



The Evaluation of Desirability Information Security and Cyber Network Indicators in Ports with an Emphasis on Passive Defense (Case Study: Imam Khomeini Harbor)

L. Khouzestani, A. Maroofnezhad* 

*Associate Professor Department of Geography and urban planning, Mahshahr Branch, Islamic Azad University, Mahshahr, Iran.

(Received: 2024/09/06, Revised: 2024/11/29, Accepted: 2025/01/02, Published: 2025/02/01)

DOR:<https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.4.4.8>

ABSTRACT

Threats may impact ports, one of a nation's buildings and infrastructures. One of the most difficult and modern subjects in the field of port defense is the prevention of harm to maritime and port infrastructure and equipment by keeping the security of information and cyber network. Given the significance of the subject, this study used 15 indicators to assess and rank the information security and cyber network indicators in Imam Khomeini Harbor from the perspective of passive defense. Survey evaluation is the form of practical research used, and the primary research methodology is the questionnaire. The decided sample size is 100 individuals, and the statistical population includes the staff members and specialists of the harbor administration as well as some officials of the institutions of the city of Bandar Imam Khomeini (RA). The Kolmogorov-Sminrov test was used to examine the normality of the data distribution, and to investigate the status of the research variables, the Bartlett and KMO tests were used and Friedman's model was also used to order the indicators.

Keywords: Information Security and Cyber Network, Ports, Passive Diffence, Imam Khomeini Harbor

Cite this article: L. Khouzestani1 and A. Maroofnezhad2 “The Evaluation of Desirability Information Security and Cyber Network Indicators in Ports with an Emphasis on Passive Defense (Case Study: Imam Khomeini Harbor),” *Electronic and Cyber Defense*, vol.12 , no.4 , pp.27-37 , . DOR: <https://dor1.net/dor/> <https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.4.4.8>

© The Author(s).

Publisher: Imam Hossein University

*Corresponding Author Email: abbas.maroofnezhad@gmail.com



ارزشیابی مطلوبیت شاخص‌های امنیت اطلاعات و شبکه سایبری در بندرها با تأکید بر پدافند

غیرعامل (مطالعه موردی: مجتمع بندری امام خمینی (ره))

لیلا خوزستانی^۱، عباس معروف نژاد^{۲*} 

۱- کارشناسی ارشد، ۲- دانشیار گروه جغرافیا و برنامه‌ریزی شهری، واحد ماهشهر، دانشگاه آزاد اسلامی، ماهشهر، ایران

(دریافت: ۱۴۰۳/۰۶/۱۶، بازنگری: ۱۴۰۳/۰۹/۰۹، پذیرش: ۱۴۰۳/۱۰/۱۳، انتشار: ۱۴۰۳/۱۱/۱۳)

DOR: <https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.4.4.8>

* این مقاله یک مقاله با دسترسی آزاد است که تحت شرایط و ضوابط مجوز Creative Commons Attribution (CC BY) توزیع شده است.



ناشر: دانشگاه جامع امام حسین (ع) نویسندگان

چکیده

بندرها در میان تأسیسات و زیرساخت‌های کشورها، می‌توانند تحت تأثیر تهدیدات قرار گیرند. بازدارندگی آسیب به تأسیسات و تجهیزات دریایی و بندری با حفظ امنیت اطلاعات و شبکه سایبری یکی از چالش‌برانگیزترین و به‌روزترین موضوعات در زمینه حفاظت از بندرها به حساب می‌آید. نظر به اهمیت موضوع، این پژوهش به ارزیابی و رتبه‌بندی مطلوبیت امنیت اطلاعات و شبکه سایبری در بندر امام خمینی (ره) از منظر پدافند غیرعامل با استفاده از چهارده گویه/ شاخص پرداخته است. نوع تحقیق کاربردی و روش تحقیق، پیمایشی-ارزیابی با تأکید بر پرسشنامه است. جامعه آماری شامل کارکنان و کارشناسان خبره اداره بندر و برخی مسئولین نهادهای شهر بندر امام خمینی (ره) بوده که حجم نمونه تعیین‌شده ۱۰۰ نفر است. به‌منظور بررسی نرمال بودن توزیع داده‌ها از آزمون کلموگروف-اسمیرنوف و جهت بررسی وضعیت متغیرهای پژوهش از آزمون بارتلت و KMO و همچنین برای رتبه‌بندی شاخص‌ها از مدل فریدمن استفاده شده است.

کلیدواژه‌ها: امنیت اطلاعات و شبکه سایبری، بندرها، پدافند غیرعامل، مجتمع بندری امام خمینی (ره)

۱. مقدمه

کمک می‌کنند، اما مانند هر فناوری نوظهور دیگر، با خود خطراتی را نیز به همراه می‌آورند. به‌عنوان مثال، سازمانی که برای افزایش اثربخشی و کارایی خود در زمینه ارتباطات، از شبکه‌های مخابراتی و اینترنتی کمک می‌گیرد، باید مخاطرات ناشی از دسترسی افراد غیرمجاز یا رقبا به اطلاعات سازمان را بپذیرد یا آن‌ها را مدیریت کند. از این‌رو، در تصمیم‌گیری برای پیاده‌سازی سامانه‌های اطلاعاتی و بهره‌گیری از مزایای فناوری اطلاعات، مانند هر نوع تصمیم دیگر، باید به بررسی خطرات احتمالی آن پرداخت و با مدیریت مخاطره‌های موجود، اثربخشی سامانه‌ها را ارتقا بخشید [۳]. در این راستا پدافند غیرعامل مهم‌ترین مقوله‌ای است که می‌تواند آسودگی خاطر شهروندان، امنیت جانی و مالی آن‌ها و ایمنی زیرساخت‌ها را فراهم آورد. دفاع یا پدافند غیرعامل مجموعه اقداماتی است که به کمک آن‌ها می‌توان با کم‌ترین امکانات و تجهیزات نسبت به دفاع عامل از طریق کاهش یا حذف آسیب‌پذیری، کنترل پیامدهای تهاجم و افزایش قدرت مرمت‌پذیری در مقابل تهاجم غافلگیرانه دشمن و بدون استفاده از سلاح و درگیری مستقیم مقاومت نمود [۴]. بعد از دهه ۱۹۸۰

امروزه با توجه به گسترش استفاده از رایانه‌ها و فضای سایبری و به‌تبع آن افزایش چشم‌گیر خطرات موجود در این فضا، نیاز مبرمی به کسب دانش در این محیط‌ها وجود دارد. تحلیل‌گران این حوزه با دانستن انواع مختلف حملات و فنون به‌کاررفته به ارزیابی اثرات هر کدام از حملات پرداخته و خود را برای دفاع پیش‌کنش‌گرانه آماده می‌کند [۱]. حامیان دفاع پیش‌کنش‌گرانه با ارائه‌ی تعریفی جدید از دفاع مشروع، از دفاع در برابر حمله‌ی مسلحانه‌ی قریب‌الوقوع صحبت می‌کنند، حمله‌ای که هنوز صورت نگرفته است، اما به‌احتمال قریب به‌یقین به‌زودی رخ خواهد داد. بر این اساس، دولت‌ها حق دارند حمله‌ی احتمالی قریب‌الوقوع را شناسایی و پیش‌بینی کرده و به‌طور پیش‌دستانه قبل از آن که دشمن اقدام کند در استفاده از نیروی مسلح پیشی بگیرند و تهدید احتمالی را دفع کنند [۲]. از سویی دیگر در دنیای امروز فناوری اطلاعات و سامانه‌های اطلاعاتی در همه بخش‌های زندگی بشر ریشه دوانیده‌اند و گرچه به تسهیل زندگی و ارتباطات بشر

سواحل، گامی در جهت استفاده و بهره‌گیری مناسب و بهینه از سواحل و بندرها به‌عنوان مناطق و مجموعه‌های بااهمیت می‌باشند. بدیهی است با افزایش درجه اهمیت یک موضوع و منطقه برای کشور، ضرایب ایمنی، امنیتی آن نیز افزایش می‌یابد و چگونگی تداوم فعالیت بندرها و سواحل در حوزه‌های تجاری و ارتباطی را در شرایط بحرانی ناشی از تهدیدات دشمن نیز موردبررسی قرار داده و با بهره‌گیری از تدابیر و تمهیدات ویژه پدافند غیرعامل، ضرایب ایمنی، امنیتی و دفاعی بندرها و سواحل را برای تداوم فعالیت‌ها در زمان‌های صلح و جنگ افزایش دهد. دامنه این تدابیر و تمهیدات از جزئی‌ترین عناصر، تجهیزات و سازه‌های بندر تا راهبردی‌ترین موضوعات کشور در ارتباط با مدیریت، آمایش سرزمین و مسائل مربوط به تجارت و اقتصاد گسترده است. زمینه‌های مختلف مقابله با تهدیدات دشمن که می‌تواند از جنگ اقتصادی، تهدید تجارت، تهدید ناوگان‌های تجاری، یا به‌ویژه جنگ الکترونیک، حملات سایبری و مختل کردن شبکه‌های اطلاعات و درنهایت اقدام به تخریب برخی از سواحل و بندرها و یا حتی تسخیر گسترده باشد؛ بسیار متنوع و هوشمندانه و کارآمد هستند.

هم‌زمان با احداث راه‌آهن سراسری کشور در سال ۱۳۰۷ هجری شمسی، دو پست اسکله چوبی در شمال غربی خلیج فارس و در انتهای آبراه خورموسی (با موقعیت جغرافیایی ۳۰ درجه و ۲۵ دقیقه شمالی و ۴۹ درجه و ۵ دقیقه شرقی) ساخته شد. پس از چندی به بندر شاپور موسوم گشت و سه سال بعد به مهم‌ترین مرکز ورود و خروج کالا تبدیل شد. در سال ۱۳۵۲ محل سکونت اهالی این نقطه، از کنار اسکله‌ها به شهر بندر امام خمینی (ره) انتقال یافت و زمینه برای توسعه هرچه بیشتر بندر مهیا گردید؛ پس از پیروزی انقلاب شکوهمند اسلامی ایران، این بندر به بندر امام خمینی (ره) تغییر نام یافت و در سال ۱۳۶۱ با تصویب هیئت‌وزیران رسماً بندر امام خمینی (ره) نام گرفت و شروعی نو را پایه نهاد. بندر امام خمینی (ره) حرکت به‌سوی تحول را از همان دو اسکله چوبی آغاز نمود و امروز با انجام بیش از ۱۵٪ از کل تجارت دریایی کشور، نوید توسعه‌ای پایدار را برای منطقه از طریق صنعت حمل‌ونقل می‌دهد. بندر امام خمینی (ره) در اوایل دهه ۱۳۹۰ پس از تغییر رژیم حقوقی خود از یک بندر عادی به منطقه ویژه اقتصادی و الحاق اراضی مجاور، هم‌اکنون با بالغ‌بر

میلادی و ظهور فرآیند جهانی‌شدن، عملکرد بندرها نیز متحول شده است. به‌طوری‌که بندرها امروزی علی‌رغم بندرها سنتی که محموله‌های خشک و خرد جابجا می‌شود، محل جابجایی محموله‌های استاندارد و کانتینری، تبادل فن‌آوری/دانش و انجام فعالیت‌های لجستیکی شده‌اند. کشور ایران با دارا بودن ۵۸۰۰ کیلومتر نوار ساحلی در شمال و جنوب کشور (با احتساب محیط پیرامون جزایر ایران در خلیج فارس و دریای عمان) که در حدود ۴۰ درصد از مرزهای کشور را تشکیل می‌دهد، در بین ۱۸۲ کشور مستقل و مشرف به دریا و اقیانوس در دنیا، رتبه چهارم رادار است. از سویی به‌طور متوسط کشورهایی که از طول خطوط ساحلی بالاتری برخوردارند، اقتصاد اقیانوس با سهم مشارکت بالاتری هم در اقتصاد ملی دارند [۵]. اهمیت زیرساخت‌های بندری و دریایی به حدی است که در ایالات‌متحده آمریکا هشت طرح راهبردی مستقل در حوزه حفاظت از زیرساخت‌های بندری و دریانوردی تهیه شده است. ایجاد زمینه‌سازی مناسب علمی برای عمق‌بخشی به مراحل مختلف راهبردی پدافند غیرعامل بندرها و استخراج مؤلفه‌ها و شاخص‌های مؤثر در کاهش آسیب‌پذیری، ارتقاء پایداری و استحکام فنی، تداوم فعالیت‌های ضروری و تسهیل مدیریت بحران در بندرها کشور در مواجهه با تهدیدات دریا پایه اهمیت زیادی دارد [۶].

امروزه جنگ‌های مدرن را می‌توان جنگ‌هایی مبتنی بر سلسله‌ای از حملات دقیق و فشرده بر دسته‌های منتخبی از اهدافی که در یک نظام سلسله‌مراتب عملکردی گزینش شده‌اند، محسوب نمود؛ که روش‌های دفاع در برابر این حملات باید مبتنی بر دفاع سطح‌بندی شده از منابع دارای اهمیت‌های عملکردی سلسله‌مراتبی باشد. از این‌رو در این فضای بحرانی که حوادث با شدت و سرعت زیاد پیایی بر کم و کیف آسیب‌ها می‌افزایند در صورت عدم وجود زیرساخت‌ها و امکانات مناسب دفاعی، حفاظتی و پشتیبانی، بروز فاجعه انسانی در پهنه مناطق موردتهاجم احتمال نیرومندی محسوب می‌شود. بندرها و سواحل ازجمله مهم‌ترین مناطق مرزی محسوب می‌گردند. اتصال به آب‌های آزاد و ارتباطات تجاری و بین‌المللی از طریق امکان تجارت دور، ازجمله ویژگی‌های بندرها و سواحل هستند. برای ایران و اغلب کشورهای جهان، تجارت و تبادل کالا از طریق دریا و با بهره‌گیری از سواحل و بندرها صورت می‌گیرد. سواحل و مناطق هم‌جوار آن‌ها در خشکی و دریا از اهمیت حیاتی برای کشورها برخوردارند. آمایش، سازمان‌دهی، ساماندهی و مدیریت یکپارچه

Cite this article: L. Khouzestani¹ and A. Maroofnezhad² "The Evaluation of Desirability Information Security and Cyber Network Indicators in Ports with an Emphasis on Passive Defense (Case Study: Imam Khomeini Harbor)," *Electronic and Cyber Defense*, vol. 12, no. 4, pp. 27-37, . DOR: <https://dori.net/dor/> <https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.4.4.8>

© The Author(s).

Publisher: Imam Hossein University

*Corresponding Author Email: abbas.maroofnezhad@gmail.com



DOI: <http://doi.org/20.1001.1.23224347.1403.12.4.4.8>

پاسخ به این سؤال اصلی است که آیا می‌توان یک ارزیابی و رتبه‌بندی از شاخص‌های مطلوبیت امنیت اطلاعات و شبکه سایبری بندرها از منظر پدافند غیرعامل در مجتمع بندری امام خمینی (ره) به دست آورد؟ بر این اساس سایر بخش‌های این مقاله به شرح زیر سازمان‌دهی شده است. در بخش بعدی با مروری بر ادبیات و پیشینه پژوهش تهدیدهای امنیت اطلاعات و شبکه سایبری در بندرها احصاء خواهد شد. سپس روش -شناسی پژوهش و چارچوب پیشنهادی ارائه می‌شود. در ادامه، چارچوب پیشنهادی برای شناسایی و ارزیابی تهدیدهای امنیت اطلاعات و شبکه سایبری مطرح و سپس با نداشت مدل مفهومی پژوهش و آزمون این مدل، تأثیر شاخص‌های امنیت اطلاعات و شبکه سایبری بر بندرها موردسنجش قرار خواهد گرفت. در انتها به بحث و نتیجه‌گیری پیرامون یافته‌های پژوهش پرداخته می‌شود.

۲. مروری بر پیشینه پژوهش و چارچوب نظری

حوزه مطالعاتی امنیت اطلاعات و شبکه سایبری در بندرها با تأکید بر پدافند غیرعامل سابقه تاریخی طولانی‌مدتی نداشته و در طی سال‌های اخیر توجه پژوهشگران به‌ویژه داخل کشور را به خود جلب کرده است. از این‌رو تعداد پژوهش‌های داخلی و خارجی که به‌طور خاص به مطالعه، ارزیابی و رتبه‌بندی امنیت اطلاعات و شبکه سایبری در بندرها با تأکید بر پدافند غیرعامل پرداخته باشند بسیار محدود بوده که در ادامه به مهم‌ترین آن‌ها اشاره می‌شود.

رجبی و همکاران [۸] به بررسی و تحلیل چالش‌های امنیت سایبری در حوزه دریایی و کشتی‌های تجاری پرداخته است. نتایج پژوهش آن‌ها نشان داد که بخش دریایی، تاکنون به دلیل عدم اتصال به اینترنت و ماهیت منزوی کشتی‌ها در دریا ایمن تلقی می‌شد، اما با ورود به عصر دیجیتال شاهد افزایش ۹۰۰ درصدی نقض امنیت سایبری در فناوری عملیاتی هستیم. سیستم‌های فناوری اطلاعات و OT در کشتی‌های مدرن به دلیل آسیب‌پذیری زیاد در برابر تهدیدات سایبری باید با تدابیر امنیتی پیشرفته‌تری آماده شوند؛ مانند اجرای یک استاندارد امنیتی جدید که تعداد و دامنه حملات سایبری را کاهش می‌دهد. بچاری لفته و نجفی شوشتری [۹] به بررسی نقش امنیت سایبری در آینده حمل‌ونقل دریایی پرداخته است. نتایج پژوهش آن‌ها نشان داد که امنیت سایبر به‌عنوان مجموعه‌ای از ابزارها، روش‌ها، مسئولین امنیتی، روش‌های مدیریت ریسک، فرایندها، آموزش، تیم و فناوری‌ها است. همچنین فضای سایبری می‌تواند به‌عنوان دنیای الکترونیکی درک شود جایی که اطلاعات نرم‌افزارها و مردم به اشتراک گذاشته می‌شود و به‌صورت یکپارچه در دنیای فیزیکی و هم‌آمیخته شده‌اند. حملات سایبری مربوط به مسائل کامپیوتری در کشتی‌ها، بندرها و تمام تجهیزات

۱۱ هزار هکتار مساحت، بزرگ‌ترین منطقه ویژه اقتصادی کشور را تشکیل می‌دهد (شکل ۳). از مهم‌ترین ویژگی‌های بندرگاه امام خمینی (ره) می‌توان به موارد زیر اشاره کرد: ۱. نزدیک‌ترین بندر جنوبی به مراکز صنعتی و جمعیتی کشور. ۲. کوتاه‌ترین و مطمئن‌ترین پل ارتباطی با کشورهای عراق، ترکیه، حوزه قفقاز و اروپای شرقی. ۳. بهره‌مند از پتانسیل‌های مناسب پس‌کرانه‌ای جاده‌ای، ریلی و هوایی. ۴. اتصال به شبکه راه‌های اصلی ترانزیتی و راه‌آهن سراسری کشور. ۵. نزدیکی به فرودگاه‌های ماهشهر، آبادان و اهواز در فواصل ۱۸، ۱۰۰ و ۱۱۰ کیلومتری. ۶. مناسب‌ترین بندر کشور جهت ترانشیپ کالا به کشورهای حوزه خلیج فارس. ۷. برخورداری از پتانسیل‌های لازم به‌منظور توسعه صادرات مجدد کالا. ۸. نقش مؤثر در اقتصاد ملی و تجارت خارجی به‌عنوان دومین بندر مهم کشور. ۹. وجود ترمینال‌های اختصاصی، کانتینری، عمومی، فرآورده‌های نفتی و مواد معدنی. ۱۰. قابلیت تخلیه و بارگیری کشتی‌های کانتینری پست پاناماکس (نسل چهارم) و کشتی‌های با ظرفیت ۱۵۰ هزار تن. ۱۱. بهره‌مندی از تجهیزات پیشرفته بندری و دریایی به‌منظور ارائه خدمات سریع و ایمن به کشتی و کالا. ۱۲. برخورداری از سیستم تک پنجره^۱ به‌منظور ارائه خدمات متمرکز به مشتری. ۱۳. برخورداری از سیستم مدیریت یکپارچه (IMS^۲) و سیستم بین‌المللی امنیت اطلاعات (ISMS^۳). ۱۴. سیستم پرداخت الکترونیک از طریق سیستم (PSPOS^۴). ۱۵. برخورداری از سامانه هوشمند حواله‌ی الکترونیکی کامیون.



شکل (۱). نقشه مجتمع بندری (بندرگاه) امام خمینی (ره) برگرفته از: باکمی تغییر نویسندهگان، اقتباس از [۷]

با توجه به تأثیر تهدیدهای امنیت اطلاعات و چالش‌های شبکه‌های سایبری بر عملکرد بندرها، پژوهش حاضر درصدد

¹ Single Window

² Integrated Management System

³ International System Management Security

⁴ Payment Systems Point of Sale

خواسته‌های سیستم در زمینه ایمنی دارند که ابتدا بایستی ساختاری مناسب طرح -ریزی شده و برای قرار گرفتن افراد در چارچوب ساختاری موردنظر تغییر فرهنگ و تغییر رفتار توأمأ مورد استفاده قرار گیرند. آموزش افراد درگیر در ترمینال‌های بندری و به‌کارگیری دستورالعمل‌ها و آیین‌نام‌های بین‌المللی و تدوین کد ملی ایمنی در این خصوص ضروری است. خیری [۱۳] در مقاله‌ای با عنوان شناسایی، تحلیل و رتبه‌بندی عوامل موثرکلیدی در پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان بندرها و دریانوردی کشور پرداخته است. نتایج به‌دست‌آمده انجام سازمان مرکزی را متقاعد نمود تا نسبت به برگزاری دوره‌های آموزشی مرتبط و بازآموزی موضوع سیستم امنیت اطلاعات و برنامه‌ریزی و تخصیص رسانه و نرم‌افزار اقدام نماید.

آکپان و همکاران^۱ [۱۴] به چالش‌های امنیت سایبری در بخش دریایی می‌پردازند. در این زمینه، انواع حملات سایبری که کشتی‌ها می‌توانند با آن‌ها مواجه شوند، همراه با حوادث دنیای واقعی مورد بحث قرار می‌گیرد؛ که از حوادث سایبری متعدد گزارش شده و پیامدهای آن‌ها، شواهد روشنی وجود دارد که نشان می‌دهد هر کشتی یا حتی بندر در صورت عدم حفاظت کافی از سیستم‌های اطلاعات کلیدی در معرض خطر حملات سایبری قرار دارد؛ بنابراین، سیستم‌های فناوری اطلاعات و OT در کشتی‌های مدرن به دلیل آسیب‌پذیری زیاد در برابر تهدیدات سایبری باید با تدابیر امنیتی پیشرفته‌تری آماده شوند.

محبوب توشر و همکاران^۲ [۱۵] به ارزیابی ریسک امنیت سایبری در حمل و نقل خودگردان می‌پردازند. کشتی‌های خودمختار در مقایسه با عملیات حمل و نقل سنتی به تعامل فیزیکی-سایبری بالاتری نیاز دارند، بنابراین آسیب‌پذیری‌های مرتبط با امنیت سایبری افزایش می‌یابد. پیچیدگی فزاینده پیرامون ویژگی‌های ذاتی صنعت حمل و نقل، ایجاد یک چارچوب انعطاف‌پذیر برای تضمین امنیت سایبری را چالش برانگیز می‌کند. نتایج نشان می‌دهد که سیستم‌های ناوبری بیشترین آسیب‌پذیری را در برابر تهدیدات سایبری بالقوه دارند، در حالی که سیستم‌های پیشران کمترین آسیب‌پذیری را در زمینه عملیات کشتیرانی خودمختار آینده دارند. در سطح زیرسیستم، سه بخش آسیب‌پذیر عبارتند از: سامانه ماهواره‌ای ناوبری جهانی (GNSS^۳)، نمایشگر نمودار

کامپیوتری است که از عملیات دریایی پشتیبانی می‌کند. عباسی [۳] در مقاله‌ای با عنوان رتبه‌بندی مخاطرات مؤثر بر سامانه‌های مدیریت امنیت اطلاعات در اداره کل بندرها و دریانوردی استان خوزستان پرداخته است. نتایج پژوهش او نشان می‌دهد مخاطرات برخاسته از سامانه‌های کنترلی با وزن نسبی ۰/۴۵۳ در رتبه اول و به ترتیب مخاطرات بر خواسته از عوامل انسانی (مدیران ارشد، مشاورین و کارکنان) با وزن نسبی ۰/۳۳۸ در رتبه دوم و مخاطرات برخاسته از خط‌مشی‌ها و رویه‌ها با وزن نسبی ۰/۱۳۹ در رتبه سوم و در نهایت مخاطرات بر خواسته از سامانه‌های اطلاعاتی با وزن نسبی ۰/۷۰ در رتبه چهارم قرار گرفته‌اند. به نقل از خبرگزاری مانا [۱۰] در مقاله‌ای با عنوان نقش مدیریت زمان در شناسایی و مقابله با تهدیدات سایبری دریایی اشاره می‌کند، مالکان و صاحبان کشتی اغلب به خدمات خارج از کشتی برای محافظت از کشتی خود در مقابل حملات سایبری متکی هستند و چه‌بسا مسئولان IT آن شرکت و یا سازمان و یا شرکتی که تهدیدات سایبری را رصد می‌کند اطلاعات زیادی درباره سیستم نداشته باشند؛ در چنین شرایطی ممکن است این سیستم جواب ندهد. در این ارتباط باید شرکتی که برای مقابله با حملات سایبری همکاری می‌کند هم از نحوه ساخت سیستم و هم از فعالیت‌های مخرب دریایی شناخت لازم را داشته باشد. در واقع ارائه‌کنندگان خدمات امنیت سایبری خارج از کشتی باید در جریان امور و عملیات محوله شرکت‌های پشتیبانی‌کننده سیستم‌ها باشند. بنچاری و صفری [۱۱] در مقاله‌ای با عنوان موانع و راه‌کارهایی برای پیاده‌سازی سیستم مدیریت امنیت اطلاعات در اداره کل بندرها و دریانوردی استان بوشهر پرداخته‌اند. تجارت الکترونیک بدون تأمین امنیت اطلاعات معنایی ندارد. برای تأمین امنیت اطلاعات در یک سازمان فقط تأمین تجهیزات سخت‌افزاری و نرم‌افزاری کافی نیست بلکه لازم است فرآیندهای مرتبط با امنیت اطلاعات در سازمان نیز اصلاح شوند. به عبارت دیگر امنیت اطلاعات با فرآیند تأمین می‌شود و نه فقط با تجهیزات. سیستم مدیریت امنیت اطلاعات، سیستمی برای پیاده‌سازی کنترل‌های امنیتی است که با برقراری زیرساخت‌های مورد نیاز ایمنی اطلاعات را تضمین می‌نماید که با وجود تب شدید استفاده از مدیریت سیستم امنیت اطلاعات در سازمان بندرها و دریانوردی، هنوز چالش‌های مدیریتی و فنی در پیاده‌سازی این استاندارد وجود دارد. عدل و همکاران [۱۲] در مقاله‌ای با عنوان نقش مدیریت ایمنی در بندرها و سواحل کشور اشاره به وصول

¹ Akpan et al² Mahbub Tusher et al³ Global Navigation Satellite System

Cite this article: L. Khouzestani¹ and A. Maroofnezhad² "The Evaluation of Desirability Information Security and Cyber Network Indicators in Ports with an Emphasis on Passive Defense (Case Study: Imam Khomeini Harbor)," *Electronic and Cyber Defense*, vol. 12, no. 4, pp. 27-37, . DOR: <https://dorl.net/dor/> <https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.4.4.8>

© The Author(s).

Publisher: Imam Hossein University

*Corresponding Author Email: abbas.maroofnezhad@gmail.com

بندرها به عنوان یک مفهوم رویکردی پرداخته‌اند. نتایج نشان می‌دهد که صرف نظر از آگاهی روزافزون نسبت موضوع سایبری و امنیت اطلاعات، باید کارهای زیادی برای کاهش تهدیدات سایبری در بندرها انجام شود. از جمله موارد دیگر، اتخاذ استانداردهای صنعتی و هماهنگی در سطح عملی است. امنیت سایبری به طور کلی یک موضوع مفهومی بوده است، در حالی که در زمینه بندرها این موضوع تاکنون به ندرت مورد مطالعه قرار گرفته است. علاوه بر این، امنیت سایبری در حال حاضر در کنوانسیون‌های ایمنی و امنیت سازمان بین‌المللی دریانوردی مربوط به بندر، مانند ISPS^۷ یا ISM^۸ گنجانده نشده است. مقایسه نتایج ارزیابی‌ها در پژوهش حاضر بیانگر آن است که شاخص‌ها/گویه‌های انتخابی این پژوهش اهمیت زیادی در شناسایی و ارزیابی محدوده مورد مطالعه از منظر پدافند غیرعامل دارد و می‌تواند در روند پیشگیری و کنترل خسارات و صدمات تا حدود زیادی ایفای نقش داشته باشد. از سویی دیگر در ارزیابی شاخص‌ها به نسبت پژوهش‌های پیشین که کمتر مورد توجه واقع شده، این پژوهش بدان‌ها به دید عمیق‌تری نگاه کرده است. بر این اساس در این پژوهش سعی شده است با رویکردی کاربردی به اهمیت و ضرورت شناسایی و ارزیابی با استفاده از چهارده شاخص به سنجش مطلوبیت امنیت اطلاعات و شبکه سایبری بندرها با تأکید بر پدافند غیرعامل در محدوده مورد مطالعه پرداخته شود. چارچوب متدولوژیک پیشنهادی این پژوهش در شکل ۱، نشان داده شده است.



شکل (۲). چارچوب متدولوژیک پیشنهادی پژوهش

الکترونیکی و سیستم اطلاعات (ECDIS)^۹ و دستگاه‌های ارتباطی در مراکز کنترل ساحلی (SCC)^{۱۰}، به شمار می‌روند. بنا بر گزارش مجله سازمانی تکنولوژی^{۱۱} [۱۶] بندرها آمریکا سالانه حدود ۵/۴ تریلیون دلار کالا جابه‌جا می‌کنند که می‌تواند بهترین هدف منحصربه‌فرد برای مجرمان سایبری باشد. حفاظت از این مراکز حمل‌ونقل برای حفظ زنجیره تأمین و حفظ اقتصاد ایالات متحده ضروری است. به گفته پاسگان ساحلی ایالات متحده، بیش از ۵۰۰ حمله سایبری در سال ۲۰۲۰ در صنایع دریایی آمریکا رخ داده است. دلیل اصلی آن سیستم‌های سنتی فناوری اطلاعات بندری و هم سیستم‌های فناوری عملیاتی است؛ که شامل جرقه‌ها، دروازه‌ها، بالابرها و سیستم‌های حمل‌ونقل است که بار را به داخل و خارج از کشتی‌ها جابجا می‌کنند. چشم‌انداز خط‌مشی سایبری ایالات متحده در سال ۲۰۲۱ مسئولیت‌های خاصی را بیان می‌کند. پاسگان ساحلی ایالات متحده از چارچوب‌ها، استانداردها و بهترین شیوه‌ها در فعالیت‌های پیشگیری و واکنش برای شناسایی و مدیریت خطرات سایبری برای استفاده خواهد کرد. در داخل بندرها، کاپیتان‌های بندر پاسگان ساحلی ایالات متحده با ترویج مدیریت ریسک سایبری، مسئولیت‌پذیری و توسعه و اجرای طرح‌های واکنش یکپارچه، حکمرانی را رهبری خواهند کرد.

زارزولو^{۱۲} [۱۷] در مقاله‌ای با عنوان امنیت سایبری در صنعت بندرها و دریانوردی پرداخته است. امروزه یکی از عوامل اصلی تغییرات در بخش بندرها، تحولات شبکه اطلاعات است که بندرها هوشمند در حال تجربه آن هستند. سطح ادغام دستگاه‌ها، عوامل و فعالیت‌های مختلف، همراه با افزایش ارتباط بین بندرها مختلف دنیا، اکوسیستم جدیدی را ایجاد کرده است که بالطبع در آن خطرات جدیدی ظاهر شده است. امنیت سایبری یکی از چالش‌های صنعت است و سیاست‌گذاران باید در کنار بخش خصوصی کار کنند تا اطمینان حاصل شود که این زیرساخت‌های حیاتی به اندازه کافی محافظت می‌شوند و در عین حال توسعه کامل فناوری‌های جدید را در بخشی که نسبتاً در انتقال به دنیای جدید از سایرین عقب‌مانده است، تسهیل کنند. بویز و همکاران^{۱۳} [۱۸] با تهیه دستورالعمل شبکه سایبری و سیستم‌های اطلاعاتی برای بندرها و کشتیرانی به سفارش وزارت حمل‌ونقل انگلستان باهدف راهنمای الزامات امنیت سایبری در بندرها و تأسیسات بندری پرداخته‌اند. این دستورالعمل بر اساس استانداردهای امنیتی و الزامات مربوط به آن‌ها با ارائه راهنمایی‌های اضافی در مورد جنبه‌های مربوط به سایبری و اقدامات امنیتی تعیین شده است. آهوکاس و همکاران^{۱۴} [۱۹] به بررسی امنیت سایبری در

^۹ Electronic Chart Display and Information System

^{۱۰} Sea coast control

^{۱۱} Journal of Government Technology

^{۱۲} Zarzuelo

^{۱۳} Boyes et al

^{۱۴} Ahokas et al

^۷ International Ship and Port Security

^۸ International Safety Management

۳. روش‌شناسی پژوهش و چارچوب متدولوژیک پیشنهادی

پژوهش حاضر بر اساس هدف کاربردی و روش تحقیق، پیمایشی- ارزیابی با تأکید بر پرسشنامه است. جامعه آماری شامل کارکنان و کارشناسان خبره اداره بندر و برخی مسئولین نهادهای شهر بندر امام خمینی (ره) بوده که حجم نمونه تعیین شده ۱۰۰ نفر است. محدوده نمونه با استفاده از روش نمونه‌گیری تصادفی طبقه‌بندی شده انجام شده است. سپس بر اساس هر طبقه نمونه‌گیری لازم انجام گردید.^۱ در تحقیق حاضر با توجه به مشخص شدن حجم نمونه، ابتدا به تهیه پرسشنامه محقق ساخته اقدام شد. روش طراحی پرسشنامه در چهار مرحله انجام شد.

- مرحله اول، استخراج عوامل و شاخص‌ها از متون.
- مرحله دوم، ارائه شاخص‌ها به خبرگان و اضافه کردن عوامل جدید و استفاده از روش دلفی برای حاصل شدن اجماع نظری روی آن‌ها.
- مرحله سوم، نهایی سازی شاخص‌ها و ارائه به خبرگان جهت وزن دهی آن‌ها.
- مرحله چهارم، استخراج پرسشنامه محقق ساخته و ورود به بخش کمی که مشتمل بر تحلیل عاملی تأییدی و مقایسه میانگین بوده است.

پرسشنامه دارای بیست و یک سؤال بوده که به دو قسمت تقسیم شده است. قسمت اول اطلاعات جمعیت‌شناسی با شش سؤال و قسمت دوم پانزده سؤال مربوط به شاخص‌های ارزیابی امنیت اطلاعات و شبکه سایبری بندرها با تأکید بر پدافند غیرعامل (جدول ۱) بوده است. به جهت اعتبار یابی این شاخص‌ها ابتدا برای روایی پرسشنامه‌های مربوط اقدام و پس از مطالعات اسنادی و میدانی (نظرسنجی از کارشناسان، متخصصین و... در قالب روش دلفی) توسط ۱۳ نفر از اساتید دانشگاه و مدیریت امور نظامی و کارشناسان مرتبط تأیید گردید. در تعیین پایایی پرسشنامه‌ها نیز پس از جمع‌آوری تعداد سی نفر از پرسش‌شوندگان، از طریق روش دلفی

^۱ برای توزیع پرسشنامه‌ها ملاک جمعیت مطلع و آگاه به موضوع پدافند غیرعامل بوده است که بر این اساس دسته‌بندی لازم انجام گردید (به دودسته: کارکنان و کارشناسان خبره و مرتبط مجتمع بندری و مسئولین نهادهای شهری بندر امام) که به ترتیب: ۷۵ درصد و ۲۵ درصد پرسشنامه‌ها اختصاص داده شد.

نسبت به پایایی پرسشنامه‌های جمع‌آوری شده اقدام و ضریب آلفای آن تعیین گردید؛ که نتایج حاکی از آن بود که پرسشنامه‌های توزیعی و سازه‌های تعیین شده دارای پایایی مناسب در عوامل یادشده است (بارزش عددی ۰/۸۳، جدول ۲). سپس با استفاده از پرسشنامه محقق ساخته که حاوی مقیاس پنج‌درجه‌ای لیکرت از بسیار ضعیف تا بسیار خوب با امتیازهای یک تا پنج اقدام گردید. پس از سنجش روایی و پایایی، پرسشنامه مذکور، به‌صورت حضوری توسط محقق به تعداد حجم نمونه (۱۰۰ نفر) به هر یک از کارشناسان خبره و... محدوده مورد مطالعه تحویل داده شد و ضمن توضیحات لازم در خصوص اهمیت دقت در پاسخ‌دهی به پرسش‌ها از آنان درخواست شد نظر خود را نسبت به هر یک از شاخص‌های تعیین شده برای ارزیابی موضوع تحقیق اعلام نمایند. برای تحلیل داده‌های جمع‌آوری شده از آمار توصیفی و استنباطی استفاده شد. در بخش آمار توصیفی از فراوانی، درصد فراوانی، میانگین و... در بخش آمار استنباطی محاسبه میزان اهمیت یا رضایت و یا وجود هر ویژگی متغیرها استفاده شد. با توجه به آن‌که میانگین امتیاز هر پرسش عددی بین (۱) تا (۵) بود. این معیار برای سنجش اهمیت پرسش‌ها یا گزینه‌ها مورد استفاده قرار گرفته. سپس بر اساس نتایج به‌دست آمده از پرسشنامه و مشاهدات میدانی به تحلیل یافته‌ها با استفاده از نرم‌افزارهای SPSS^۲ پرداخته شد. بدین منظور در نرم‌افزار فوق برای نرمال بودن توزیع داده‌ها و وضعیت مؤلفه‌های پژوهش از آزمون‌های: کلموگروف-اسمیرنوف^۳ و بارتلت^۴ و KMO^۵ و آزمون فریدمن^۶ استفاده شده است.

جدول (۱). شاخص‌های موردسنجش در پژوهش

شاخص	کد	مآخذ
۱. توجه به اهمیت افراد در شغل‌های حساس	C1	نویسندگان
۲. نظارت و توجه به دسترسی نداشتن افراد غیرمستول در حیطه‌بندی اسناد و مدارک فنی	C2	نویسندگان
۳. آموزش تخصصی مناسب و مداوم کارکنان به‌ویژه در بخش‌های حساس در طول سال	C3	نویسندگان
۴. ناحیه بندی و حیطه‌بندی امنیتی (مثلاً) کنترل شده به بخش‌های مختلف یا غیر کنترل شده و آزاد	C4	نویسندگان

^۲ Statistical Package for the Social Sciences

^۳ Kolmogorov-Smirnov

^۴ Bartlett

^۵ Kaiser-Mayer-Olkin

^۶ Feridman

Cite this article: L. Khouzestani¹ and A. Maroofnezhad² "The Evaluation of Desirability Information Security and Cyber Network Indicators in Ports with an Emphasis on Passive Defense (Case Study: Imam Khomeini Harbor)," *Electronic and Cyber Defense*, vol. 12, no. 4, pp. 27-37, . DOR: <https://dorl.net/dor/> <https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.4.4.8>

© The Author(s).

Publisher: Imam Hossein University

*Corresponding Author Email: abbas.maroofnezhad@gmail.com



C2	۰/۸۷	C10	۰/۸۳
C3	۰/۷۹	C11	۰/۸۵
C4	۰/۸۸	C12	۰/۸۷
C5	۰/۸۰	C13	۰/۸۴
C6	۰/۸۱	C14	۰/۸۹
C7	۰/۷۸	C15	۰/۸۱
C8	۰/۸۲	T.A	۰/۸۳

۴. یافته‌ها و نتایج

بدیهی است با افزایش درجه اهمیت یک موضوع و منطقه برای کشور، ضرایب ایمنی، امنیتی آن نیز افزایش می‌یابد و چگونگی تداوم فعالیت بندرها و سواحل در حوزه‌های تجاری و ارتباطی را در شرایط بحرانی ناشی از تهدیدات دشمن نیز موردبررسی قرار داده و با بهره‌گیری از تدابیر و تمهیدات ویژه پدافند غیرعامل، ضرایب ایمنی، امنیتی و دفاعی بندرها و سواحل را برای تداوم فعالیت‌ها در زمان‌های صلح و جنگ افزایش دهد. دامنه این تدابیر و تمهیدات از جزئی‌ترین عناصر، تجهیزات و سازه‌های بندر تا راهبردی‌ترین موضوعات کشور در ارتباط با مدیریت، آمایش سرزمین و مسائل مربوط به تجارت و اقتصاد گسترده است. زمینه‌های مختلف مقابله با تهدیدات دشمن که می‌تواند از جنگ اقتصادی، تهدید تجارت، تهدید ناوگان‌های تجاری، جنگ الکترونیک، حملات تخریبی و درنهایت اقدام به تخریب برخی از سواحل و بندرها و یا حتی تسخیر گسترده باشد؛ بسیار متنوع و هوشمندانه و کارآمد هستند. حوزه‌های فنی و مهندسی ساخت بندرها، تجهیزات، سازه‌های دریایی و ساختمان‌های فعالیتی، اقلیم‌شناسی، جغرافیا، مکان‌یابی بندرها و آبراهه‌ها، آمایش سرزمین و سواحل و بسیاری از مسائل دیگر در این خصوص موردتوجه قرار خواهند گرفت. با به‌کارگیری تمهیدات پدافند غیرعامل و بهره‌گیری از تدابیر و توصیه‌های آن در زمینه‌های مختلف، علاوه بر تداوم فعالیت‌ها و افزایش ضرایب دفاعی و امنیتی در برابر تهدیدات دشمن؛ قطعاً ضرایب ایمنی در برابر انواع حوادث و سوانح طبیعی، فنی و مهندسی و خطاهای انسانی نیز افزایش یافته و صرفه‌جویی‌های ناشی از تجمع در شیوه‌های ایمنی به وجود خواهد آمد و بندرها و سواحل ایمن‌تر، امن‌تر و قابل دفاع‌تر خواهند شد. در ادامه پژوهش بر اساس یافته‌های توصیفی از مجموع ۱۰۰ پرسشنامه توزیع‌شده در بین نمونه‌های انتخاب‌شده پژوهش، اطلاعات به‌دست‌آمده به شرح جدول ۳، نشان داده‌شده است.

جدول (۳). درصد/ فراوانی پاسخ به سؤالات توصیفی پژوهش

۵. اقدامات حفاظتی برای مراکز الکترونیک (مثلاً کابل‌های پاور، مراکز دیتا و مخابرات در مقابل تهدیدات (سلاح‌های الکترومغناطیس و...)	C5	[۲۰]
۶. حفاظت سایبری توسط افراد متخصص از دیتاسنترها و دیتا بیس‌ها	C6	[۲۰]
۷. جانمایی دیتاسنترها و دیتابیسیس‌ها از نظر نزدیکی یا مجاورت به مراکز خطرزا (مثلاً اماکن مستعد برای اشتعال یا انفجار یا نفوذ باد و آب و...)	C7	[۲۰]
۸. سیستم‌های تهویه و سرمایشی مناسب و مطلوب برای حفاظت و نگهداری دیتاسنترها و...	C8	[۲۰]
۹. حفاظت و نگهداری از منابع سخت‌افزاری سرورها (رم‌ها، هارددیسک‌ها و...) به‌ویژه سیستم‌های مرتبط با ناوبری و هدایت-کنترل و مدیریت کشتی‌های خارجی و داخلی	C9	[۲۰]
۱۰. پشتیبان‌گیری به‌موقع (Backup) از مراکز دیتاسنتر و سرورها و...	C10	[۲۰]
۱۱. استفاده از نرم‌افزارهای مقابله‌کننده با بدافزارها و لایه‌های حفاظتی برای جلوگیری از ورود ویروس‌ها به سیستم‌ها و سرورهای مراکز دیتا بندر	C11	[۲۰]
۱۲. استفاده از یوپی‌اس (UPS) در مراکز دیتا و سرورها و سایر سیستم‌های الکترونیکی حساس	C12	[۲۰]
۱۳. وجود نیروهای متخصص و واکنش سریع و اضطراری در مقابل حوادث ناگهانی و بحرانی در برابر حملات سایبری رایانه‌ای و هکری در بندر	C13	[۲۱]

جدول (۱). شاخص‌های موردسنجش در پژوهش

۱۴. ناحیه بندی و سطح‌بندی حفاظتی در استفاده از سامانه‌ها و شبکه‌های فناوری اطلاعات و ارتباطات (مثلاً ورود به نقاط حساس شبکه‌ها و رایانه‌ها و...)	C14	[۲۱]
۱۵. برگزاری مانورها و دوره‌های آموزشی کارکنان جهت شناسایی حفره‌های امنیتی شبکه، سامانه و سایر مراکز رایانه‌ای در طول سال	C15	[۲۱]

برگرفته از: نویسندگان (۱۴۰۱)، با اقتباس از [۲۱، ۲۰]

جدول (۲). میزان پایایی سازه‌های استنباطی تحقیق

کد	میزان آلفا	کد	میزان آلفا
C1	۰/۸۳	C9	۰/۷۸

جدول (۵). نتایج آزمون KMO و بار تلت برای عامل پژوهش

میزان آشنایی	جنسیت (تعداد/ درصد)	میزان تحصیلات (تعداد/درصد)	میزان پژوهش (پدافند غیرعامل) (تعداد/درصد)	میزان پژوهش (پدافند غیرعامل) (تعداد/درصد)	میزان پژوهش (پدافند غیرعامل) (تعداد/درصد)	میزان پژوهش (پدافند غیرعامل) (تعداد/درصد)
امنیت اطلاعات و شبکه سایبری	۰/۸۷۹	۹۱۰/۲۵	۱۰۵	۰/۰۰۰		

با توجه به نتایج جدول ۵، اندازه کفایت نمونه به دست آمده برای مؤلفه پژوهش (امنیت اطلاعات و شبکه سایبری) بزرگتر از ۰/۷ است. همچنین مقدار سطح معناداری آزمون محاسبه شده برای مؤلفه پژوهش کمتر از ۰/۰۵ شده است؛ بنابراین می توان نتیجه گرفت که این نتایج حاکی از کفایت نمونه است. با توجه به عدم نرمال بودن متغیرها برای تأیید مدل و پاسخ به پرسش پژوهش از مدل یابی معادلات ساختاری به روش حداقل مربعات جزئی^۱ (PLS) با استفاده از نرم افزار SMARTPLS استفاده شده است (جدول ۶).

روش تخمین PLS ضرایب را به گونه ای تعیین می کند که مدل حاصله، بیشترین قدرت تفسیر و توضیح را دارا باشد؛ بدین معنا که مدل بتواند با بالاترین دقت و صحت، متغیر وابسته نهایی را پیش بینی نماید. روش حداقل مربعات جزئی که در بحث الگو - سازی رگرسیونی آن را با^۱ PLS نیز معرفی می کنند، یکی از روش های آماری چند متغیره محسوب می شود که به وسیله آن می توان علیرغم برخی محدودیت ها مانند نامعلوم بودن توزیع متغیر پاسخ، وجود تعداد مشاهدات کم و یا وجود خودهمبستگی جدی بین متغیرهای مستقل؛ یک یا چند متغیر پاسخ را به طور هم زمان در قبال چندین متغیر مستقل الگوسازی نمود [۲۲].

جدول (۶). نتایج حاصل از یافته های تحلیل عاملی تأییدی

عامل	t-value	ضریب استاندارد	R ²
امنیت اطلاعات و شبکه سایبری	۱۰/۹۱۱	۰/۷۳۷	۰/۵۴۳

میزان آشنایی	جنسیت (تعداد/ درصد)	میزان تحصیلات (تعداد/درصد)	میزان پژوهش (پدافند غیرعامل) (تعداد/درصد)	میزان پژوهش (پدافند غیرعامل) (تعداد/درصد)	میزان پژوهش (پدافند غیرعامل) (تعداد/درصد)	میزان پژوهش (پدافند غیرعامل) (تعداد/درصد)
امنیت اطلاعات و شبکه سایبری	۰/۸۷۹	۹۱۰/۲۵	۱۰۵	۰/۰۰۰		

بر اساس یافته های توصیفی اشاره شده در جدول ۴، ۷۹ درصد پاسخ دهندگان مرد و ۲۱ درصد زن؛ و میزان آشنایی پاسخ دهندگان به موضوع پدافند غیرعامل، ۳ درصد متوسط و ۹۷ درصد زیاد بوده است. به لحاظ تحصیلات، ۵۴ درصد تحصیلات لیسانس، ۳۵ درصد فوق لیسانس، ۴ درصد دانشجوی دکتری و ۷ درصد دکتری تخصصی داشته اند. برای بررسی پرسش مطرح شده در پژوهش و به منظور سنجش نرمال بودن توزیع داده ها از آزمون کلموگروف-اسمیرنوف استفاده شد؛ که در جدول ۴، نشان داده شده است.

جدول (۴). نتایج آزمون کلموگروف اسمیرنوف

عامل پژوهش	اسمیرنوف Z (آماره کلموگروف)	Sig (سطح معناداری)	تعداد نمونه	نتیجه نرمالیتی
امنیت اطلاعات و شبکه سایبری	۰/۱۸۴	۰/۰۰۰	۱۰۰	نرمال نیست

نتایج به دست آمده از جدول ۴، نشان می دهد مقدار سطح معنی داری در مؤلفه امنیت اطلاعات و شبکه سایبری از مقدار خطای ۰/۰۵ کمتر است، پس فرض صفر رد می شود و این مؤلفه نرمال نیست. با توجه به نتایج جدول ۴، برای محاسبه اندازه کفایت نمونه مؤلفه امنیت اطلاعات و شبکه سایبری در پژوهش و همچنین مقدار سطح معناداری، از آزمون KMO و آزمون بار تلت استفاده گردید؛ که در جدول ۵، نشان داده شده است.

^۱Partial Least Square

Cite this article: L. Khouzestani¹ and A. Maroofnezhad² "The Evaluation of Desirability Information Security and Cyber Network Indicators in Ports with an Emphasis on Passive Defense (Case Study: Imam Khomeini Harbor)," *Electronic and Cyber Defense*, vol.12 , no.4 , pp.27-37 , . DOR: <https://dorl.net/dor/> <https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.4.4.8>

© The Author(s).

Publisher: Imam Hossein University

*Corresponding Author Email: abbas.maroofnezhad@gmail.com



ندارد و میانه‌های تمامی متغیرهای مورد آزمون برابر است. چنانچه مؤلفه p - مقدار از سطح خطا کمتر باشد، در آن صورت، فرض H_0 رد می‌شود و گرنه دلیلی بر رد این فرض وجود ندارد (جدول ۷).

جدول (۷). نتایج آزمون فریدمن بر روی مؤلفه امنیت اطلاعات و

شبکه سایبری

تعداد	درجه آزادی	مقدار آماره χ^2	P- مقدار
۱۰۰	۴	۲/۹۴۴	۰/۵۶۷

مطابق آزمون فریدمن میانگین رتبه‌ی هر یک از شاخص‌های امنیت اطلاعات و شبکه سایبری محاسبه شده است (شکل ۳) که با توجه به این نتایج، بالاترین میانگین رتبه مربوط شاخص، سیستم‌های تهویه و سرمایشی مناسب و مطلوب برای حفاظت و نگهداری دیتاسنترها و... با میانگین رتبه ۳/۸۰ در جایگاه اول و شاخص آموزش تخصصی مناسب و مداوم کارکنان به‌ویژه در بخش‌های حساس در طول سال با میانگین رتبه ۳/۶۰ در جایگاه پانزدهم (آخر) قرار گرفته‌اند؛ بنابراین با توجه به نتایج رتبه‌بندی شاخص‌ها، می‌توان اذعان داشت وضعیت کلی میزان آسیب‌پذیری امنیت اطلاعات و شبکه سایبری در سطح مجتمع بندری امام خمینی (ره) بالاست و توجه و افزایش و اهمیت به ضریب‌های حفاظتی و امنیتی با رعایت دستورالعمل‌های پدافند غیرعامل می‌تواند در جلوگیری از بروز خطرات احتمالی کارساز باشد.

جدول (۸). میانگین رتبه شاخص‌های امنیت اطلاعات و شبکه سایبری مجتمع بندری امام خمینی (ره) از منظر پدافند غیرعامل به‌وسیله آزمون

فریدمن

کد	متغیر	میانگین رتبه
C1	حفاظت از عدم به‌کارگیری افراد در شغل‌های حساس	۳/۷۱
C2	نظارت بر دسترسی نداشتن افراد غیرمسئول به دستورالعمل‌های طبقه‌بندی و حیطه‌بندی اسناد و مدارک فنی	۳/۶۹
C3	آموزش تخصصی مناسب و مداوم کارکنان به‌ویژه در بخش‌های حساس در طول سال	۳/۶۰
C4	ناحیه بندی و حیطه‌بندی امنیتی (مثلاً کنترل شده به بخش‌های مختلف یا غیر کنترل شده و آزاد)	۳/۶۳
C5	اقدامات حفاظتی برای مراکز الکترونیک (مثلاً کابل‌های پاور، مراکز دیتا و مخابرات در مقابل تهدیدات (سلاح‌های الکترومغناطیس و...)	۳/۷۶
C6	حفاظت سایبری توسط افراد متخصص از دیتاسنترها و دیتا بیس‌ها	۳/۶۸
C7	جانمایی دیتاسنترها و دیتابیس‌ها از نظر نزدیکی یا مجاورت به مراکز خطرزا (مثلاً اماکن مستعد برای اشتعال یا انفجار یا نفوذ باد و آب و...)	۳/۷۲
C8	سیستم‌های تهویه و سرمایشی مناسب و مطلوب برای حفاظت و نگهداری دیتاسنترها	۳/۸۰

و...

در جدول ۶، بار عاملی و عدد معناداری مربوط به شاخص پژوهش نشان می‌دهد عامل امنیت اطلاعات و شبکه سایبری با ضریب $0/737$ میزان تأثیرگذاری بالایی دارد. همچنین مقادیر R^2 نشان‌دهنده میزان تبیین پدافند غیرعامل توسط شاخص پژوهش است.

۴-۱. آزمون فریدمن

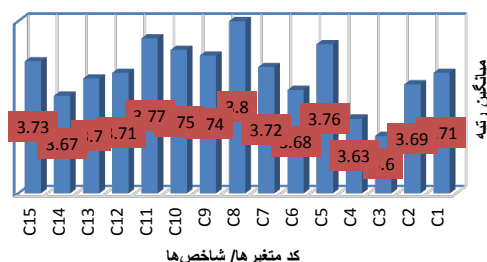
این آزمون برای مسائل مربوط به طرح‌های با اندازه‌های تکراری قابل استفاده است. در طرح‌های با اندازه‌های تکراری، هر آزمودنی یک رکورد از پرونده داده‌ها است که دارای k متغیر است. نمرات حاصله از k موقعیت یا فرصت در این متغیرها وارد می‌شود. محقق علاقه‌مند به تعیین تغییرات معنی‌دار آزمودنی‌ها در تمام موقعیت‌ها یا فرصت‌های مورد اشاره است. به این منظور، آزمون فریدمن به مقایسه میانه‌های متغیرها می‌پردازد و معنی‌دار بودن این تفاوت‌ها را بررسی می‌کند. در این آزمون، یافته‌های متغیرها در هریک از رکوردها، رتبه گذاری می‌شود و با استفاده از میانگین رتبه‌های متغیرها در نمونه، فرض برابری میانه‌های متغیرها مورد آزمون قرار می‌گیرد.

$$X_{1-\alpha}^2(n-1) \quad (1)$$

درباره n متغیر مورد بررسی، اگر مقدار آماره χ^2 به‌دست آمده بزرگ‌تر از α (اندازه خطای آزمون) و $n-1$ (درجه آزادی) باشد، آنگاه فرض H_0 مبنی بر برابری میانه‌ها رد می‌شود، یعنی حداقل یک متغیر وجود دارد که میانه آن تفاوت معنی‌داری با یکی دیگر از متغیرهای مورد آزمون دارد و گرنه دلیلی بر رد فرض H_0 وجود

۳/۷۴	حفاظت و نگهداری از منابع سخت‌افزاری سرورها (رم‌ها، هارددیسک‌ها و...) به‌ویژه سیستم‌های مرتبط با ناوبری و هدایت-کنترل و مدیریت کشتی‌های خارجی و داخلی	C9
۳/۷۵	پشتیبان‌گیری به‌موقع (Backup) از مراکز دیتاسنتر و سرورها و...	C10
۳/۷۷	استفاده از نرم‌افزارهای مقابله‌کننده با بدافزارها و لایه‌های حفاظتی برای جلوگیری از ورود ویروس‌ها به سیستم‌ها و سرورهای مراکز دیتا بندر	C11
۳/۷۱	استفاده از یوپی‌اس (UPS) در مراکز دیتا و سرورها و سایر سیستم‌های الکترونیکی حساس	C12
۳/۷۰	وجود نیروهای متخصص و واکنش سریع و اضطراری در مقابل حوادث ناگهانی و بحرانی در برابر حملات سایبری رایانه‌ای و هکری در بندر	C13
۳/۶۷	ناحیه بندی و سطح‌بندی حفاظتی در استفاده از سامانه‌ها و شبکه‌های فناوری اطلاعات و ارتباطات (مثلاً ورود به نقاط حساس شبکه‌ها و رایانه‌ها و...)	C14
۳/۷۳	برگزاری مانورها و دوره‌های آموزشی کارکنان جهت شناسایی حفره‌های امنیتی شبکه، سامانه و سایر مراکز رایانه‌ای در طول سال	C15

مجتمع بندری امام خمینی (ره) از منظر پدافند غیرعامل با استفاده از پانزده شاخص شناسایی و انتخاب‌شده پژوهش بوده است. نتایج حاصل از این پژوهش نشان داد اندازه کفایت نمونه به‌دست‌آمده برای هر یک از متغیرهای پژوهش بزرگ‌تر از ۰/۷ شده است؛ و مقدار سطح معنا-داری آزمون محاسبه‌شده برای تمامی متغیرهای پژوهش کمتر از ۰/۰۵ است که نتایج حاکی از کفایت نمونه‌ها برای انجام تحلیل عاملی تأییدی بوده است. همچنین عامل امنیت اطلاعات و شبکه سایبری با ضریب ۰/۷۳۷ میزان تأثیرگذاری بالایی را نشان داده و مقادیر R^2 نشان‌دهنده میزان تبیین پدافند غیرعامل توسط شاخص پژوهش بوده است. با توجه به نتایج آزمون فریدمن برای محاسبه رتبه‌بندی پانزده شاخص امنیت اطلاعات و شبکه سایبری این نتایج نشان داد، بالاترین میانگین رتبه مربوط متغیر سیستم‌های تهویه و ... با میانگین رتبه ۳/۸۰ در جایگاه اول و متغیر آموزش تخصصی مناسب و مداوم کارکنان به‌ویژه در بخش‌های حساس در طول سال با میانگین رتبه ۳/۶۰ در جایگاه پانزدهم (آخر) قرار گرفته‌اند. اهمیت و ضرورت انجام این تحقیق نشانگر این موضوع است که قابلیت تأثیرگذاری هریک از متغیرهای پژوهش در محدوده مورد مطالعه از نظر ظرفیت و نظارت، متفاوت می‌باشند. از سویی دیگر در ارزیابی این متغیرها به نسبت پژوهش‌های پیشین که کمتر مورد توجه واقع شده، این پژوهش بدان‌ها به دید عمیق‌تری نگاه کرده است. در بحث شاخص امنیت اطلاعات و شبکه سایبری



شکل (۳). نمودار رتبه‌بندی شاخص‌های امنیت اطلاعات و شبکه سایبری در مجتمع بندری امام خمینی (ره) به‌وسیله آزمون فریدمن

۵. نتیجه‌گیری

حوزه‌های فنی و مهندسی ساخت بندرها، سازه‌های دریایی و حوزه و تجهیزات الکترونیک و سیستم اطلاعات شبکه و بسیاری از مسائل دیگر در این خصوص مورد توجه قرار خواهند گرفت. با به‌کارگیری تمهیدات پدافند غیر-عامل و بهره‌گیری از تدابیر و توصیه‌های آن در زمینه‌های مختلف، علاوه بر تداوم فعالیت‌ها و افزایش ضرایب دفاعی و امنیتی در برابر تهدیدات دشمن؛ قطعاً ضرایب ایمنی در برابر انواع حوادث و سوانح طبیعی، فنی و مهندسی و خطاهای انسانی نیز افزایش یافته و صرفه‌جویی‌های ناشی از تجمع در شیوه‌های ایمنی به وجود خواهد آمد و بندرها و سواحل ایمن‌تر، امن‌تر و قابل دفاع‌تر خواهیم داشت. آنچه در پژوهش حاضر به‌عنوان هدف اشاره شد، سنجش و رتبه‌بندی مطلوبیت شاخص‌های امنیت اطلاعات و شبکه سایبری در

Cite this article: L. Khouzestani¹ and A. Maroofnezhad² "The Evaluation of Desirability Information Security and Cyber Network Indicators in Ports with an Emphasis on Passive Defense (Case Study: Imam Khomeini Harbor)," *Electronic and Cyber Defense*, vol. 12, no. 4, pp. 27-37, . DOR: <https://dorl.net/dor/> <https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.4.4.8>

© The Author(s).

Publisher: Imam Hossein University

*Corresponding Author Email: abbas.maroofnezhad@gmail.com



- [7] "The site of the General Administration of Ports and Maritime Affairs of Imam Khomeini Port, (In Persian)," 2022.
- [8] H. Rajabi, M. Ghasemi, and M. Dehghani, "Investigation and analysis of cyber security challenges in maritime and commercial ships," *Journal of Maritime Police Security*, vol. 14, no. 52, pp. 23-39. (In Persian), 2023.
- [9] M. R. Bechari and S. M. Lefte Shoushtari, "Examining the role of cyber security in the future of maritime transport," presented at the The second international conference on electrical engineering, computer science and information technology, Hamedan, 2017.
- [10] M. n. agency, "'The role of time management in identifying and countering maritime cyber threats,'" The first independent information network of the maritime community," vol. News code 94963, (In Persian), ed, 2023.
- [11] H. Banchari and I. Safari, "Obstacles and solutions for implementing information security management system (ISMS) in Bushehr Ports and Maritime Administration," presented at the International Science and Engineering Congress, Tehran, 2016.
- [12] M. A. Adel, M. Mubasher Amini, and M. Saibani, "The role of safety management in ports and coasts of the country," presented at the 9th Maritime Industry Conference, Mazandaran, 2016.
- [13] S. Khairi, "Identification, analysis and ranking of key effective factors in the implementation of information management system in government organizations (case study: Ports and Shipping Organization)," *Ports and Maritime Organization*, vol. 2, no. 3, pp. 36-46 (In Persian), 2015.
- [14] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, "Cybersecurity Challenges in the Maritime Sector," *MDPI Journal*, vol. 2, no. 1, pp. 123-138, 2022.
- [15] H. Mahbub Tusher, Z. Haque Munim, T. E. Notteboom, T. Eun Kim, and S. Nazir, "Cyber security risk assessment in autonomous shipping," *Maritime Economics & Logistics Journal*, vol. 24, pp. 208-227, 2022.
- [16] G. C. Kessler and S. D. Shepard, *Maritime cybersecurity: a guide for leaders and managers*. Gary C. Kessler and Steven D. Shepard, 2020.
- [17] I. P. Zarzuelo, "Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue," *Transport Policy Journal*, vol. 100, pp. 1-4, 2021.
- [18] H. Boyes, R. Isbell, and A. Luck, *Cyber Security for ports and port Systems*. Institution of Engineering and Technology. London: United Kingdom (IET), 2020, p. 71.
- [19] J. Ahokas, T. Kiiski, J. Malmsten, and L. M. Ojala, *Cybersecurity in ports: A conceptual approach*. epubli GmbH. Berlin, 2017, pp. 343-359.

پیشنهادهایی که می‌توان با لحاظ کردن شاخص‌های انتخابی پژوهش مطرح شود:

۱. توجه و تقویت امنیت لجستیک دریایی به‌ویژه در آینده پیشرو. زیرابه گفته محققین تا سال ۲۰۳۵ لجستیک دریایی تحت سلطه سیستم‌های رایانه‌ای قرار خواهد گرفت؛ بنابراین مهارت در علم محاسبات ریاضی به شکل متوالی از ماشین و نرم‌افزار پیچیده مشتق خواهد شد. مثلاً تمام سیستم‌های رایانه‌ای، لجستیک دریایی در سال ۲۰۳۵ از اطلاعات، فناوری و مردم تشکیل خواهد شد.

۲. تنظیم دستورالعمل‌های ایمنی و برگزاری دوره‌های آموزشی اولیه و ادواری به‌منظور به حداقل رساندن خطاهای انسانی.

۳. ایجاد سازمان پدافند غیرعامل دریایی باهدف جهش امنیت پایدار دریایی.

۶. مراجع

- [1] K. Shoshian and A. Mirghadri, "Modeling of Obfuscated Multi- Stage cyber Attacks," *Scientific Journal Electronic and cyber defense*, vol. 8, no. 2, pp. 61-73 (In Persian), 2020. <https://dor.isc.ac/dor/20.1001.1.23224347.1399.8.2.6.8>
- [2] M. Jafarzadeh and J. Bigi, "A comparative study of pre-emptive and preventive defense from the perspective of international law with an emphasis on the September 11 attacks," presented at the First International Comprehensive Law Congress, Allameh Tabatabaie University, Tehran, 2014.
- [3] S. Abbasi, "Effective risk ranking of information security management systems(case study:Will of all ports and shipping in Khuzestan province)," *Quarterly of the maritime transport industry*, vol. 5, no. 3, pp. 4-13 (In Persian), 2018.
- [4] H. M. Razmi and M. Gholami, "Analyzing the principles and guidelines of school architecture design from the point of view of passive defense," *Architecture Quarterly*, vol. 3, no. 17, pp. 1-16 (In Persian), 2019.
- [5] K. Afradi and R. Khajeh Ali, "Definition of the design and planning framework of the port-coastal cities according to the non-active defense strategy," *Oceanographic Quarterly*, vol. 5, no. 20, pp. 137-143 (In Persian), 2013. <https://dor.isc.ac/dor/20.1001.1.15621057.1393.5.20.14.9>
- [6] H. A. Sayari and M. Mansour Dehghan, "Designing a strategic model of passive defense of ports in the south of the country with an emphasis on sea-based threats," *Strategic Defense Studies Quarterly*, vol. 17, no. 65, pp. 49-70 (In Persian), 2015.

Cite this article: L. Khouzestani and A. Maroofnezhad "The Evaluation of Desirability Information Security and Cyber Network Indicators in Ports with an Emphasis on Passive Defense (Case Study: Imam Khomeini Harbor)," *Electronic and Cyber Defense*, vol. 12, no. 4, pp. 27-37, . DOR: <https://dori.net/dor/> <https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.4.4.8>

© The Author(s).

Publisher: Imam Hossein University

*Corresponding Author Email: abbas.maroofnezhad@gmail.com



- Maritime Affairs of Khuzestan Province - Imam Khomeini Port, 2022. (In Persian) .
- [22] A. Azar, R. Gholamzadeh, and M. Ghanawati, Path-structural modeling in Smart PLS software application management, First edition ed. Tehran Negah Danesh Publications, 2011, p. 280.
- [20] G. Javadpur, M. MansourDehghan, and A. Naghizadeh, Defense Passive And Crisis Management In Ports, First Edition ed. Publications of Ports and Maritime Organization, 2018.
- [21] Guidelines and checklists of the management department HSE General Directorate of Ports and
- [23]