فصلنامه علمی مطالعات بین‌رشته‌ای دانش راهبردی
سال دهم، شماره ٤١، زمستان ١٣٩٩، صفحات ٢٩٨-٢٧٣

مقاله پژوهشی: # طراحی مدل شایستگی کارکنان در حوزه امنیت سایبری

حسن کاویانی[1]، ناصر میرسپاسی[2] و غلامرضا معمارزاده طهران[3]

تاریخ دریافت: ۹۸/۱۰/۲۰ **تاریخ پذیرش: ۹۹/۰٤/۱۰**

چکیده

در دهه‌های اخیر و هم‌زمان با افزایش ضریب نفوذ اینترنت و فضای سایبری، طیف وسیعی از دولت‌ها به منظور محافظت از زیرساخت‌ها و شهروندان خود در مقابل تهدیدات بالقوه و بالفعل سایبری، اقدام به بازطراحی و بازنگری در سیاست‌ها، ساختارها و راهبردهای خود در عرصه‌های امنیتی و نظامی نموده‌اند. یکی از مهم‌ترین این اقدامات طراحی مدل‌های شایستگی جهت تأمین، پرورش و به‌کارگیری اثربخش و کارآمد منابع انسانی در این حوزه است. از این رو در این تحقیق به طراحی مدل شایستگی کارکنان در حوزه امنیت سایبری به‌عنوان هدف اصلی تحقیق مبادرت نموده‌ایم. پژوهش حاضر از منظر هدف، کاربردی- توسعه‌ای و از جنبه گردآوری و تحلیل داده‌ها، کمی می‌باشد. به‌منظور تحقق اهداف تحقیق در مرحله اول، پس از استخراج ٢٤ شاخص از مطالعات اکتشافی، مدل مفهومی تحقیق در قالب و ساختار مدل کوه یخی طراحی گردید. در مرحله دوم بر اساس اجزای مدل، پرسشنامه‌ای تنظیم گردید. روایی صوری و پایایی این پرسشنامه با نظرخواهی از تعداد هشت نفر از خبرگان مورد بررسی قرار گرفت. در مرحله سوم بر اساس نظریات ٤٣ نفر از خبرگان علمی و اجرایی حوزه امنیت سایبری کشور، مطلوبیت اجزای مدل با استفاده از نرم‌افزارهای spss و pls مورد ارزیابی قرار گرفت. بر اساس نتایج تحقیق، مدل شایستگی کارکنان شامل دو بعد شایستگی‌های فنی و تخصصی و شایستگی‌های عمومی است. شایستگی‌های فنی و تخصصی متشکل از دانش و مهارت است. شایستگی‌های عمومی نیز مؤلفه‌های خودمفهومی، ویژگی‌های شخصیتی و انگیزه‌ها را در برمی گیرد.

کلید واژه‌ها: شایستگی، امنیت سایبری، مدل کوه یخی.

۱. دانشجوی دکتری مدیریت دولتی، دانشکده مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران
۲. استاد مدیریت دولتی، دانشکده مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران (مسئول مکاتبات)- Mirsepassi@srbiau.ac.ir
۳. دانشیار مدیریت دولتی، دانشکده مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران

مقدمه

افزایش تهدیدات در فضای سایبری منجر به افزایش تقاضا برای متخصصـان و کارکنـان حرفه‌ای امنیت سایبری گردیده است، زیرا در حقیقت توانایی محافظت از زیرسـاخت‌هـا و خنثی نمودن تهدیدهای سایبری به میزان آمادگی و صلاحیت آن‌ها بستگی دارد (بریلینگیت و همکـاران[1]،۲۰۲۰). با این حال مبرهن است که تأمین و پرورش چنین منـابع انسـانی توانمنـد و شایسته‌ای بدون شناخت از ویژگی‌های مطلوب مورد نیاز آن‌ها امکان‌پذیر نمی‌باشد. از ایـن رو در سالیان اخیر طراحی مدل‌های شایستگی در حوزه امنیت سایبری به‌عنوان شرطی لازم در جهت مدیریت اثربخش سرمایه‌های انسانی مورد توجه بسیاری از کشورها قـرار گرفتـه است. این مدل‌ها به‌مثابه ابزار توصیفی مهارت، دانش، ویژگی‌های شخصیتی و رفتاری مؤثر بر تحقق مطلوب وظایف و مسئولیت‌های هر شغل را تعیین می‌نمایند. شاخص‌هایی که مـی توانند به‌عنوان معیاری جهت جذب و پرورش منـابع انسـانی توانمنـد، ارزیـابی کارکنـان و پرداخت حقوق و مزایا مورد استفاده قرار گیرند (وایت من،۲۰۱۸).

در دهه‌های اخیر و همگام با افزایش ضریب نفوذ اینترنـت و شـبکه‌هـای ارتبـاطی بـه موازات سایر کشورها، تهدیدات و حملات سایبری به کشور نیز با رشد چشمگیری مواجـه بوده است. برابر برخی از آمارها در سال ۱۳۹٤، روزانه ۱۳ تا ١٤ هزار حمله اینترنتـی علیـه کشور صورت می‌گرفته است (فاضلی و افضلی، ۱۳۹٤) که تعداد حملات شناسایی و دفع‌شده آن در سال ۱۳۹۸ به‌صورت میانگین به روزانه بیش از ۹۰ هزار حمله افزایش یافته اسـت(معـاون قرارگاه سایبری سازمان پدافند غیرعامل،۱۳۹۸). در چنین شرایطی تحقق امنیت ملی کشـور در گـروی برخورداری و تربیت منابع انسانی شایسته و توانمند است. موضوعی که علیرغم تصریح در حوزه سیاست‌گذاری و در قالب بند «٤» حکم انتصاب شورای عالی فضای مجازی (۱۳۹٤) و نیز سند راهبردی پدافند سایبری کشور (۱۳۹٤)، تـاکنون چهـارچوب اجرایـی مناسـب و جامعی در قالب قانون، تصویب‌نامه یا آیین‌نامه اجرایـی بـرای آن تـدوین نگردیـده اسـت. موضوعی که مؤید مغفول ماندن این موضوع راهبردی در بدنـه اجرایـی کشـور مـی‌باشـد. درحالی‌که ارائه مدل جامع از ویژگی‌ها و صلاحیت‌های مورد تأییـد و تأکیـد از کارکنـان و

1. Brilingaite et al

منابع انسانی در تراز انقلاب اسلامی و حوزه امنیت سایبری، یکی از اولـین الزامـات تحقـق امنیت پایدار در صنعت فناوری‌های ارتباطی و اطلاعاتی می‌باشد. در حـوزه علمـی نیـز بـا وجود برخی تلاش‌های انجام‌شده در راستای طراحی و معرفی صـلاحیت‌هـای مـورد نیـاز کارکنان در حوزه‌های امنیتی و دفاعی، لیکن تـلاش منسـجم و دقیقـی در خصـوص تبیـین شایستگی‌های مورد نیاز کارکنان در حوزه امنیت سایبری انجام نشده است. به همـین دلیـل محققان قصد دارند مدل شایستگی‌های منابع انسانی متناسب بـا بـوم ایـران و سـازمان‌هـای نظامی متولی در حوزه امنیت سایبری را استخراج و بر اسـاس مـدل کـوه یخـی اسپنسـر و اسپنسر تبیین نمایند. لذا آنچه ذهن نویسندگان را به‌عنوان چالش و دغدغه اصـلی بـه خـود معطوف نموده است، این است که مدل شایستگی کارکنان در حوزه امنیت سایبری کدامند؟ بنابراین مسئله اصلی تحقیق فقدان مدل‌های شایستگی کارکنان در حوزه امنیت سایبری مـی باشد. به‌طور خلاصه عوامل ایجابی که باعث اهمیت این تحقیق شده‌اند، عبارت‌اند از:

الف) با توجه به نقش محوری منابع انسانی در حوزه امنیت سایبری، طراحی مـدل‌هـای شایستگی منطبق با بوم ایران و حوزه مذکور به‌عنوان نقشـه راه و ابـزار ارزیـابی نظـام‌هـای مدیریت منابع انسانی، باعث افزایش اقتدار امنیتی و دفاعی می‌گردد.

ب) توسعه مدل‌های موجود شایستگی منابع انسانی متناسب با بوم ایران، رشته مدیریت دولتی و صنعت امنیت سایبری از دیگر وجوه اهمیت تحقیق حاضر می‌باشد.

ج) باعث ایجاد فهم، بینش و معیارهای مشترک در خصوص چگونگی تحقـق سیاسـت های کلی نظام در حوزه‌های «امنیت فضای تولیـد و تبـادل اطلاعـات و ارتباطـات، پدافنـد غیرعامل و سند راهبردی پدافند سایبری و نیز تحقق اسناد بالادستی» می‌گردد.

عوامل سلبی که باعث ضرورت اجرای تحقیق گردیده است، عبارت‌اند از:

الف) فقدان مدل‌های جامع شایستگی منجر به برخورد سلیقه‌ای و غیرعلمـی، اخـلال و ناهماهنگی در نظام‌هـای چهارگانـه مـدیریت منـابع انسـانی (تـأمین، توسـعه، حفـظ و بـه کارگیری) می‌گردد که این موضوع باعث سرخوردگی و ناامیدی کارکنان توانمند و شایسـته خواهد شد.

ب) بی‌توجهی در خصوص تدوین و طراحی مدل‌ها و چهارچوب‌های شایستگی متناسب با حوزه امنیت سایبری کشور می‌تواند به کاهش توان دفاعی- امنیتی در حوزه مذکور منتهی گردد.

ج) کاهش خلأ تحقیقاتی و پژوهشی در خصوص مدل‌های شایستگی در حوزه امنیت سایبری کشور و سیاست‌های ابلاغی در بند «٤» حکم انتصاب شورای عالی فضای مجازی (١٣٩٤) از دیگر وجوه ضرورت تحقیق حاضر می‌باشد.

پیشینه‌شناسی تحقیق

در ادامه برخی از پژوهش‌های صورت‌گرفته در خصوص مدل‌های شایستگی در بخش دولتی و حوزه امنیت سایبری ارائه گردیده است.

در پیمایشی که در بین ۵۰۰ نفر از مدیران و رهبران حوزه امنیت سایبری در کشور آمریکا صورت پذیرفت. مدلی برای شایستگی منابع انسانی شرکت‌های امنیتی و سایبری طراحی گردید. این مدل شامل سه بعد اصلی به شرح ذیل است:

۱. **دانش‌های اصلی:** مفاهیم مشترک امنیتی سایبری، سیاست‌های تنظیم‌گری، بهترین تجارب این حوزه و مفاهیم حقوقی.
۲. **مهارت‌های اصلی:** مهارت بررسی و جست‌وجوی اینترنتی، ارزیابی ریسک، تحلیل داده‌ها، توانایی اتخاذ تصمیمات سودمند در کسب‌وکار، مهارت‌های تحلیلی کسب‌وکار، مدیریت تغییرات، مهارت‌های بین فردی، مهارت‌های بازاریابی، مهارت‌های مذاکره، مهارت‌های فروش و مهارت کار تیمی.
۳. **توانایی‌های کلیدی:** انطباق‌پذیری، فرهنگ یادگیری، محرمانگی (حفظ اسرار)(دانشگاه فونیکس،۲۰۱۸).

مرکز ملی آمادگی حوادث و استراتژی امنیت سایبری ژاپن در سال ۲۰۱۱ میلادی پس از بررسی وضعیت و چالش‌های امنیت اطلاعات در سطح ملی، اذعان داشت که بهبود کامل امنیت اطلاعات زمانی حاصل می‌شود که توسعه منابع انسانی پیشرفته برای حوزه فناوری اطلاعات و ارتباطات در تمام سطوح نهادینه گردد. این سازمان به این منظور برنامه

ای را تدوین و ارائه نموده است که هدف از آن توسعه منابع انسانی امنیت اطلاعات در سازمان‌های دولتی، شرکت‌ها و مؤسسات آموزشی می‌باشد. در این برنامه پنج مفهوم بنیادین در جهت توسعه منابع انسانی امنیت اطلاعات شامل توسعه و حفظ منابع انسانی پیوندی (هیبریدی)، ایجاد محیط مناسب جهت توسعه منابع انسانی امنیت اطلاعات، تقویت همکاری دانشگاه و صنعت، توسعه منابع انسانی از طریق تحقیق و توسعه پیشرفته و احیای صنعت امنیت اطلاعات و نیز توسعه منابع انسانی به‌عنوان بازیگران بین‌المللی ارائه گردیده است. در خصوص منابع انسانی پیوندی (هیبریدی)، با توجه به اینکه حوزه منابع انسانی امنیت اطلاعات از لحاظ فنی ارتباط نزدیکی با حوزه‌هایی چون ریاضیات، کامپیوتر، مهندسی ارتباطات و از جنبه مدیریتی با اقتصاد، حقوق، حسابداری، جامعه‌شناسی و روان شناسی دارد؛ در این راستا تأکید شده است که منابع انسانی امنیت اطلاعات در کنار تخصص فنی در مورد نظام‌های اطلاعاتی و امنیت اطلاعات به تخصص در حوزه مدیریت و به‌ویژه مدیریت ریسک نیاز دارند. همچنین با توجه به تغییرات پویا و مستمر محیط حوزه امنیت اطلاعات، متخصصان باید قادر به کشف و پاسخگویی فوری و مناسب به ریسک‌ها و مسائل پیش‌آمده باشند.

وزارت امنیت داخلی آمریکا (۲۰۱٦ م) جعبه‌ابزاری برای ساختن یک نیروی کار امنیت سایبری ارائه نموده است. در این جعبه‌ابزار کارکنان به سه سطح مبتدی، میانی و ارشد تقسیم‌بندی شده و بر این اساس شایستگی‌های عمومی و تخصصی، برخی آموزش‌های لازم و نیز شرایط استخدام آنان ارائه شده است. در این جعبه‌ابزار از ویژگی‌های توانایی اعمال دانش در موقعیت‌های کاری جدید، دشوار و پیچیده، تفکر انتقادی، مهارت تحلیلی، ارتباطات کتبی و شفاهی، توجه به جزئیات، حل خلاقانه مسائل، مذاکره و تأثیرگذاری، رهبری و مدیریت کارکنان به‌عنوان شایستگی محوری و مورد نیاز سطوح مختلف یاد شده است.

پورعابدی و همکاران وی (۱۳۹۵) در تحقیقی به طراحی مدل شایستگی چندبعدی مدیران و کارکنان در سازمان تنظیم مقررات و ارتباطات رادیویی با استفاده از رویکرد ترکیبی اقدام نموده‌اند. نتایج این تحقیق ٤٠ گروه شایستگی مشتمل بر چهار لایه شایستگی

های پایه (مهارت ارتباطی، مهارت یادگیری، ابتکار و خلاقیت، مشتری‌مداری و...)، شایستگی‌های مدیریتی (جهت‌گیری راهبردی، نتیجه‌گرایی، مدیریت پروژه، مدیریت سازمان و منابع انسانی، مدیریت تحقیقات و...)، شایستگی‌های عمومی (قوانین و مقررات در فضای فناوری اطلاعات، اصول امنیتی فضای مذکور و...) و شایستگی تخصصی (حقوق تنظیم‌گری، صدور پروانه و...) است.

با توجه به نتایج بررسی پیشینه تحقیق، به نظر می‌رسد در عرصه بین‌المللی، طراحی مدل‌های شایستگی کارکنان در حوزه امنیت سایبری یکی از موضوعاتی است که در سالیان اخیر بیش از گذشته مورد توجه کشورهای مختلف قرار گرفته است. موضوعی که در تحقیقات داخلی چندان مورد توجه دستگاه‌های اجرایی و پژوهشگران قرار نگرفته است. لذا انجام این پژوهش از لحاظ مناسبت و ضرورت طراحی چهارچوبی شایستگی منابع انسانی در حوزه امنیت سایبری، اقدامی نوآورانه محسوب می‌گردد.

شایستگی

ریشه مفهوم شایستگی، کلمه لاتین competenia به معنای «مجاز به داوری» و همچنین «حق صحبت کردن» می‌باشد (کائوشیکی و همکاران، ۲۰۱٤). این مفهوم دارای سابقه‌ای به قدمت تاریخ تمدن‌های باستان می‌باشد. به‌طوری‌که رومیان در تلاش برای به‌کارگیری سربازان مناسب‌تر، ویژگی‌های مهارتی را تعیین می‌کردند و مبنای به‌کارگیری افراد قرار می‌داده‌اند. ولی معرفی رویکرد مبتنی بر شایستگی به‌عنوان رویکردی تأثیرگذار در حوزه کسب‌وکار و مدیریت منابع انسانی از دهه ۱۹۷۰ میلادی آغاز گردیده است. در این زمان روان‌شناس برجسته دانشگاه هاروارد، دیوید مک کللند[1] ایده آزمون شایستگی را به جای آزمون هوش به‌منظور بهبود رویه‌های استخدام و به‌کارگیری کارکنان در آژانس اطلاعات ایالات‌متحده پیشنهاد نمود (فوتیس و همکاران،۲۰۰٦). این نظریه برگرفته از دیدگاه مبتنی بر منابع[2] می‌باشد. در این نظریه کسب مزیت رقابتی پایدار تنها از طریق منابع، قابلیت‌ها و شایستگی‌های

1. David Mcclelland
2. Resource-based View

داخلی حاصل می‌شود. لذا مدیران مؤسسات و سازمان‌ها ملزم به مشخص نمودن این شایستگی‌ها و سپس مدیریت اثربخش و کارآمد آن‌ها می‌باشند (کلودیا و همکاران، ۲۰۰۹). با این وجود به‌رغم گذشت سال‌ها از ظهور مفهوم شایستگی و مدل‌های مرتبط با آن، کماکان وحدت نظری در خصوص معنای این مفهوم وجود ندارد. شایستگی که برخی مصادیق آن در جدول «۱» ارائه گردیده است.

جدول ۱: برخی تعاریف مفهوم شایستگی

نویسنده	تعریف شایستگی
مک کللند[1] (۱۹۷۳ م)	شایستگی ابزاری است که توسط آن می‌توان فرد عالی را از افراد معمولی تشخیص داد.
فوتیس (۲۰۰۶ م)	شایستگی ترکیبی از دانش، مهارت و رفتار آشکار و ضمنی است که به کارکنان پتانسیل اثربخشی در انجام وظایفشان را می‌دهد.
ویچیتا (۲۰۰۷ م)	شایستگی ویژگی فردی قابل اندازه‌گیری و اتکاء (اعتماد) است که می‌تواند تفاوت بین مجریان برتر و متوسط یا مجریان اثربخش – ناکارآمد را نشان دهد.
ویلکاکس (۲۰۱۲ م)	شایستگی عبارت است از یک مهارت یا توانایی فردی که از تحلیل وظایف شغلی مشخص شده است.
زوزانا (۲۰۱۶ م)	شایستگی به‌عنوان توانایی افراد برای انجام فعالیت‌ها است.
وایت من (۲۰۱۸ م)	شایستگی عبارت است از دانش، مهارت و توانایی‌های تأثیرگذار بر وظایف اصلی شغل
اولریش و همکاران (۱۳۸۸)	شایستگی‌ها دانش، مهارت‌ها و رفتاری هستند که افراد در خلال انجام کارشان از خود نشان می‌دهند.
عارف و همکاران (۱۳۹۶)	شایستگی عبارت است از مجموعه‌ای از دانش‌ها، مهارت‌ها، توانایی‌ها، انگیزه‌ها، نگرش‌ها و خصیصه‌های یک فرد که در صورت وجود فرصت و امکانات مناسب منجر به عملکرد بالا در شغل یا موقعیت‌های خاص می‌گردد.

به‌طورکلی تحول مفهوم شایستگی را در قالب سه مکتب اصلی روان‌شناسی افتراقی[2]، روان‌شناسی آموزشی و رفتاری[3] و علوم مدیریت[4] می‌توان تبیین نمود:

۱. به نقل از ضرابی و همکاران (۱۳۹۱)

2. Differential Psychology
3.Educational and Behavioral Psychology
4.Management Sciences

۱. روان‌شناسی افتراقی (روان‌شناسی تفاوت‌های فردی): در این نوع روان‌شناسی بر تفاوت‌های انسانی و به‌ویژه توانایی‌هایی که به‌سختی توسعه داده می‌شوند، به‌مانند هوش، توانایی شناختی و فیزیکی، ارزش‌ها، ویژگی‌های شخصیتی و علایق تأکید می‌شود. در ذیل این چهارچوب، شایستگی‌ها به‌عنوان ویژگی‌های اصلی کارکنان تعریف می‌شود که با عملکرد مؤثر و اثربخش در یک شغل مرتبط هستند، کاربرد اصلی این رویکرد تعیین خصوصیات و ویژگی‌هایی است که منجر به عملکرد برتر می‌گردد.

۲. روان‌شناسی آموزشی و رفتاری: این چهارچوب بر تعیین طیف وسیعی از آموزش و توسعه شایستگی‌های لازم برای عملکرد موفق شغلی تأکید دارد. در این ماتریس بر به کارگیری ماتریس شایستگی آگاهانه تأکید می‌شود. در این ماتریس چهار مرحله روان شناسی به شرح ذیل برای یادگیری مهارت‌ها و فنون تعیین گردیده است:

الف) عدم شایستگی ناآگاهانه: در این مرحله فرد شایستگی‌های لازم برای انجام وظایف خود را دارا نمی‌باشد. علاوه بر این، در این مرحله فرد از عدم شایستگی خود بی اطلاع می‌باشد.

ب) عدم شایستگی آگاهانه: در این مرحله فرد شایستگی لازم برای انجام وظایف خود را دارا نمی‌باشد، لیکن خود بر این امر آگاه می‌باشد.

ج) شایستگی آگاهانه: در این مرحله فرد شایستگی لازم برای انجام وظایف خود را دارا می‌باشد و خود بر این امر آگاه می‌باشد.

د) شایستگی ناآگاهانه: در این مرحله فرد به شایستگی کامل در انجام وظایف دست یافته است، لذا نیازی به فکر کردن درباره آن ندارد. به عبارتی نیازی به مراجعه به خودآگاه وجود ندارد.

اهمیت این چهارچوب برای کارکنان تعیین شایستگی‌ها و اجرای برنامه‌های آموزشی و توسعه‌ای و حرکت از عدم شایستگی ناآگاهانه به شایستگی‌های آگاهانه است.

۳. علوم مدیریت: در رویکرد علوم مدیریت، بیش از افراد بر شغل تأکید می‌گردد. تعیین شایستگی‌ها اغلب با تحلیل شغل آغاز و با لیستی از دانش، مهارت، نگرش و ویژگی های شخصیتی خاتمه می‌یابد (ویلکاکس،۲۰۱۲).

در چهارچوب مفاهیم ارائه‌شده، برخی از پژوهشگران اقدام به ارائه مدل‌های متنوعی از شایستگی نموده‌اند. در این میان اسپنسر و اسپنسر (۱۹۹۳ م) با توجه به تعریف خود از شایستگی (ویژگی بنیادین کارکنان که با عملکرد اثربخش و یا برتر در یک شغل یا موقعیت مرتبط است)، پنج ویژگی به شرح ذیل را به‌عنوان شایستگی‌های اصلی تعیین نموده‌اند:

۱. **انگیزه‌ها:** چیزهایی که افراد درباره آن‌ها فکر می‌کنند و محرک کارهایشان است.
۲. **خصایص:** خصوصیات شخصیتی و نحوه واکنش افراد به شرایط و افراد.
۳. **خود مفهومی:** ارزش‌ها و نگرش‌های افراد.
٤. **مهارت:** توانایی انجام وظیفه‌ای خاص.
۵. **دانش:** اطلاعات درباره حوزه‌ای خاص.

طبق این نظریه مهم‌ترین ویژگی‌های شایستگی‌ها توانایی آن‌ها در پیش‌بینی عملکرد یا رفتار شغلی آینده بر اساس یکسری معیارهای استاندارد و پذیرفته‌شده است (چانگ و همکاران، ۲۰۱۱).

طبق نظر اسپنسر و اسپنسر، دانش و مهارت شایستگی‌های قابل مشاهده‌ای می‌باشند که در شغل مورد نیاز هستند، درحالی‌که ویژگی‌های دیگر اغلب شایستگی‌های مخفی می باشند و کمتر بدان‌ها توجه می‌شود، درحالی‌که این ابعاد عملکرد فرد را در شغل پیش می‌رانند (ضرابی و همکاران، ۲۳:۱۳۹۱).

شایستگی در حوزه امنیت سایبری

در کنار ابعاد تجهیزاتی و فنی، منابع انسانی متعهد و متخصص و نیز شهروندان آگاه نسبت به فضای سایبری، یکی از کلیدی‌ترین شروط موفقیت در تأمین امنیت سایبری می باشد (گروه اطلاعات و حفاظت اطلاعات، ۱۳۹۵). از این رو در سالیان اخیر کشورهای مختلف در راستای ارتقای قابلیت‌های مواجه و پاسخگویی مناسب به تهدیدات سایبری، اقدام به تدوین چهارچوب‌ها، الگوها و دستورالعمل‌هایی در راستای تعیین و توسعه شایستگی‌های مورد نیاز نیروی کار متخصص خود نموده‌اند. به‌طور مثال در کشور آمریکا طرح ملی آموزش امنیت سایبری، تدوین و اجرایی گردیده است. در این

چهارچوب از طبقات و حوزه‌های تخصصی برای سازمان‌دهی و دسته‌بندی انـواع مشـابه مشاغل استفاده شده است. هر حوزه تخصصی شامل وظایف، دانش، مهارت و توانایی‌هـا یا به عبارتی شایستگی‌های مشترک است. این چهارچوب ساختاری مرجع اسـت کـه بـه دنبال تبیین ماهیت بین رشته‌ای مشاغل سایبری می‌باشـد. ایـن چهـارچوب همچنـین بـه عنوان منبعی بنیادین برای توصیف و به اشتراک گذاشتن اطلاعات در مورد وظایف امنیت سایبری و دانش، مهارت‌ها و توانایی‌های[1] مورد نیاز برای انجام وظایفی است که می‌تواند وضعیت امنیت سایبری یک سازمان را تقویت کند. این چهارچوب چگـونگی شناسـایی، استخدام، توسعه و حفظ استعداد امنیت سایبری را بهبود مـی‌بخشـد. اولـین چهـارچوب نیروی کار امنیت سایبری در سپتامبر ۲۰۱۲ میلادی منتشر شد. در این طرح فعالیـت‌هـای امنیت سایبری در هفت طبقه ارائه ایمن، عملیات و نگهـداری، حفاظـت و دفـاع، تجزیـه وتحلیل، جمع‌آوری و اطلاعات، تحقیق و نظارت و راهبری سازمان‌دهی و دانش، مهارت و قابلیت‌های مورد نیاز برای انجام وظایف سایبری مشخص شـده اسـت. بـا اسـتفاده از طرح ملی آموزش امنیت سایبری، درک نیازهای سـازمانی و ارزیـابی میـزان ایـن نیازهـا تحقق می‌یابد و به سازمان در طراحی، اجرا و نظارت بر برنامه‌های موفق امنیت سـایبری کمک می‌کند (ویلیام و همکاران،۲۰۱۷).

مدل مفهومی تحقیق

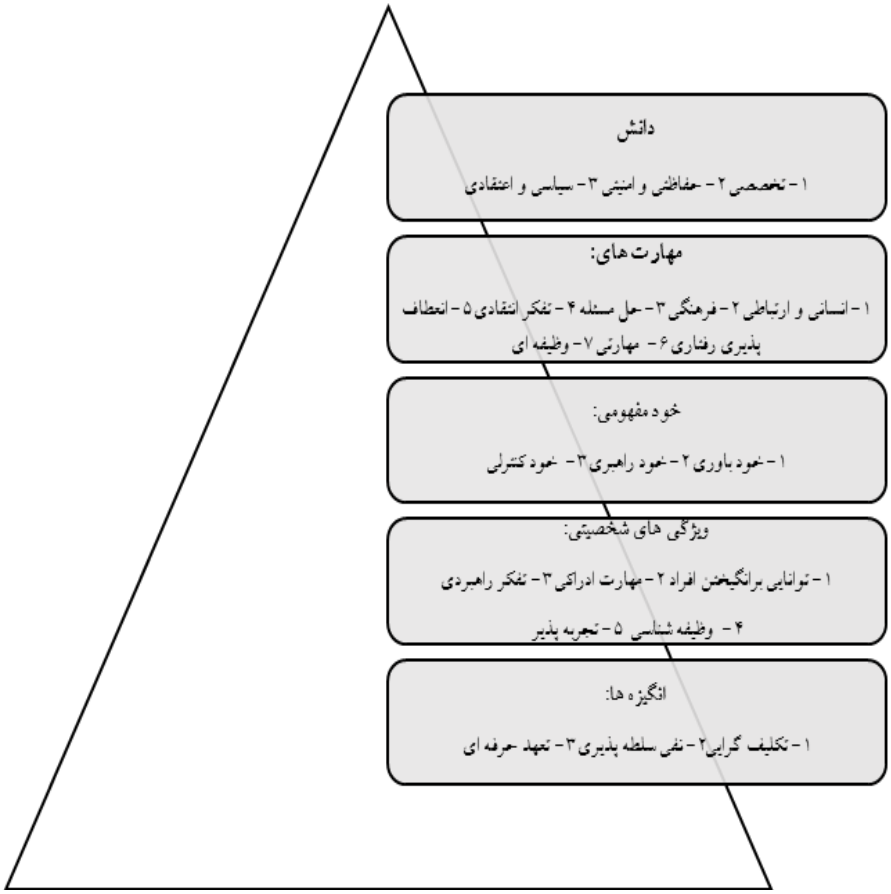
پس از کدگذاری مفـاهیم اسـتخراج‌شـده از مطالعـات اکتشـافی، مـدل شایسـتگی‌هـای کارکنان در حوزه امنیت سایبری مشتمل بر دو بعد و پنج مؤلفه مطـابق جـدول شـماره «۲» تدوین گردیده است.

1. KSAs

جدول ۲: ابعاد و مؤلفه‌های شایستگی کارکنان در حوزه امنیت سایبری

بعد	مؤلفه‌ها	برخی منابع مورد استناد (برگرفته از مطالعات اکتشافی)
شایستگی فنی و تخصصی	دانش سایبری (حوزه‌های رایانه، الکترونیک، مخابرات و مدیریت فناوری اطلاعات)	کواسیچ (۲۰۱٦)، کمیسیون ملی ارتقای امنیت سایبری (۲۰۱٦)، وزارت امنیت داخلی ایالات‌متحده (۲۰۱٦)، ریس و همکاران (۲۰۱۵)، توبی و همکاران (۲۰۱۱)، یزدانیان و همکاران (۱۳۹٦)، یوریس و همکاران (۲۰۱٦)، اداره مدیریت کارکنان (۲۰۱۸) ودانشگاه فونیکس (۲۰۱۸)
	مهارت‌های (انسانی و ارتباطی، فرهنگی، حل مسئله، تفکر انتقادی، انعطاف پذیری رفتاری، مهارتی و وظیفه‌ای)	محمدی و همکاران (۱۳۹٤)، کارانجا (۲۰۱۷)، هاشمی و همکاران (۱۳۸۹)، ژنگ (۲۰۱٦)، کلمبرگ و همکاران (۲۰۱۲)، جوزف و همکاران (۲۰۱٦)، استراتژی امنیت ملی آمریکا (۱۳۸۳)، توماس و همکاران (۱۳۹۲)، کواسیچ (۲۰۱٦)، کاویانی و همکاران (۱۳۹٦)، نایت (۲۰۱۵)
شایستگی عمومی	خودمفهومی (خودباوری، خودراهبری و خودکنترلی)	استیفن (۲۰۱۷)، هاشمی و همکاران (۱۳۸۹)، ژنگ (۲۰۱٦)، تسنگ و همکاران (۲۰۰۸)، رسته مقدم و همکاران (۱۳۹۰)، وندر (۲۰۰۷)، جمشیدی (۱۳۹٦) و معدنی و همکاران (۱۳۹۵)
	ویژگی‌های شخصیتی (توانایی برانگیختن افراد، مهارت ادراکی، تفکر راهبردی، وظیفه‌شناسی و تجربه‌پذیری)	مرکز ملی آمادگی حوادث و استراتژی امنیت سایبری ژاپن (۲۰۱۱)، کمیته پدافند غیر عامل کشور (۱۳۹٤)، هانسن و همکاران (۲۰۰۹) کواسیچ (۲۰۱٦)، خلیل و همکاران (۲۰۱۷)، آلگاراجا (۲۰۱۳) و وزارت امنیت داخلی ایالات‌متحده (۲۰۱٦)
	انگیزه‌ها (تکلیف‌گرایی، نفی سلطه‌پذیری و تعهد حرفه‌ای)	هاشمی و همکاران (۱۳۸۹)، محمدی و همکاران (۱۳۹٤)، وزارت نیروی دریایی آمریکا (۲۰۱۹)، موسویان (۱۳۹۷)، پورصادق (۱۳۹٦)، معدنی و همکاران (۱۳۹۵)، جمشیدی (۱۳۹٦)، فرهی و همکاران (۱۳۹۵) و عتیف و همکاران (۲۰۱٤)

بر اساس نتایج این بخش، مدل شایستگی کارکنان در حوزه امنیت سایبری بر اساس ساختار مدل شایستگی کوه یخی اسپنسر و اسپنسر در قالب دو بعد شایستگی‌های فنی (حرفه‌ای) و شایستگی‌های عمومی، پنج مؤلفه دانش، مهارت، خودمفهومی، ویژگی‌های شخصیتی و انگیزه‌ها و ۲٤ شاخص مطابق شکل «۱» تدوین گردید. (لازم به توضیح است دانش تخصصی شامل چهار شاخص دانش تخصصی در حوزه‌های رایانه، الکترونیک، مخابرات و مدیریت فناوری اطلاعات است).



شکل ۱: مدل مفهومی تحقیق

در بعد شایستگی فنی (حرفه‌ای)، مطابق مدل کوه یخی اسپنسر و اسپنسر، دو مؤلفه دانش (شامل دانش تخصصی در چهار حوزه مخابرات، الکترونیک، رایانه و مدیریت فناوری اطلاعات، دانش حفاظتی و امنیتی و دانش سیاسی و اعتقادی) و مهارت (شامل مهارت‌های انسانی و ارتباطی، فرهنگی، حل مسئله، تفکر انتقادی، انعطاف‌پذیری وظیفه‌ای، انعطاف‌پذیری مهارتی، انعطاف‌پذیری رفتاری) مورد توجه قرار گرفته است. در بعد شایستگی‌های عمومی نیز سه مؤلفه خودمفهومی (شامل خودباوری، خودکنترلی و خودراهبری)، ویژگی‌های شخصیتی (شامل توانایی برانگیختن افراد، مهارت ادراکی، تفکر راهبردی و تحول‌آفرینی، وظیفه‌شناس و مسئولیت‌پذیر و تجربه‌پذیر و پرشور بودن) و

انگیزه‌ها (شامل تعهد حرفه‌ای، تکلیف‌گرایی و نفی سلطه‌پذیری) به‌عنوان اجزای اصلی مدل مفهومی تعیین گردیده است.

روش‌شناسی تحقیق

مطالعه حاضر از منظر هدف نوعی تحقیق توسعه‌ای محسوب می‌گردد. لیکن با توجه به اینکه نتایج این تحقیق به‌منظور حل مسئله متداول در درون سازمان‌های متولی امنیت سایبری مورد استفاده قرار خواهد گرفت، می‌توان آن را گونه‌ای از تحقیقات کاربردی قلمداد نمود. همچنین تحقیق حاضر از منظر نحوه اجرا تحقیقی پس‌رویدادی و تک‌نمونه ای است که با استفاده از تحقیق میدانی، داده‌های مورد نیاز خود را جمع‌آوری و با استفاده از رویکرد کمی به تحلیل آن‌ها می‌پردازد.

در این پژوهش در گام نخست با بررسی پیشینه، نظریات و اسناد بالادستی، ابعاد، مؤلفه ها و شاخص‌های مدل شایستگی کارکنان در حوزه امنیت سایبری استخراج گردیده است. در مرحله دوم پس از تدوین پرسشنامه‌ای حاوی ۲٤ سؤال بر اساس مفاهیم مستخرجِ از مطالعات اکتشافی، به‌منظور تعیین روایی و پایایی، پرسشنامه در اختیار تعداد هشت نفر از خبرگان حوزه امنیت سایبری (با حداقل پنج سال اشتغال در مسئولیت مدیریت ارشد در حوزه امنیت سایبری، داشتن مدرک دکترای تخصصی، داشتن مدرک رشته مدیریت در حداقل یکی از مقاطع تحصیلی) قرار داده شد که نتایج از تأیید روایی ظاهری و ضریب آلفای کرونباخ معادل ۰/۸۹۱ برای کل پرسشنامه حکایت دارد. جامعه آماری پژوهش شامل دو گروه فرماندهان و مدیران عالی حوزه امنیت سایبری (ستاد کل نیروهای مسلح، ارتش جمهوری اسلامی ایران، سپاه پاسداران انقلاب اسلامی، نیروی انتظامی و سازمان پایداری ملی) و اساتید دانشگاهی و اعضای هیئت‌علمی دانشگاه‌های نظامی (دانشگاه عالی دفاع ملی، دانشگاه امام حسین (ع) دانشگاه مالک اشتر، دانشگاه پدافند هوایی خاتم‌الانبیاء(ص) و دانشکده فارابی) است که تعداد آن‌ها ۵۹ نفر برآورد گردید. با توجه به محدود بودن تعداد نفرات، از روش سرشماری جهت توزیع پرسشنامه‌ها و جمع‌آوری اطلاعات استفاده شد.

در مرحله تجزیه‌وتحلیل داده‌ها با استفاده از نرم‌افزارهای Spssو Smart pls، تعداد ٤٣ پرسشنامه دریافتی از خبرگان بررسی گردید.

یافته‌ها و تجزیه‌وتحلیل داده‌ها

الف) ویژگی‌های جمعیت‌شناختی پاسخگویان

با توجه به مفروضات تعیین‌شده جهت شناسایی خبرگان علمی و اجرایی، تعداد ۵۲ نفر جهت بررسی مقوله‌ها، ابعاد، مؤلفه‌ها و شاخص‌های استخراج‌شده از مطالعات اکتشافی تعیین گردیده‌اند. پس از هماهنگی‌های صورت‌گرفته و ارسال پرسشنامه‌های مربوطه، تعداد ٤٣ پرسشنامه جمع‌آوری شد و مبنای تحلیل داده‌ها قرار گرفت. ویژگی‌های جمعیت شناختی پاسخگویان به شرح جدول شماره ۳ است.

جدول ۳: ویژگی‌های جمعیت‌شناسی پاسخگویان

ردیف	ویژگی جمعیت‌شناسی	ابعاد	تعداد
۱	مدرک تحصیلی	دکترا	۲۹
		کارشناسی ارشد	١٤
۲	وابستگی سازمانی	دانشگاه دفاع ملی	٤
		دانشگاه مالک اشتر	۱
		دانشگاه امام حسین	۳
		دانشگاه خاتم‌الانبیاء (ص)	۳
		ستاد کل نیروهای مسلح	۵
		سازمان پایداری ملی	۵
		ارتش ج.ا.ا	۱۳
		سپاه پاسداران	٤
		نیروی انتظامی	۲

ب) بررسی مطلوبیت مؤلفه‌های مدل شایستگی کارکنان در حوزه امنیت سایبری

پس از شناسایی ابعاد، مؤلفه‌ها و شاخص‌های مدل شایستگی کارکنان در حوزه امنیت سایبری در گام اول از تحلیل داده‌ها، اجزای الگو به‌منظور تعیین مطلوبیت در معرض نقد و

ارزیابی خبرگان قرار گرفتند که نتایج تعیین مطلوبیت مؤلفه‌ها بر اساس تعداد شاخص‌ها در جدول ٤ ارائه شده است.

جدول ٤: محاسبه میانگین وزنی و مطلوبیت مؤلفه‌های مدل مفهومی تحقیق

مؤلفه‌ها	نقطه نظرات خبرگان									
	فراوانی نظرات					وزن مؤلفه‌ها		مطلوبیت مؤلفه‌ها		
	خ.ز	ز	م	ک	خ.ک	وزن کلی شاخص	میانگین وزنی	مطلوب	نسبتاً مطلوب	نامطلوب
دانش (٦)	١٩٠	٤٢	٢١	٥	٠	١١٩١	٤/٦٢	*		
مهارت (٧)	٢٢٢	٥٠	٢١	٦	٢	١٣٨٧	٤/٦١	*		
خودمفهومی (٣)	٨٨	٨	٨	١٢	١٣	٥٣٣	٤/١٣	*		
ویژگی شخصیتی (٥)	١٤٨	٢٣	١٩	١٣	١٢	٩٢٧	٤/٣١	*		
انگیزه ه (٣)	٩٤	١٥	١٢	٦	١	٥٧٩	٤/٤٩	*		

اعداد درج‌شده در جلوی هر مؤلفه، تعداد شاخص‌ها (سؤالات) است.

با عنایت به اینکه میانگین وزنی کلیه مؤلفه‌ها بالاتر از ٤ است، می‌توان نتیجه گرفت که از منظر خبرگان، کلیه مؤلفه‌های پیشنهادی مدل شایستگی کارکنان در حوزه امنیت سایبری دارای مطلوبیت لازم می‌باشند.

ج) برازش مدل مفهومی

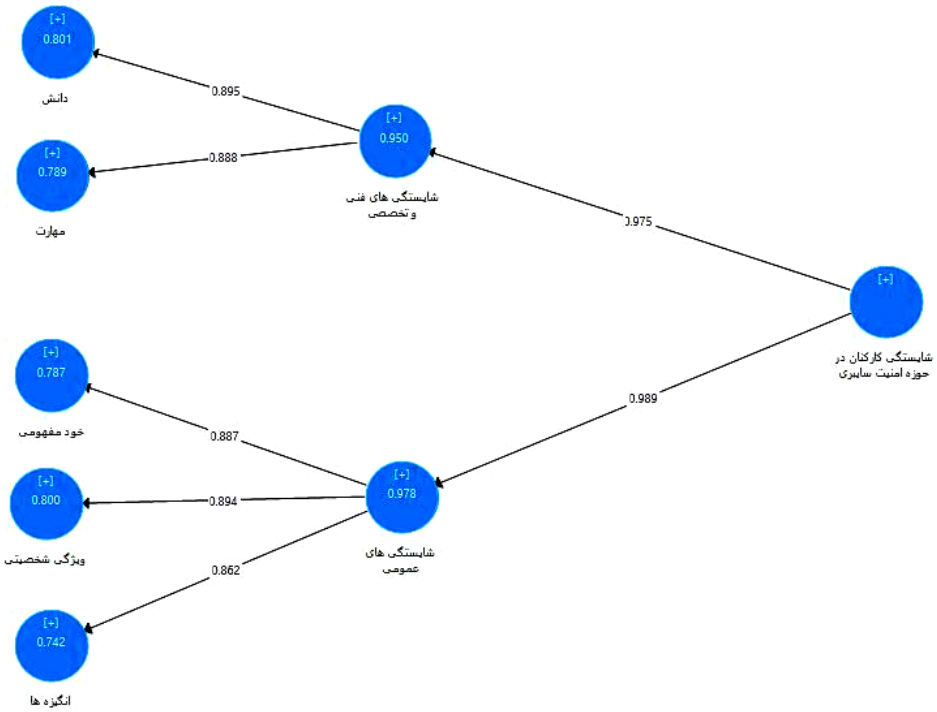
در این مرحله به‌منظور برازش مدل مفهومی از نرم‌افزار Smart pls استفاده شده است. این مرحله شامل برازش مدل اندازه‌گیری (رابطه گویه‌ها با سازه‌ها)، برازش مدل ساختاری (رابطه میان سازه‌ها) و برازش مدل کلی است که نتایج آن‌ها در جدول شماره ٥ ارائه شده است.

جدول ۵: نتایج برازش (اندازه‌گیری، ساختاری و برازش کلی) مدل مفهومی تحقیق

ابعاد /مؤلفه‌ها	برازش مدل اندازه‌گیری				برازش مدل ساختاری (متغیرهای درون‌زا)		برازش کلی مدل GOF≥0/3
	ضریب کرونباخ (α≥0/7)	مقادیر اشتراکی (c≥0/6)	پایایی ترکیبی (Cr≥0/7)	روایی همگرا (AVE≥0/5)	R2	Q2	
شایستگی کارکنان	۰/۹۵	۰/۹۵	۰/۹۵	۰/۵۱	متغیر برون‌زا		GOF=√(0/822×0/784)=0/72
شایستگی‌های حرفه‌ای	۰/۹۰	۰/۹۲	۰/۹۲	۰/۵۲	۰/۹۵	۰/٤٦٣	
شایستگی‌های عمومی	۰/۹۳	۰/۹٤	۰/۹٤	۰/۵۱	۰/۹۷۸	۰/٤٦٤	
دانش	۰/۸۵	۰/۸۷	۰/۹	۰/۷	۰/۸۰۱	۰/۵۲۱	
مهارت	۰/۷۹	۰/۸٤	۰/۸٦	۰/٦۲	۰/۷۸۹	۰/٤٦۱	
خودمفهومی	۰/۸۵	۰/۸۵	۰/۹۱	۰/۷۷	۰/۷۸۷	۰/۵۷۳	
ویژگی شخصیتی	۰/۸۱	۰/۸۲	۰/۸۹	۰/۷۳	۰/۸۰۰	۰/۵۵٤	
انگیزه‌ها	۰/٦٤	۰/۷۳	۰/۸٤	۰/۷۳	۰/۷٤۲	۰/۵۱۹	

بررسی برازش اندازه‌گیری و ساختاری ابعاد مدل مفهومی مؤید آن است که در وجوه مورد بررسی، کلیه ابعاد و مؤلفه‌ها حائز نمرات قابل قبول می‌باشند. صرفاً در خصوص ضریب آلفای کرونباخ، مؤلفه انگیزه‌های خروجی نرم‌افزار، کمتر از میزان قابل قبول است، لیکن با توجه به مقدار قابل قبول پایایی ترکیبی و مقادیر اشتراکی، این کاستی قابل اغماض است. نتایج برازش کلی مدل نیز نشان‌گر آن است که مدل در پیش‌بینی متغیرهای مکنون درون‌زا دارای قدرت و توانایی بالایی است. همچنین نتایج بررسی ضرایب استانداردشده

بار عاملی در شکل «۲» نشان از قابل قبـول بـودن بارهـای عـاملی بـین ابعـاد، مؤلفـه‌هـا و شاخص‌های مدل مفهومی دارد.



شکل ۲: نتایج بررسی بارهای عاملی مدل مفهومی تحقیق

نتیجه‌گیری و پیشنهاد

مطابق شکل (۳) مدل نهایی شایستگی کارکنان در حوزه امنیت سـایبری شـامل دو بعـد شایستگی‌های فنی و تخصصی و شایستگی‌های عمـومی اسـت. مطـابق نظریـه کـوه یخـی اسپنسر و اسپنسر، شایستگی‌های فنی و تخصصی به مصـداق قسـمت بیرونـی و نمایـان و شایستگی‌های عمومی قسمت زیرین و بنیادین مدل شایستگی است. نتایج تحقیق در حوزه شایستگی فنی و تخصصی با یافته‌ها و توصیه‌هـای اداره مـدیریت کارکنـان ایـالات‌متحـده (۲۰۱۸ م)، دانشگاه یونیکس (۲۰۱۸ م)، وزارت امنیـت داخلـی ایـالات‌متحـده (۲۰۱۷ م) و ویلیام و همکاران (۲۰۱۷ م) هم‌راستا است. یافته‌های پژوهش در حوزه ابعاد عمومی نیز بـا

نتایج تحقیقات کاویانی و همکاران (۱۳۹۷)، مرکز ملی آمادگی حوادث و راهبرد امنیت سایبری ژاپن (۲۰۱۱ م)، هاشمی و همکاران (۱۳۸۹) و هانسن و همکاران (۲۰۰۹ م) مطابقت دارد.

در عصر حاضر کارکنان شایسته کلید موفقیت سازمان‌ها و نهادها می‌باشند. از این رو استخدام و پرورش کارکنان شایسته بیش از گذشته مورد توجه قرار گرفته است. با این وجود مبرهن است که محور اصلی تحقق مطلوب فرآیندهای مدیریت منابع انسانی در گام اول مستلزم شناسایی شایستگی‌های اصلی و نهادینه‌سازی و به‌کارگیری آن‌ها در فرآیندهای تأمین و توسعه منابع انسانی است. با این وجود اسپنسر و اسپنسر معتقدند علیرغم آسان بودن توسعه و پرورش دانش و مهارت‌ها، سایر شایستگی‌ها (خود مفهومی، ویژگی‌های شخصیتی و انگیزه‌ها) به‌سختی پرورش می‌یابند. از این رو افراد در بدو ورود به خدمت باید حائز میزان قابل قبولی از شایستگی‌های مذکور باشند. بر این اساس و با توجه به یافته‌های تحقیق و به‌منظور تحقق مدل شایستگی کارکنان در حوزه امنیت سایبری، موارد ذیل پیشنهاد می‌گردد:

۱. در کنار آموزش طولی و عرضی متداول، تسهیم اطلاعات و تجارب بین کارکنان و نهادهای متولی امنیت سایبری، سازوکاری مؤثر در جهت ارتقای دانش و مهارت‌های کارکنان قلمداد می‌گردد. این مهم از طریق ایجاد سیستم جامع پردازش مرکزی جهت جمع‌آوری، یکپارچه‌سازی و تسهیم اطلاعات، قابلیت اجرایی خواهد داشت. رویکردی که ارتش آمریکا جهت جمع‌آوری و تسهیم اطلاعات رزمی تا سطوح تاکتیکی و رده گردان در قالب سیستم تحلیل منابع آزاد[1] از آن بهره‌برداری نموده است.

۲. توانایی شناخت و برقراری رابطه با سایر همکاران و ذی‌نفعان، یکی از شاخص‌های تأثیرگذار در ارتقای توان کارکنان در حوزه امنیت سایبری می‌باشد که از طریق آموزش مهارت‌های ارتباطی غیرکلامی، فن بیان، شنونده فعال بودن و هوش هیجانی در بین کارکنان تقویت می‌گردد.

1. All source analysis system

۳. با توجه به گستره عملیاتی فعالیت‌های کارکنان در حوزه امنیت سایبری ضروری است که کارکنان از فرهنگ‌ها، باورها و مبانی فلسفی حاکم بر سایر کشورها آگاهی داشته باشند. لذا پس از ارزیابی توانایی‌های کارکنان در ابعاد شناختی، فیزیکی و احساسی و انگیزشی، باید برنامه‌های آموزشی مناسب به‌منظور تقویت این شایستگی‌ها طراحی گردد.

٤. توسعه و ارتقای شایستگی‌هایی چون مهارت ادراکی، انعطاف‌پذیری رفتاری و... نیازمند استفاده از سازوکارهایی متفاوت از سازوکارهای آموزش رسمی و متداول در مؤسسات عالی است؛ زیرا در حقیقت اهداف و مأموریت دانشگاه‌ها متفاوت از سازمان‌ها و نهادهای متولی در حوزه‌های امنیتی و دفاعی است. در دانشگاه‌ها تمام فعالیت‌ها و برنامه‌ها در راستای آموزش افراد در حوزه‌های علمی و کاملاً تخصصی است، درحالی‌که در حوزه امنیت سایبری، تربیت افرادی فراتخصصی با توانایی نگرش چندوجهی و تحلیلی قدرتمند (کارکنان جنرالیست) باید مدنظر قرار گیرد. این اهداف تربیتی و آموزشی اغلب از طریق شبیه‌سازی تهدیدات و حملات سایبری با استفاده از سازوکارهایی چون تیم قرمز و آبی[1]، SDL[2]، بازی‌های مدیریتی، ایفای نقش و... تحقق می‌یابند.

۵. بر اساس نتایج تحقیق در میان شاخص‌های مهارت‌های اندیشه‌ورزی، تفکر راهبردی بیش از سایر مهارت‌ها مورد تأیید قرار گرفته است. مهارتی که به‌منظور نهادینه‌سازی آن در عرصه امنیتی و نظامی می‌توان از نرم‌افزارهای شبیه‌سازی جنگ‌های آینده و نیز نظریه تئوری بازی‌ها استفاده نمود.

٦. با عنایت به اینکه ایجاد نگرش و اعتقاد به مفاهیم و آموزه‌هایی چون تکلیف‌گرایی، شهادت‌طلبی و نفی سلطه‌پذیری غالباً در تربیت بلندمدت افراد ریشه دارد. ضروری است که راهبردهای اجرایی مناسب، چندسطحی و قابل تبدیل به مفاهیم ملموس با همفکری و مشارکت کلیه دستگاه‌های اجرایی تدوین شود و به اجرا درآید. با این

1.Red team & Blue team
2. Sceniro definition language

حال ازجمله راهکارهای کوتاه‌مدت این مهم شناسایی و جذب کارکنان (کارمندیابی) از طریق نهادهای انقلابی من‌جمله بسیج دانشگاه‌ها و مؤسسات عالی و مساجد محلات و پرورش آن‌ها در محیط متناسب است.

۷. در سالیان اخیر استفاده از ظرفیت‌ها و توانایی‌های کانون‌های ارزیابی در سنجش و توسعه شایستگی کارکنان، رویکردی متداول در بخش دولتی و خصوصی بوده است. رویکردی که در حوزه دفاعی و امنیتی غالباً به‌صورت موردی (صرفاً در هنگام استخدام) مورد توجه قرار می‌گیرد. با این حال با توجه به مأموریت‌ها و شایستگی‌های مورد نیاز کارکنان در حوزه امنیت سایبری، به نظر می‌رسد که ایجاد کانون‌های ارزیابی شایستگی به‌عنوان سازوکاری عملیاتی و علمی می‌تواند در توسعه شایستگی‌های کارکنان تأثیرگذار باشد.

شکل ۲: مدل نهایی تحقیق

فهرست منابع و مآخذ

الف. فارسی

- اولریش، دیو؛ بروک بنک، وین؛ جانسون، دنی؛ سندهولتر ،کورت و یانگر، جان(۱۳۸۸)، ***« شایستگی های منابع انسانی»***. مترجمان: مسعود بنش و افشین دبیری. تهران. انتشارات سرآمد. چاپ اول
- توماس، دیوید و کرایندکس(۱۳۹۲)، « ***هوش فرهنگی، مهارت های انسانی برای کسب و کار جهانی»***. مترجمان: ناصر میرسپاسی، احمد ودادی و اعظم دشتی. تهران. انتشارات میر.چاپ اول
- پورصادق، ناصر(۱۳۹٦)، شناسایی و تبیین فرهنگ سازمانی جهادی، ***فصلنامه پژوهش های مدیریت انتظامی***، سال دوازدهم، شماره ۲،صص ۱۷۵-۱۹۷
- پورعابدی، محمدرضا؛ وحید ، ضرابی؛ سجادی، حنان و رضی زهرا(۱۳۹۵)، طراحی مدل شایستگی چند بعدی مدیران و کارکنان، ***پژوهش های مدیریت منابع انسانی***، سال هشتم، شماره دوم،صص ۲۷-۵۲
- جمشیدی، محمد حسین و اسلامی، محسن(۱۳۹٦)، تفکر و فرهنگ بسیجی در اندیشه امام خمینی(ره)، ***دو فصلنامه مطالعات قدرت نرم***، سال هفتم، شماره ۱٦،صص ٤۲-٦٤
- رسته مقدم، آرش و عباس پور، عباس(۱۳۹۰)، طراحی مدل مفهومی یکپارچه ی سازمان یادگیرنده، ***رهیافتی نو در مدیریت آموزش***، شماره ٤،صص ۲۱-۵۵
- ضرابی، وحید؛ مداح، معصومه؛ رضی، زهرا و سجادی، حنان (۱۳۹۱)، ***توسعه منابع انسانی با رویکرد شایستگی در سازمان ها: مورد کاوی سازمان تنظیم مقررات و ارتباطات رادیوئی***. تهران. انتشارات جهاد دانشگاهی
- عارف، هادی و مرادی، سید عباس(۱۳۹٦)، شفاف سازی مفهوم" شایستگی "در مدیریت منابع انسانی با رویکرد تحلیل مفهومی، ***فصلنامه علمی-پژوهشی مدیریت سازمان های دولتی***، دوره ۵، شماره ۲ ،۱۳-۳۰
- فاضلی، حبیب الله و افضلی، توحید (۱۳۹٤)، دیپلماسی ایالات متحده در قبال جمهوری اسلامی ایران در دولت اوباما(با تاکید بر فضای سایبری)، ***دو فصلنامه مطالعات قدرت نرم***، شماره۱۲، صص۱۳۹-۱٦۰
- فرهی ، علی؛ سنجقی، محمد ابراهیم؛سلطانی، محمدرضا و محمدیان ، یداله (۱۳۹۵)،طراحی الگوی فرهنگ جهادی یکی از نهادهای انقلاب اسلامی، ***پژوهش‌های مدیریت منابع انسانی*** ، دوره ۸ شماره۲،صص ۵۳-۸۳.
- کاویانی، حسن؛ فتح آبادی، حسین و منوچهری، کمال(۱۳۹۷)، تاثیر انعطاف پذیری منابع انسانی بر دو سوتوانی سازمانی در یگان های نظامی، ***فصلنامه مطالعات منابع انسانی***، سال هشتم، شماره ۲۹،صص ۹۱-۱۱٦
- کمیته دائمی پدافند غیرعامل کشور(۱۳۹٤)، ***سند راهبردی پدافند سایبری کشور***، www.saramad.ir
- کمیسیون تدوین استراتژی امنیت ملی آمریکا (۱۳۸۳)، ***استراتژی امنیت ملی آمریکا در قرن ۲۱***. مترجمان: جلال

دهمشگی، بابک فرهنگی، ابوالقاسم راه چمنی. تهران. موسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر. چاپ چهارم

- گروه اطلاعات و حفاظت اطلاعات(۱۳۹۵)، راهبرد سایبری ترکیه: اصول و محورها، ***ماهنامه تخصصی مطالعات امنیت ملی***، سال سوم، شماره ٤٧و٤٨، صص٢٦-٤٥
- محمدی، ابوالفضل؛ فرهی، علی؛ سلطانی، محمدرضا و تارودی پور ،خدایار(۱۳۹٤)، طراحی و تبیین الگوی توسعه منابع انسانی یکی از سازمان های نیروهای مسلح، ***پژوهش های مدیریت منابع انسانی***، سال هفتم، شماره۱،صص ۲۱۲-۱۸۷
- معدنی، جواد؛ حسین پور ،داوود و یاری، معصومه(۱۳۹۵)، طراحی مدل فرهنگ جهادی مبتنی بر مبانی دینی و ارزش های انقلاب اسلامی در دانشگاه اسلامی(مورد مطالعه دانشگاه علامه طباطبایی)، ***مدیریت در دانشگاه اسلامی***، سال پنجم ، شماره ، ؛صص٤٩-٧١
- موسویان، سید علی(۱۳۹۷)، شاخصه های روحیه جهادی، ***فصلنامه اسلام پژوهان***، سال پنجم، شماره هفتم،صص ۸۳-٦٧
- هاشمی، حسین؛ علی اکبری، حسن؛ بازرگانی، محمد و نادری خورشیدی، علیرضا(۱۳۸۹)، طراحی الگوی آینده پژوهی در توسعه منابع انسانی(مورد: سپاه پاسداران انقلاب اسلامی)، ***پژوهش های مدیریت منابع انسانی***، سال۲، شماره۲،صص ٤٧-٧٠
- یزدانیان، حمید و جلالی فراهانی، غلامرضا(۱۳۹٦)، متغییرهای کلیدی منابع انسانی در تقویت دفاع سایبری جمهوری اسلامی ایران، ***فصلنامه امنیت ملی***، سال هفتم، شماره٢٦،صص ۱۲۷-۱٤۲

ب– انگلیسی

- Alagaraja , Meera .(2013). Mobilizing organizational alignment through strategic human resource development. ***Human Resource Development International***, 16(1), 74-93
- Atif, Ahmad &Sean, Maynard.(2014), Teaching information security management: reflections and experiences. ***Information Management & Computer Security***, 22 (5), 513-536
- Brilingaite, Agne ., Linas, Bukauskas & Aušrius, Juozapavicius .(2020). A framework for competence development and assessment in hybrid cybersecurity exercises. ***Computers & Security*** ,88 ,1-13
- Chung, Ruey-Gwo & Chien-Yao, Wu.(2011). The identification of personnel director's competency profile through the use of the job competence assessment method. ***African Journal of Business Management***, 5(2), 405-415
- Claudia, Ogrean., Mihaela, Herciu & Lucian, Belascu.(2009). Competency-Based Management and Global Competencies – Challenges for Firm Strategic Management, ***International Review of Business Research Papers***, 5 (4), 114-122

- Commission on enhancing national cybersecurity.(2016). ***Report on securing and growing the digital economy.*** available at: iapp.org/resources/article/report-on-securing-and-growing-the-digital-economy
- Department of Navy. (2019). ***Cybersecurity readiness review***, avaialable at: https://www.navy.mil/strategic/CyberSecurityReview.pdf
- Ferdinandus Jansen, Buiel P.P &Meiler T(2018), improving human capital for socs and csirts: a collective need for individual competencies, ***The Dutch National Cyber Security Centre (NCSC***)
- Fotis, Draganidis & Gregoris, Mentzas.(2006). Competency based management: a review of systems and approaches. ***Information Management & Computer Security***. 14 (1), 51-64
- Hansen, Carol D& Lee, Yih-teen .(2009).***The Cultural Context of Human Resource Development.*** Published by Palgrave Macmilllan
- Homeland.(2016).***Cybersecurity workforce development toolki***, at available: https://niccs.uscert.gov/sites/default/files/documents/pdf/cybersecurity_workforce_development_toolkit.pdf?trackDocs=cybersecurity_workforce_development_toolkit.pdf
- Kaushiki, Tripathi & Manisha, Agrawal.(2014). Competency Based Management In Organizational Context: A Literature Review**.** ***Global Journal of Finance and Management***, 6(4), 349-356.
- Khalil, M & Dirani ,Christine Silva Hamie .(2017). Human resource education in the Middle East region. ***European Journal of Training and Development***, 41 (2), 102 – 118
- Klimburg, Alexander .(2012). ***National Cyber Security Framework Manual***. NATO CCD COE Publication, Tallinn
- Knight, Jennine .(2015). Investing in Human Resource Development: Strategic Planning for Success in Academic Libraries, ***In Advances in Library Administration and Organization***, Published online: www.emeraldinsight.com/doi/abs/10.1108/S0732-067120150000033001
- Kovacich Gerald L(2016), ***The information systems security officer's guide Establishing and Managing a Cyber Security Program***, Third edition, Published by Elsevier
- National center of incident readiness and strategy for cybersecurity. (2011). ***Information Security Human Resource Development Program***, available at: www.nisc.go.jp/eng/pdf/hrd_pg_eng.pdfUnited
- Reece, R& Stahl, B.(2015).The professionalisation of information security: Perspectives of UK practitioners. ***computers & security***,48, 182 -195
- States Office of Personnel Management.(2018***). Interpretive Guidance for Cybersecurity Positions***, at available: https://www.opm.gov/policy-data-oversight/classification-qualifications/reference-materials/ interpretive -guidance- for cybersecurity-positions
- Stefan, Bauer, Edward, Bernroider & Katharina Chudzikowski. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. ***computers & security,*** 68,145–159

- Tobey , David & Michael , Assante. (2011). ***Enhancing the Cybersecurity Workforce.*** available at: www.researchgate.net/publication/220386260_Enhancing_the_Cybersecurity_Workforce
- Tseng, Chien-Chi & McLean, Gary .(2008). Strategic HRD practices as key factors in organizational learning. ***Journal of European Industrial Training***, 32(6),.418-432
- University of Phoenix.(2018***). Competency Models for Enterprise Security and Cybersecurity***, at available: http://www.apollo.edu/content/dam/apolloedu/microsite/security_industry/AEG-UOPX%20Security%20Competency%20Models%20report.pdf
- Vichita, Vathanophas & Jintawee ,Thai-ngam. (2007). Competency Requirements for Effective Job Performance in The Thai Public Sector. ***Contemporary Management Research***,3(1),45-70
- Whitman, Michael.(2018). Industry Priorities for Cybersecurity Competencies. ***Journal of The Colloquium for Information System Security Education (CISSE)***. 6(1), 1-21
- Wilcox, Yuanjing.(2012). An Initial Study to Develop Instruments and Validate the Essential Competencies for Program Evaluators (ECPE). ***A dissertation submitted to the faculty of the graduate school of the university of Minnesota***
- William,Newhouse., Keith, Stephanie., Scribner, Benjamin & Greg, Witte. (2017***). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework***, publication at: : https://doi.org/10.6028/NIST.SP.800-181
- Zeng, Kui .(2016***). Exploring cybersecurity requirements in the defense acquisition process***. A Dissertation Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Science Capitol technology university
- Zuzana, Skorková.(2016). Competency models in public sector, ***3rd International Conference on New Challenges in Management and Organization: Organization and Leadership, Dubai, UAE***