Development of a Strategic Human Capital Management Framework for Cybersecurity Defense in the Gas Industry

Amin Monazami Motlagh[1] - Abdolrahman Keshvari[2]

Abstract

This study aims to develop a strategic human capital management framework for cybersecurity defense in the gas industry. Given the significant increase in cyber attacks on critical infrastructure, developing a comprehensive framework for managing specialized human resources in this field is an undeniable necessity. This research is applied-developmental in terms of purpose and uses a mixed-methods approach (qualitative-quantitative) in terms of methodology. In the qualitative phase, the main dimensions and components of the framework were identified using thematic analysis and semi-structured interviews with 18 experts. In the quantitative phase, a researcher-developed questionnaire with 72 items was distributed among 196 cybersecurity specialists and managers in the gas industry. Data analysis was performed using structural equation modeling and SPSS and SmartPLS software. Findings showed that the final framework includes 6 main dimensions (specialized skill development strategies, cyber talent management, cybersecurity culture, agile organizational structure, cyber governance, and cybersecurity defense knowledge management), 15 components, and 54 indicators. Path analysis results showed that there is a significant relationship between the six dimensions of the framework and strategic human capital management ($P<0.01$). The most important finding of the research emphasizes the pivotal role of specialized skill enhancement and cybersecurity culture development components in creating efficient

1. Phd Student, Strategic Management, Faculty of Defense, University and Institute of National Defense and Strategic Research, Tehran, Iran. (Corresponding Author). aminmonazamimotlagh2@gmail.com
2. Assistant Professor, Industrial Safety, Faculty of Safety and Security Measures, Imam Hussein (AS) University, Tehran, Iran, negahdasht@yahoo.com.

human capital. The presented framework can be used as a comprehensive model for planning, recruiting, retaining, and developing specialized human resources in the field of cybersecurity defense in the gas industry.

Keywords
Cyber Defense, Strategic Human Capital Management, Gas Industry, Cybersecurity, Competency Framework.

مقاله علمی ـ پژوهشی

تاریخ دریافت ۱۴۰۴/۰۱/۲۳ تاریخ پذیرش ۱۴۰۴/۰۲/۱۷

توسعه چارچوب مدیریت راهبردی سرمایه انسانی متخصص در حوزه پدافند سایبری صنعت گاز

امین منظمی مطلق[۱] ـ عبدالرحمن کشوری[۲]

چکیده

پژوهش حاضر با هدف توسعه چارچوب مدیریت راهبردی سرمایه انسانی متخصص در حوزه پدافند سایبری صنعت گاز انجام شده است. با توجه به افزایش چشمگیر حملات سایبری به زیرساخت‌های حیاتی، توسعه چارچوبی جامع برای مدیریت نیروی انسانی متخصص در این حوزه ضرورتی انکارناپذیر است. این پژوهش از نظر هدف، کاربردی ـ توسعه‌ای و از لحاظ روش‌شناسی، آمیخته (کیفی ـ کمی) است. در مرحله کیفی با استفاده از تحلیل مضمون و مصاحبه‌های نیمه‌ساختاریافته با ۱۸ نفر از خبرگان، ابعاد و مؤلفه‌های اصلی چارچوب شناسایی شد. در مرحله کمی، پرسشنامه محقق ساخته با ۷۲ گویه بین ۱۹۶ نفر از متخصصان و مدیران پدافند سایبری صنعت گاز توزیع گردید. تحلیل داده‌ها با استفاده از مدل‌سازی معادلات ساختاری و نرم‌افزارهای SPSS و SmartPLS انجام شد. یافته‌ها نشان داد چارچوب نهایی شامل ۶ بعد اصلی (راهبردهای توسعه مهارت‌های تخصصی، مدیریت استعداد سایبری، فرهنگ امنیت سایبری، ساختار سازمانی چابک، حکمرانی سایبری و مدیریت دانش پدافند سایبری)، ۱۵ مؤلفه و ۵۴ شاخص است. نتایج تحلیل مسیر نشان داد بین ابعاد شش‌گانه چارچوب و مدیریت راهبردی سرمایه انسانی رابطه معنادار وجود دارد (P<0.01). مهم‌ترین یافته پژوهش، تأکید بر نقش محوری مؤلفه‌های مهارت‌افزایی تخصصی و توسعه فرهنگ امنیت سایبری در ایجاد سرمایه انسانی کارآمد است.

۱. دانشجوی دکترا، مدیریت راهبردی، دانشکده دفاع، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران. (نویسنده مسئول) aminmonazamimotlagh2@gmail.com

۲. استادیار، ایمنی صنعتی، دانشکده ایمنی و اقدامات تأمینی، دانشگاه جامع امام حسین (ع)، تهران، ایران. negahdasht@yahoo.com

چارچوب ارائه‌شده می‌تواند به‌عنوان الگویی جامع برای برنامه‌ریزی، جذب، نگهداشت و توسعه نیروی انسانی متخصص در حوزه پدافند سایبری صنعت گاز مورد استفاده قرار گیرد.

واژگان کلیدی: پدافند سایبری، مدیریت راهبردی سرمایه انسانی، صنعت گاز، امنیت سایبری، چارچوب شایستگی.

مقدمه

امروزه صنعت گاز به‌عنوان یکی از زیرساخت‌های حیاتی کشور، نقش مهمی در اقتصاد و امنیت انرژی ایفا می‌کند. با گسترش روزافزون فناوری‌های دیجیتال و هوشمندسازی سیستم‌های کنترلی در این صنعت، تهدیدات سایبری نیز به‌طور چشمگیری افزایش یافته است. حملات سایبری به تأسیسات گاز می‌تواند اختلالات جدی در تأمین انرژی، خسارات مالی هنگفت و حتی آسیب‌های جانی به همراه داشته باشد. نگاه ما به نیروی انسانی توانمند می‌بایست راهبردی باشد و تصویرسازی از یک نیروی سایبری و طراحی مفهومی، نخستین گام در استقرار سازمان سایبری محسوب می‌شود (یوسفی و محترمی، ۱۴۰۰).

پدافند سایبری به مجموعه اقدامات دفاعی و پیشگیرانه برای محافظت از سیستم‌ها، شبکه‌ها و داده‌ها در برابر حملات سایبری اطلاق می‌شود. با پیچیده‌تر شدن تهدیدات سایبری، نیاز به نیروی انسانی متخصص در این حوزه نیز افزایش یافته است. سیتول و همکاران (۲۰۲۰) در پژوهش خود نشان دادند که موفقیت سازمان‌ها در مقابله با تهدیدات سایبری، تنها به فناوری‌ها و سیستم‌های پیشرفته وابسته نیست، بلکه مدیریت راهبردی سرمایه انسانی متخصص در این حوزه، عامل تعیین‌کننده اصلی است. همچنین کالدرمیدیس و همکاران (۲۰۲۲) تأکید می‌کنند که سرمایه‌گذاری در حوزه امنیت سایبری بدون توجه به توسعه شایستگی‌های تخصصی نیروی انسانی، اثربخشی لازم را نخواهد داشت.

صنعت گاز ایران با چالش‌های متعددی در زمینه تأمین و نگهداشت نیروی انسانی متخصص در حوزه پدافند سایبری مواجه است. از یک‌سو، سرعت تحولات تکنولوژیک و تغییر مداوم ماهیت تهدیدات سایبری، نیازمند به‌روزرسانی مستمر دانش و مهارت‌های نیروی انسانی است. از سوی دیگر، فاصله میان آموزش‌های دانشگاهی با نیازهای واقعی صنعت در این حوزه، کمبود متخصصان کارآمد را به همراه داشته است. همچنین، فقدان چارچوب مشخص برای شناسایی، ارزیابی و توسعه شایستگی‌های مورد

نیاز در حوزه پدافند سایبری، برنامه‌ریزی راهبردی در این زمینه را با دشواری مواجه ساخته است (Rob et al., 2016).

مروری بر پیشینه پژوهش‌های داخلی و خارجی نشان می‌دهد علیرغم اهمیت موضوع، تاکنون چارچوبی جامع برای مدیریت راهبردی سرمایه انسانی در حوزه پدافند سایبری صنعت گاز ارائه نشده است. هونگ و همکاران (۲۰۲۰) چارچوبی برای شایستگی‌های شغلی در پاسخگویی فنی به تهدیدات سایبری ارائه کرده‌اند، اما این چارچوب محدود به جنبه‌های فنی بوده و ابعاد راهبردی و مدیریتی را در بر نمی‌گیرد. دوتویت (۲۰۲۲) نیز چارچوبی برای توسعه شایستگی‌های ضد جاسوسی سایبری پیشنهاد کرده است، اما این چارچوب نیز به‌طور خاص برای صنعت گاز طراحی نشده و نیازهای ویژه این صنعت را پوشش نمی‌دهد.

پژوهش‌های داخلی نیز عمدتاً بر جنبه‌های فنی امنیت سایبری متمرکز بوده‌اند. کاویانی و همکاران (۲۰۲۰) الگویی برای توسعه راهبردی منابع انسانی در حوزه امنیت سایبری نیروهای مسلح ارائه کرده‌اند، اما این الگو نیز به‌طور خاص برای صنعت گاز کاربردی نیست. با توجه به شکاف تحقیقاتی موجود و اهمیت روزافزون پدافند سایبری در صنعت گاز، ضرورت طراحی چارچوبی جامع و کاربردی برای مدیریت راهبردی سرمایه انسانی متخصص در این حوزه آشکار می‌شود.

این پژوهش با هدف توسعه چارچوبی جامع برای مدیریت راهبردی سرمایه انسانی متخصص در حوزه پدافند سایبری صنعت گاز انجام شده است. پژوهش حاضر به دنبال پاسخ به سؤالات زیر است:

۱. ابعاد و مؤلفه‌های اصلی چارچوب مدیریت راهبردی سرمایه انسانی متخصص در حوزه پدافند سایبری صنعت گاز کدام‌اند؟

۲. شاخص‌های هریک از مؤلفه‌های شناسایی‌شده چیست؟

۳. میزان اهمیت و اولویت هریک از ابعاد، مؤلفه‌ها و شاخص‌های شناسایی‌شده چگونه است؟

۴. روابط میان ابعاد چارچوب پیشنهادی چگونه است؟

بر اساس بررسی پیشینه پژوهش و چارچوب نظری، فرضیه‌های زیر تدوین شده است:

H1: راهبردهای توسعه مهارت‌های تخصصی تأثیر معناداری بر مدیریت راهبردی سرمایه انسانی در حوزه پدافند سایبری صنعت گاز دارد.

H2: مدیریت استعداد سایبری تأثیر معناداری بر مدیریت راهبردی سرمایه انسانی در حوزه پدافند سایبری صنعت گاز دارد.

H3: فرهنگ امنیت سایبری تأثیر معناداری بر مدیریت راهبردی سرمایه انسانی در حوزه پدافند سایبری صنعت گاز دارد.

H4: ساختار سازمانی چابک تأثیر معناداری بر مدیریت راهبردی سرمایه انسانی در حوزه پدافند سایبری صنعت گاز دارد.

H5: حکمرانی سایبری تأثیر معناداری بر مدیریت راهبردی سرمایه انسانی در حوزه پدافند سایبری صنعت گاز دارد.

H6: مدیریت دانش پدافند سایبری تأثیر معناداری بر مدیریت راهبردی سرمایه انسانی در حوزه پدافند سایبری صنعت گاز دارد.

تحقیق حاضر، با توسعه چارچوبی جامع برای مدیریت راهبردی سرمایه انسانی در حوزه پدافند سایبری صنعت گاز، می‌تواند به سازمان‌های فعال در این صنعت در جهت شناسایی، جذب، نگهداشت و توسعه نیروی انسانی متخصص یاری رساند. همچنین، این چارچوب می‌تواند به‌عنوان مبنایی برای تدوین برنامه‌های آموزشی، ارزیابی عملکرد، مسیر ارتقای شغلی و سیاست‌گذاری‌های کلان در حوزه منابع انسانی صنعت گاز مورد استفاده قرار گیرد.

روش‌شناسی

پژوهش حاضر از نظر هدف، کاربردی ـ توسعه‌ای، از لحاظ ماهیت، اکتشافی ـ تبیینی و از نظر روش‌شناسی، آمیخته (کیفی ـ کمی) با طرح اکتشافی متوالی است. با توجه به ماهیت میان‌رشته‌ای موضوع و نبود چارچوب جامع در زمینه مدیریت راهبردی سرمایه انسانی در حوزه پدافند سایبری صنعت گاز، استفاده از روش آمیخته ضروری به نظر می‌رسید. این پژوهش در دو مرحله اصلی کیفی و کمی انجام شده است که در ادامه به تشریح هریک از این مراحل پرداخته می‌شود.

در مرحله کیفی، با هدف شناسایی ابعاد، مؤلفه‌ها و شاخص‌های چارچوب مدیریت راهبردی سرمایه انسانی در حوزه پدافند سایبری صنعت گاز، از روش تحلیل مضمون استفاده شد. داده‌های کیفی از طریق مصاحبه‌های نیمه‌ساختاریافته با خبرگان صنعت گاز و متخصصان حوزه پدافند سایبری جمع‌آوری گردید. جامعه آماری در این مرحله شامل مدیران ارشد، متخصصان و کارشناسان حوزه فناوری اطلاعات و امنیت

سایبری در صنعت گاز و همچنین اساتید دانشگاهی متخصص در این حوزه بود.

برای انتخاب نمونه از روش نمونه‌گیری هدفمند و تکنیک گلوله‌برفی استفاده شد. معیارهای ورود به مطالعه عبارت بودند از: ۱. داشتن حداقل ۱۰ سال سابقه کار در زمینه پدافند سایبری یا مدیریت منابع انسانی در صنعت گاز؛ ۲. دارا بودن مدرک تحصیلی حداقل کارشناسی ارشد در رشته‌های مرتبط با فناوری اطلاعات، امنیت سایبری یا مدیریت منابع انسانی؛ و ۳. آشنایی کافی با چالش‌های صنعت گاز در حوزه امنیت سایبری.

فرآیند مصاحبه تا رسیدن به اشباع نظری ادامه یافت که درنهایت با ۱۸ نفر مصاحبه انجام شد. تمامی مصاحبه‌ها ضبط و سپس به متن تبدیل شدند. برای تحلیل داده‌های کیفی از روش تحلیل مضمون و نرم‌افزار MAXQDA نسخه ۲۰۲۲ استفاده شد. فرآیند تحلیل مضمون شامل سه مرحله کدگذاری باز، کدگذاری محوری و کدگذاری انتخابی بود. در مرحله کدگذاری باز، متن مصاحبه‌ها چندین بار مطالعه و مفاهیم اولیه استخراج شدند. در مرحله کدگذاری محوری، مفاهیم مشابه در قالب مقوله‌های محوری دسته‌بندی شدند. درنهایت، در مرحله کدگذاری انتخابی، مقوله‌های محوری در قالب ابعاد اصلی چارچوب مفهومی سازمان‌دهی شدند.

برای اطمینان از روایی و پایایی داده‌های کیفی، از معیارهای اعتبارپذیری، انتقال‌پذیری، اطمینان‌پذیری و تأییدپذیری استفاده شد. برای افزایش اعتبارپذیری، از روش بازبینی توسط اعضا استفاده شد و نتایج کدگذاری‌ها به تأیید مشارکت‌کنندگان رسید. برای افزایش انتقال‌پذیری، توصیف دقیقی از فرآیند پژوهش ارائه گردید. برای اطمینان‌پذیری، از روش بازبینی همکار استفاده شد و فرآیند کدگذاری توسط دو پژوهشگر به‌طور مستقل انجام و نتایج با یکدیگر مقایسه شد. برای تأییدپذیری نیز، تمامی مستندات و یادداشت‌های پژوهشگر حفظ و نگهداری شدند.

در مرحله کمی، با هدف اعتبارسنجی چارچوب مفهومی استخراج‌شده از مرحله کیفی و بررسی روابط میان ابعاد و مؤلفه‌های آن، از روش پیمایشی استفاده شد. جامعه آماری در این مرحله شامل کلیه مدیران، متخصصان و کارشناسان حوزه فناوری اطلاعات، امنیت سایبری و منابع انسانی در شرکت ملی گاز ایران و شرکت‌های تابعه بود که بر اساس آمار رسمی، تعداد آن‌ها ۳۸۵ نفر برآورد شد.

برای تعیین حجم نمونه از فرمول کوکران با سطح اطمینان ۹۵ درصد و خطای ۵ درصد استفاده شد:

$n = N \times Z^2222 \times p(1-p) \div [d^2 \times (N-)) + Z^2222 \times p(1-p)]\ n = 385 \times (1.96)^2 \times 0.5(1-0.5) \div [(0.05)^2 \times (385-1) + (1.96)^2 \times 0.5(1-))))\ ]\ n\ 8\ 8888888\ 133$

بر این اساس، حجم نمونه ۱۹۳ نفر تعیین شد. برای جمع‌آوری داده‌ها، با توجه به نتایج حاصل از مرحله کیفی، پرسشنامه‌ای محقق ساخته با ۷۲ گویه و بر اساس طیف لیکرت ۵ درجه‌ای (از کاملاً مخالفم=۱ تا کاملاً موافقم=۵) طراحی شد. این پرسشنامه شامل دو بخش اصلی بود: بخش اول شامل سؤالات جمعیت‌شناختی (سن، جنسیت، میزان تحصیلات، سابقه کار و سمت سازمانی) و بخش دوم شامل گویه‌های مربوط به ابعاد و مؤلفه‌های چارچوب مفهومی بود.

برای سنجش روایی محتوایی پرسشنامه، از شاخص‌های نسبت روایی محتوایی (CVR) و شاخص روایی محتوایی (CVI) استفاده شد. پرسشنامه در اختیار ۱۰ نفر از خبرگان قرار گرفت و از آن‌ها خواسته شد تا نظر خود را درباره ضرورت، مرتبط بودن، وضوح و سادگی هر گویه اعلام نمایند. گویه‌هایی که CVR آن‌ها کمتر از ۰/۶۲ (بر اساس جدول لاوشه) و CVI آن‌ها کمتر از ۰/۷۹ بود، از پرسشنامه حذف یا اصلاح شدند.

برای سنجش روایی سازه، از تحلیل عاملی تأییدی استفاده شد. همچنین، برای سنجش پایایی پرسشنامه، از ضریب آلفای کرونباخ و پایایی ترکیبی (CR) استفاده شد. پایایی پرسشنامه برای ابعاد مختلف بین ۰/۷۸ تا ۰/۹۲ محاسبه شد که نشان‌دهنده پایایی مطلوب ابزار پژوهش است.

پس از تأیید روایی و پایایی ابزار پژوهش، پرسشنامه‌ها به‌صورت الکترونیکی و حضوری بین اعضای نمونه توزیع شد. از ۲۱۰ پرسشنامه توزیع شده، ۱۹۶ پرسشنامه تکمیل و بازگردانده شد (نرخ بازگشت ۹۳/۳ درصد). برای تحلیل داده‌های کمی از نرم‌افزارهای SPSS نسخه ۲۶ و SmartPLS نسخه ۳,۳,۳ استفاده شد. برای تحلیل داده‌ها، از آمار توصیفی (فراوانی، درصد، میانگین و انحراف معیار) و آمار استنباطی (تحلیل عاملی تأییدی و مدل‌سازی معادلات ساختاری) استفاده شد.

یافته‌ها

تحلیل مضمون مصاحبه‌های انجام‌شده منجر به شناسایی ۱۶۲ کد باز، ۱۵ مؤلفه و ۶ بعد اصلی برای چارچوب مدیریت راهبردی سرمایه انسانی متخصص در حوزه پدافند سایبری صنعت گاز شد. ابعاد و مؤلفه‌های شناسایی‌شده در جدول ۱ ارائه شده است.

هریک از ابعاد و مؤلفه‌های شناسایی‌شده دارای شاخص‌هایی هستند که درمجموع ۵۴ شاخص شناسایی شد. جدول ۲ برخی از مهم‌ترین شاخص‌های هر مؤلفه را نشان می‌دهد.

جدول ۱. ابعاد و مؤلفه‌های چارچوب مدیریت راهبردی سرمایه انسانی متخصص در حوزه پدافند سایبری صنعت گاز

ردیف	ابعاد	مؤلفه‌ها
۱	راهبردهای توسعه مهارت‌های تخصصی	۱-۱. برنامه‌های آموزشی تخصصی پدافند سایبری ۱-۲. یادگیری مبتنی بر شبیه‌سازی حملات ۱-۳. همکاری‌های بین‌المللی برای توسعه مهارت
۲	مدیریت استعداد سایبری	۲-۱. شناسایی و جذب استعدادهای سایبری ۲-۲. نگهداشت متخصصان کلیدی ۲-۳. مسیر ارتقای شغلی متخصصان سایبری
۳	فرهنگ امنیت سایبری	۳-۱. آگاهی‌سازی و آموزش عمومی ۳-۲. مسئولیت‌پذیری در قبال امنیت سایبری
۴	ساختار سازمانی چابک	۴-۱. تیم‌های واکنش سریع ۴-۲. مدل‌های سازمان‌دهی منعطف
۵	حکمرانی سایبری	۵-۱. چارچوب‌های قانونی و مقرراتی ۵-۲. استانداردها و پروتکل‌های امنیتی ۵-۳. راهبردهای کلان پدافند سایبری
۶	مدیریت دانش پدافند سایبری	۶-۱. مستندسازی تجارب و درس آموخته‌ها ۶-۲. به اشتراک‌گذاری دانش سایبری

منبع: یافته‌های پژوهش

جدول ۲. شاخص‌های اصلی مؤلفه‌های چارچوب مدیریت راهبردی سرمایه انسانی متخصص در حوزه پدافند سایبری صنعت گاز

مؤلفه	شاخص‌های اصلی
برنامه‌های آموزشی تخصصی پدافند سایبری	دوره‌های آموزشی تخصصی مبتنی بر نیازسنجی گواهینامه‌های حرفه‌ای بین‌المللی آموزش‌های مستمر حین خدمت
یادگیری مبتنی بر شبیه‌سازی حملات	برگزاری رزمایش‌های سایبری پلتفرم‌های شبیه‌سازی حملات تمرین‌های عملی مقابله با حملات
همکاری‌های بین‌المللی برای توسعه مهارت	تبادل دانش با مراکز بین‌المللی همکاری با سایر شرکت‌های گاز در حوزه امنیت
شناسایی و جذب استعدادهای سایبری	سازوکارهای شناسایی استعدادهای سایبری نظام جذب تخصصی در حوزه پدافند سایبری همکاری با دانشگاه‌ها و مراکز آموزشی
نگهداشت متخصصان کلیدی	مدل‌های انگیزشی ویژه متخصصان سایبری جبران خدمات رقابتی محیط کار چالشی و یادگیرنده

مؤلفه	شاخص‌های اصلی
مسیر ارتقای شغلی متخصصان سایبری	مسیرهای ارتقای شغلی تعریف‌شده طراحی مشاغل تخصصی در حوزه پدافند سایبری
آگاهی‌سازی و آموزش عمومی	برنامه‌های آگاهی‌سازی کارکنان آموزش‌های عمومی امنیت سایبری
مسئولیت‌پذیری در قبال امنیت سایبری	فرهنگ گزارش‌دهی حوادث سایبری تقویت حس مالکیت در قبال امنیت سایبری

منبع: یافته‌های پژوهش

بر اساس یافته‌های کیفی، مدل مفهومی پژوهش به‌صورت شکل ۱ ترسیم شد.

شکل ۱. مدل مفهومی چارچوب مدیریت راهبردی سرمایه انسانی متخصص در حوزه پدافند سایبری صنعت گاز

منبع: این مدل برگرفته از یافته‌های تحلیل مضمون مصاحبه‌ها و پیشینه پژوهش‌های مرتبط است.

نتایج تحلیل مضمون مصاحبه‌ها منجر به شناسایی ۶ بعد، ۱۵ مؤلفه و ۵۴ شاخص برای چارچوب مدیریت راهبردی سرمایه انسانی متخصص در حوزه پدافند سایبری صنعت گاز شد. ابعاد اصلی شامل راهبردهای توسعه مهارت‌های تخصصی، مدیریت استعداد سایبری، فرهنگ امنیت سایبری، ساختار سازمانی چابک، حکمرانی سایبری و مدیریت دانش پدافند سایبری است. این ابعاد و مؤلفه‌ها در قالب مدل مفهومی پژوهش ترسیم گردید که مبنای بررسی‌های کمی در مرحله بعدی قرار گرفت.

برای بررسی برازش مدل اندازه‌گیری، از تحلیل عاملی تأییدی استفاده شد. نتایج تحلیل عاملی تأییدی مرتبه اول نشان داد که تمامی بارهای عاملی گویه‌ها بالاتر از ۰/۵ و معنادار هستند .($P<0.01$) همچنین، شاخص‌های برازش مدل در سطح مطلوبی قرار

دارند (RMSEA=0.068، CFI=0.92، GFI=0.87، AGFI=0.84)؛ بنابراین، مدل اندازه‌گیری از برازش مناسبی برخوردار است.

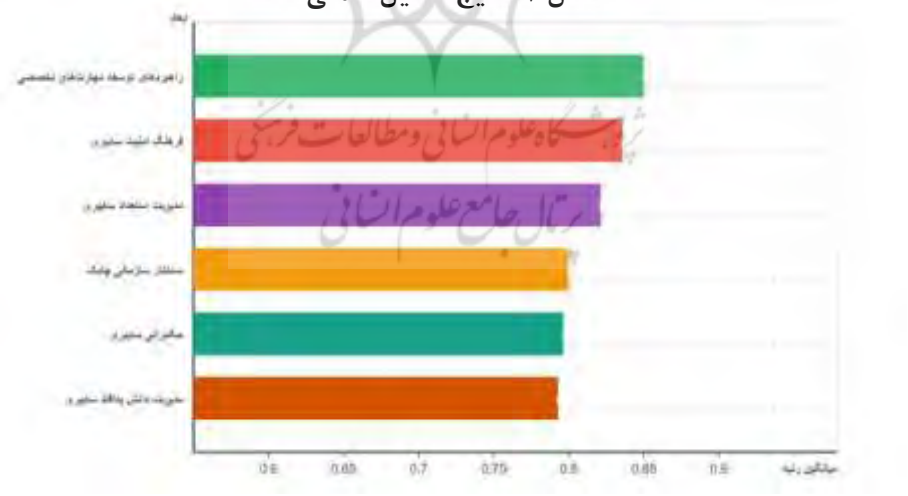
در تحلیل عاملی تأییدی مرتبه دوم، بارهای عاملی ابعاد شش‌گانه بر سازه مکنون مدیریت راهبردی سرمایه انسانی در حوزه پدافند سایبری صنعت گاز مورد بررسی قرار گرفت. نتایج در جدول ۴ ارائه شده است.

جدول ۴. نتایج تحلیل عاملی تأییدی مرتبه دوم ابعاد چارچوب مدیریت راهبردی سرمایه انسانی متخصص در حوزه پدافند سایبری صنعت گاز

ابعاد	بارعاملی	t-value	سطح معناداری	رتبه
راهبردهای توسعه مهارت‌های تخصصی	۰/۸۷	۱۸/۷۴	۰/۰۰۱	۱
مدیریت استعداد سایبری	۰/۷۸	۱۵/۴۳	۰/۰۰۱	۳
فرهنگ امنیت سایبری	۰/۸۲	۱۶/۹۲	۰/۰۰۱	۲
ساختار سازمانی چابک	۰/۷۲	۱۳/۶۷	۰/۰۰۱	۴
حکمرانی سایبری	۰/۷۱	۱۳/۲۵	۰/۰۰۱	۵
مدیریت دانش پدافند سایبری	۰/۷۰	۱۲/۹۶	۰/۰۰۱	۶

منبع: یافته‌های پژوهش

شکل ۲. نتایج تحلیل عاملی



نتایج تحلیل عاملی تأییدی مرتبه دوم نشان داد که تمامی ابعاد شش‌گانه از بارعاملی بالایی (بالاتر از ۰/۷) بر سازه مکنون مدیریت راهبردی سرمایه انسانی برخوردار هستند و این بارهای عاملی از نظر آماری معنادار هستند .(P<0.001) بیشترین بارعاملی

مربوط به بعد راهبردهای توسعه مهارت‌های تخصصی (۰/۸۷) و کمترین بارعاملی مربوط به بعد مدیریت دانش پدافند سایبری (۰/۷۰) است.

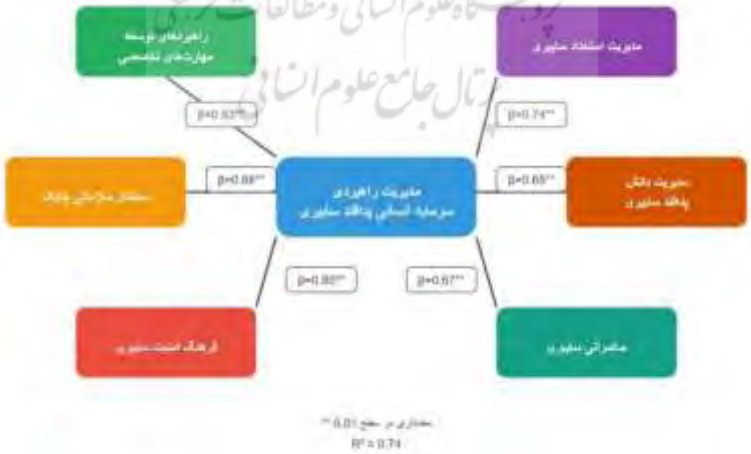
برای آزمون فرضیه‌های پژوهش از روش مدل‌سازی معادلات ساختاری و نرم‌افزار SmartPLS استفاده شد. نتایج آزمون فرضیه‌ها در جدول ۵ ارائه شده است.

جدول ۵. نتایج آزمون فرضیه‌های پژوهش

فرضیه	مسیر	ضریب مسیر	t-value	سطح معناداری	نتیجه آزمون
H1	راهبردهای توسعه مهارت‌های تخصصی → مدیریت راهبردی سرمایه انسانی	۰/۸۳	۱۷/۸۶	۰/۰۰۱	تأیید
H2	مدیریت استعداد سایبری → مدیریت راهبردی سرمایه انسانی	۰,۷۴	۱۴,۳۵	۰/۰۰۱	تأیید
H3	فرهنگ امنیت سایبری → مدیریت راهبردی سرمایه انسانی	۰,۸۰	۱۶,۴۲	۰/۰۰۱	تأیید
H4	ساختار سازمانی چابک → مدیریت راهبردی سرمایه انسانی	۰,۶۸	۱۲,۷۹	۰/۰۰۱	تأیید
H5	حکمرانی سایبری → مدیریت راهبردی سرمایه انسانی	۰,۶۷	۱۲,۴۳	۰/۰۰۱	تأیید
H6	مدیریت دانش پدافند سایبری → مدیریت راهبردی سرمایه انسانی	۰,۶۵	۱۱,۹۲	۰/۰۰۱	تأیید

منبع: یافته‌های پژوهش

شکل ۳. نتایج آزمون فرضیه‌ها



نتایج آزمون فرضیه‌ها نشان داد که تمامی فرضیه‌های پژوهش در سطح اطمینان ۹۹ درصد تأیید می‌شوند. بیشترین تأثیر مربوط به راهبردهای توسعه مهارت‌های

تخصصی (۰/۸۳) و کمترین تأثیر مربوط به مدیریت دانش پدافند سایبری (۰/۶۵) است.

برای رتبه‌بندی مؤلفه‌های چارچوب مدیریت راهبردی سرمایه انسانی متخصص در حوزه پدافند سایبری صنعت گاز، از آزمون فریدمن استفاده شد. نتایج در جدول ۶ ارائه شده است.

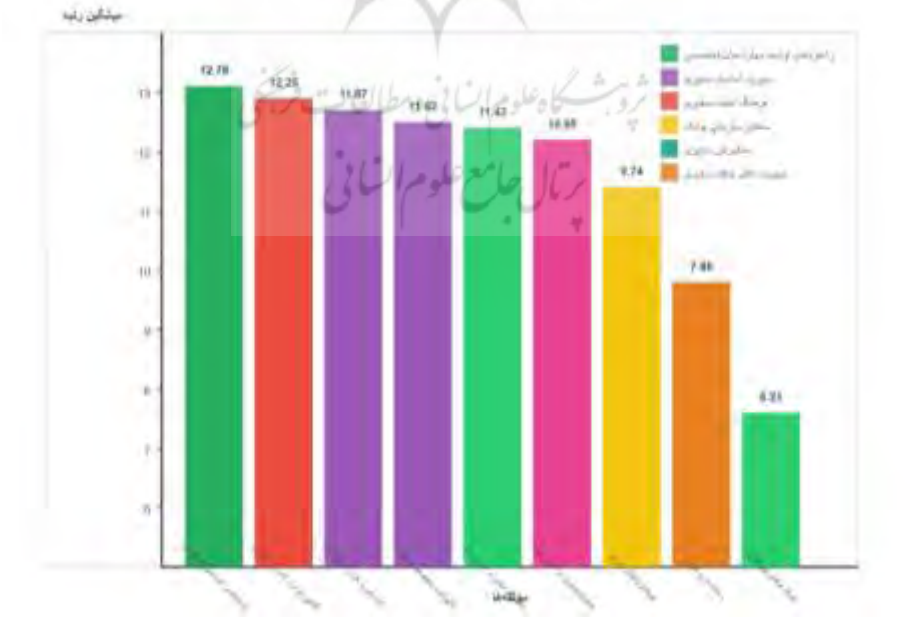
جدول ۶. نتایج رتبه‌بندی مؤلفه‌های چارچوب مدیریت راهبردی سرمایه انسانی متخصص در حوزه پدافند سایبری صنعت گاز

رتبه	مؤلفه	میانگین رتبه	میانگین	انحراف معیار
۱	برنامه‌های آموزشی تخصصی پدافند سایبری	۱۲/۷۸	۴/۵۲	۰/۶۳
۲	آگاهی‌سازی و آموزش عمومی	۱۲/۲۵	۴/۴۸	۰/۷۱
۳	شناسایی و جذب استعدادهای سایبری	۱۱/۸۷	۴/۳۶	۰/۶۹
۴	نگهداشت متخصصان کلیدی	۱۱/۶۲	۴/۳۱	۰/۷۴
۵	یادگیری مبتنی بر شبیه‌سازی حملات	۱۱/۴۳	۴/۲۷	۰/۷۶
...	...	...	...	...
۱۵	همکاری‌های بین‌المللی برای توسعه مهارت	۵/۲۱	۳/۴۲	۰/۹۸

مقدار کای اسکوئر: ۴۸۷/۳۲، درجه آزادی: ۱۴، سطح معناداری: ۰/۰۰۱

منبع: یافته‌های پژوهش

شکل ۴. نمودار رتبه‌بندی مؤلفه‌های چارچوب



نتایج آزمون فریدمن نشان داد که تفاوت معناداری بین رتبه مؤلفه‌های چارچوب وجود دارد. (P<0.001) پنج مؤلفه اصلی به ترتیب اولویت عبارت‌اند از: برنامه‌های آموزشی تخصصی پدافند سایبری، آگاهی‌سازی و آموزش عمومی، شناسایی و جذب استعدادهای سایبری، نگهداشت متخصصان کلیدی و یادگیری مبتنی بر شبیه‌سازی حملات.

تحلیل داده‌های کمی حاصل از پرسشنامه نشان داد تمامی ابعاد شش‌گانه چارچوب دارای تأثیر معنادار بر مدیریت راهبردی سرمایه انسانی در حوزه پدافند سایبری صنعت گاز هستند و همه فرضیه‌های پژوهش تأیید شدند. بیشترین تأثیر مربوط به راهبردهای توسعه مهارت‌های تخصصی (۰/۸۳) و کمترین تأثیر مربوط به مدیریت دانش پدافند سایبری (۰/۶۵) بود. همچنین، نتایج رتبه‌بندی مؤلفه‌ها نشان داد برنامه‌های آموزشی تخصصی، آگاهی‌سازی و آموزش عمومی و شناسایی و جذب استعدادهای سایبری در رتبه‌های اول تا سوم اهمیت قرار دارند.

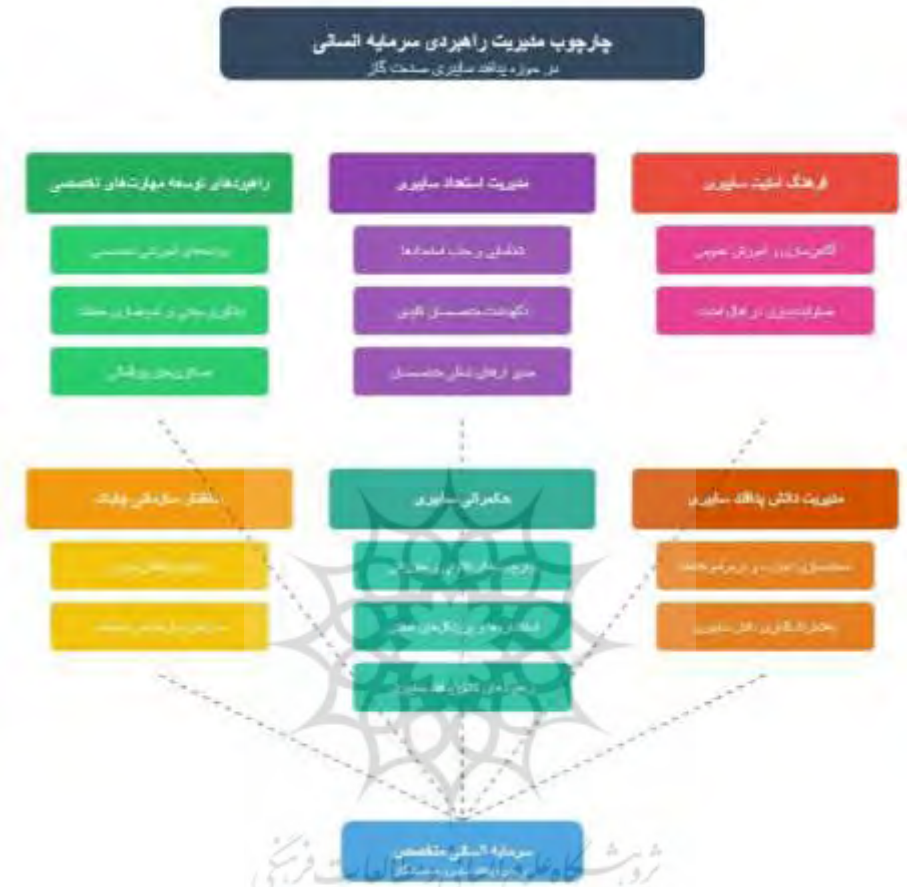
بحث و نتیجه‌گیری

پژوهش حاضر با هدف توسعه چارچوب مدیریت راهبردی سرمایه انسانی متخصص در حوزه پدافند سایبری صنعت گاز انجام شد. یافته‌های پژوهش منجر به شناسایی ۶ بعد، ۱۵ مؤلفه و ۵۴ شاخص شد که در قالب چارچوبی جامع ارائه گردید. این چارچوب می‌تواند به‌عنوان نقشه راهی برای برنامه‌ریزی، جذب، نگهداشت و توسعه سرمایه انسانی متخصص در حوزه پدافند سایبری صنعت گاز مورد استفاده قرار گیرد.

یافته‌های پژوهش نشان داد که راهبردهای توسعه مهارت‌های تخصصی بیشترین تأثیر را بر مدیریت راهبردی سرمایه انسانی در حوزه پدافند سایبری دارد. این یافته با نتایج پژوهش دوتویت (۲۰۲۲) همخوانی دارد. دوتویت در پژوهش خود تأکید می‌کند که توسعه مهارت‌های تخصصی نیروی انسانی در حوزه ضد جاسوسی سایبری، مهم‌ترین عامل در موفقیت سازمان‌ها برای مقابله با تهدیدات سایبری است. همچنین، این یافته با نتایج پژوهش هونگ و همکاران (۲۰۲۰) نیز همسو است. آن‌ها در پژوهش خود به این نتیجه رسیدند که توسعه شایستگی‌های شغلی در پاسخگویی فنی به تهدیدات سایبری، عامل کلیدی در موفقیت سازمان‌ها است.

دومین بعد تأثیرگذار بر مدیریت راهبردی سرمایه انسانی در حوزه پدافند سایبری، فرهنگ امنیت سایبری شناسایی شد.

شکل ۵. چارچوب مدیریت راهبردی سرمایه انسانی



این یافته با نتایج پژوهش مویم و همکاران (۲۰۲۳) مطابقت دارد. آن‌ها در پژوهش خود به این نتیجه رسیدند که عوامل مرتبط با فرهنگ امنیت سایبری، تأثیر قابل‌توجهی بر موفقیت اقدامات امنیتی سازمان‌ها دارد. همچنین، البراک (۲۰۲۴) در پژوهش خود تأکید می‌کند که ادغام امنیت سایبری، قابلیت استفاده و تعامل انسان ـ کامپیوتر برای امن‌سازی سیستم‌های مدیریت انرژی ضروری است.

مدیریت استعداد سایبری به‌عنوان سومین بعد تأثیرگذار شناسایی شد. این یافته با نتایج پژوهش گارگ (۲۰۲۳) همخوانی دارد. گارگ در پژوهش خود نشان داد که اقدامات مدیریت منابع انسانی، از جمله جذب و نگهداشت استعدادها، تأثیر قابل‌توجهی بر آسیب‌پذیری کارکنان در برابر حملات سایبری دارد.

ساختار سازمانی چابک، حکمرانی سایبری و مدیریت دانش پدافند سایبری، به

ترتیب در رتبه‌های چهارم تا ششم قرار گرفتند. این یافته‌ها با نتایج پژوهش‌های راب و همکاران (۲۰۱۶)، کالدرمیدیس و همکاران (۲۰۲۲) و ویرا و همکاران (۲۰۲۴) همخوانی دارد. این پژوهشگران در مطالعات خود به اهمیت ساختارهای سازمانی منعطف، چارچوب‌های حکمرانی سایبری و مدیریت دانش در بهبود امنیت سایبری سازمان‌ها تأکید کرده‌اند.

نکته قابل‌توجه در یافته‌های پژوهش، اهمیت بالای مؤلفه‌هایی مانند برنامه‌های آموزشی تخصصی پدافند سایبری، آگاهی‌سازی و آموزش عمومی و شناسایی و جذب استعدادهای سایبری است. این یافته نشان می‌دهد که در صنعت گاز، توسعه مهارت‌های تخصصی و عمومی کارکنان و جذب نیروهای متخصص، از مهم‌ترین اولویت‌ها در مدیریت راهبردی سرمایه انسانی در حوزه پدافند سایبری است.

منابع

کاویانی، حسن؛ میرسپاسی، ناصر؛ معمارزاده طهران، غلامرضا. (۲۰۲۰). الگوی توسعه راهبردی منابع انسانی در حوزه امنیت سایبری نیروهای مسلح ج.ا.ایران. *مطالعات مدیریت راهبردی دفاع ملی*، سال ۵، شماره ۱۷، صص ۱۴۸-۱۲۷.

یوسفی، آ.؛ محترمی، ا. (۱۴۰۰). ارائه چارچوبی برای توانمندسازی سرمایه انسانی در دفاع سایبری. *فصلنامه علمی و پژوهشی فرماندهی و کنترل*، ۵ (۴)، ۱-۲.

Albarrak, A. M. (2024). Integration of cybersecurity, usability, and human-computer interaction for securing energy management systems. *Sustainability*, 16 (18), 8144.

Brader, T. (2006). *Campaigning for hearts and minds: How emotional appeals in political ads work*. Chicago: University of Chicago Press.

Du Toit, J. L. (2022). A Cyber Counterintelligence Competence Framework. *Information Systems Management Journal*, 21(1), 368-377.

Elder, L. & Paul, R. (2006). *The miniature guide to the art of asking essential questions*. Dillon Beach, CA: Foundation for Critical Thinking.

Garg, S. (2023). Opening the Black Box of Employee Vulnerability to Cyberattacks. *Proceedings of the Academy of Management*, 2023(1), 10001-10013.

Hong, S. J., Kim, J. S., Kim, Y. G., & Park, H. J. (2020). A Proposal of Cybersecurity Technical Response Job Competency Framework and its Applicable Model Implementation. *Journal of the Korea Institute of Information Security & Cryptology*, 30(6), 1167-1187.

Kalderemidis, I., Koloveas, P., Mitropoulos, D., Douligeris, C., &

Panagiotis, G. (2022). GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments. *IACR Conference Proceedings*, 680, 673-680.

Miller, T. E., Bender, B. E., & Schuh, J. H. (2005). *Promoting reasonable expectations: Aligning student and institutional views of the college experience*. San Francisco, CA: Jossey-Bass.

Mwim, E. N., Ochara, N. M., & Pistorius, C. (2023). Conceptual Mapping of the Cybersecurity Culture to Human Factor Domain Framework. *International Conference on Information Society Proceedings*, 729-742.

Newman, J. L., Fuqua, D. R., Gray, E. A., & Simpson, D. B. (2006). Gender differences in the relationship of anger and depression in a clinical sample. *Journal of Counseling & Development*, 84, 157-161.

Okoye, H. G., & Haspel, M. (2006). The impact of gentrification on voter turnout. *Social Science Quarterly*, 87(1), 110-121.

Rob, R. A., Dadfar, M., Nowak, D., Sulaiman, I., & Demerjian, H. (2016). Addressing cyber security for the oil, gas and energy sector. *Saudi Arabia Smart Grid and Green Energy Conference*, 1-7.

Vieira, P. F., Filho, J. C. D. P., & Reis, R. P. (2024). Industrial Cybersecurity, Process Safety and Human Factors: A Comprehensive 360-Degree Approach. *Oil Industry Journal*, 35396, 1-15.