبردی، سال پانزدهم، شماره سوم، شماره مسلسل۵۷، ص ۵۱ الی۷۰.

10- Dos Santos, Flávio Roberto Souza, Cabral, Sandro.“FMEA and PMBOK applied to project risk management”,journal of information systems and technology management, Vol. 5, No. 2, 2008.

11- Health Service Executie (HSE). Risk Management In Mental Health Services. Guidance Document.

WWW.HSE.IE/eng/services/publications/mentalhealth/riskmanagement mentalhealth.pdf

12- Segismundo,Andre,Miguel,P.A.C., “FAILURE MODE AND EFFECTS ANALYSIS(FMEA) IN THE CONTAXT OF RISK MANAGEMENT IN NEW PRODUCT DEVELOPMENT(a case study in an automotive company) ”,international journal of quality & reliability management, vol 25,no 9, pp899~912,2008.

13- United state of America;department of defence.risk management guide for DOD asquisition.six edition(version 1.0). August,2006.

14- Us Department Of Homeland Security. Risk Management Fundamentals.Homeland security risk manageent doctorine. April2011.