فصلنامهٔ علمی راهبرد دفاعی، سال بیستم، شمارهٔ ۷۸، تابستان ۱۴۰۱

فرمانده معظم کل قوا: «امروز پدافند در آرایش نیروهای مسلح در خط مقدم قرار می‌گیرد. در وضع کنونی آرایش نیروهای مسلح ما با اوضاع کشور و منطقه و با آنچه از مسایل جاری منطقه و کشور همه خوب می‌دانید در این آرایش، نیروی پدافند جزء خطوط مقدم اصلی است» (۱۳۹۶/۰۶/۱۲).

مقالهٔ پژوهشی: معرفی مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی ج.ا.ایران

20.1001.1.17351723.1401.20.78.1.9

علیرضا شفیعی[۱] مسعود باجلانی[۲] عباس ملکی[۳] محمودرضا شفیعی[۴]

تاریخ دریافت: ۱۴۰۰/۱۰/۰۲ تاریخ پذیرش: ۱۴۰۰/۱۲/۱۲

چکیده

پیچیدگی و گستردگی فضای سایبر و ارتباط حداکثری مأموریت‌های سازمان‌های امنیتی با این فضا، موجب فاصله گرفتن سازمان‌های امنیتی از دانش مطلوب سایبری شده است؛ بنابراین کاستن فاصله موجود نیازمند پرداختن به عوامل مؤثر در ارتقاء دانش سایبری بوده که پژوهش حاضر در پی شناسایی و کشف این عوامل می‌باشد. هدف از این پژوهش شناسایی و معرفی مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی است. جامعه آماری پژوهش، شامل افرادی از جامعه اطلاعاتی- امنیتی است که نسبت به دانش سایبری اشرافیت دارند. پژوهش حاضر به لحاظ هدف، کاربردی بوده که به روش میدانی نسبت به گردآوری اطلاعات از طریق مصاحبه، پرسشنامه، اسناد کتابخانه‌ای و پایگاه‌های اینترنتی اقدام شده است. با روش توصیفی ـ تحلیلی نسبت به تجزیه‌وتحلیل اطلاعات به‌دست آمده با استفاده از نرم‌افزار SPSS به‌این شکل که در قسمت آمار توصیفی از آماره‌هایی همچون فراوانی، میانگین، انحراف معیار، چولگی و کشیدگی و در بخش آمار استنباطی از آزمون کای‌مربع و آزمون فریدمن استفاده شده است. نتایج بیانگر آن‌است که در میان سه حوزه «سرمایه انسانی»، «ساختار آموزشی» و «فناوری‌های آموزشی»، توجه به «سرمایه انسانی» تاثیرگذارترین بعد در ارتقای دانش سایبری شناخته شده و شاخص «احساس نیاز افراد» در صدر سایر مؤلفه‌های این حوزه قرار گرفته است؛ در بعد «ساختار آموزشی»، «کاربردی بودن آموزش‌ها» در اولویت بالاتری نسبت به سایر موارد است و در حوزه «فناوری‌های آموزشی» نیز شاخص «طراحی نرم‌افزارهای آموزشی در بستر شبکه داخلی» بیشترین تاثیر را بر ارتقای دانش سایبری سازمان‌های امنیتی به خود اختصاص داد.

۱. کارشناس ارشد پدافند غیرعامل گرایش امنیت ملی، نویسنده مسئول: mt_121s@yahoo.com
۲. کارشناس ارشد حفاظت اطلاعات
۳. استادیار جغرافیای سیاسی دانشکده فارابی
۴. کارشناس ارشد پدافند غیرعامل گرایش امنیت ملی

واژگان کلیدی: آموزش؛ دانش سایبری؛ سرمایه انسانی؛ ساختار آموزشی؛ فناوری‌های آموزشی؛ سازمان‌های امنیتی.

مقدمه

فرماندهی معظم کل قوا(مدظله‌العالی) درباره فضای مجازی که جزء اصلی ساختار فضای سایبر است، می‌فرمایند: «فضای مجازی واقعاً یک دنیای رو به رشدِ غیرقابل توقّف است، یعنی واقعاً آخر ندارد؛ آدم هر چه نگاه می‌کند، آن چیزِ اوّلِ بلا آخر، فضای مجازی است. هر چه انسان پیش می‌رود در این فضا، این همین طور ادامه دارد. این یک فرصت‌های بزرگی در اختیار هر کشوری می‌گذارد، تهدیدهایی هم در کنارش دارد؛ ما بایستی کاری کنیم که از آن فرصت‌ها حدّاکثر استفاده را بکنیم، از این تهدیدها تا آن‌جایی که ممکن است خودمان را بر کنار نگه بداریم (بیانات در دیدار رئیس‌جمهور و اعضای هیأت دولت ۱۳۹۵/۰۶/۰۳).

امروزه شاهد هستیم دیگر فضای سایبر یک فضای تک بعدی وب سایتی نیست، امروز مخاطب بدون این که احساس کند در میان چندین وجه از اشکال سایبر دست و پا می‌زند. از آغاز قرن بیست‌ویکم به بعد توانایی نفوذ به وسیله فضای سایبری به مهم‌ترین منبع قدرت تبدیل شده است (سهیلی و خضرلو، ۱۳۹۷: ۳۷). حال با وضعیت اشاره شده شناخت این شرایط نیاز به آموزش دارد که این مهم با طی روندی مستمر امکان دارد. برنامه‌های آموزش کارکنان در یک سازمان می‌تواند نیاز به نیروی انسانی متخصص در آینده را نیز رفع کند و تضمینی برای حل مشکلات کارکنان باشد زیرا کارکنان در پرتو آموزش صحیح است که می‌توانند وظایف خود را به نحو مطلوب انجام دهند (فتحی و اجارگاه، ۱۳۷۶: ۴۳). با توجه به درگیر شدن مأموریت‌ها با فضای سایبر و چالش‌های موجود در این عرصه ضروری است که ریل آموزشی سازمانی تغییر یافته و مبتنی بر مهارت محوری و مأموریت پایه باشد و ارتقای دانش سایبری کارکنان را با عنایت جدی به عواملی هم‌چون سرمایه انسانی، ساختار آموزشی و فناوری آموزشی تبیین نمود. در چنین وضعیتی رصد و شناخت مستمر فرصت‌ها و تهدیدات سایبری از ضروریات است. بر این اساس تکیه بر دانش سایبری به مفهوم تولید آگاهی و درک محیط پیرامون که پایه طراحی و هدایت عملیات و

حفظ برتری در تمام ابعاد است به سازمان‌های امنیتی امکان می‌دهد که در خصوص کنترل تهدیدات و اشراف بر محیط عملیاتی اقدام نمایند.

۱. کلیات

۱-۱. بیان مسئله

در عصرحاضر شاهد بروز و ظهور آسیب‌ها و تهدیدات جدیدی در زمینه حفاظت از اسناد و اطلاعات، دارایی‌های اطلاعاتی، سرورها و تجهیزات شبکه‌ای، نفوذ به تجهیزات نوین نظامی و... هستیم (مردعلی و صالحی، ۱۳۸۹: ۶). تأمین دانش سایبری به‌موقع و دقیق به درک سازمان‌های امنیتی از دشمن و محیط عملیاتی کمک می‌نماید و ابزاری ضروری در دستیابی این سازمان‌ها به اهداف مورد نظر است. همچنین دانش سایبری، سازمان را در برابر تهدیدات پیش رو ایمن‌تر می‌سازد و ابهامات احتمالی در فعالیت‌ها را کاهش می‌دهد و موجب کم شدن غافلگیری در برابر دشمنان می‌شود و سازمان‌های امنیتی را قادر می‌سازد متناسب با برنامه‌های حریف، طرح‌های پیشگیرانه و مقابله‌ای خود را در مقابل تهدیدات پیش رو تنظیم کنند. حال برای رسیدن به این اشراف اطلاعاتی نیاز است که دانش سایبری کارکنان سازمان ارتقا یابد تا اهداف پیش گفته تحقق یابد. با رشد روزافزون فناوری و هژمونی فضای سایبر این برداشت شکل گرفت که تأمین امنیت فقط در استفاده از زور نیست بلکه اشرافیت براین فضا، تأثیر بسزایی در برهم‌زدن تعادل قدرت دارد و می‌تواند موجبات امنیت و یا ناامنی را فراهم کند. با توجه به پیچیدگی و گستردگی فضای سایبر و ارتباط حداکثری مأموریت‌های سازمان‌های امنیتی با این فضا، سازمان‌های موصوف هنوز تا رسیدن به دانش مطلوب سایبری فاصله دارند و این مهم نیازمند شناخت عوامل مؤثر در دانش سایبری می‌باشد؛ بنابراین این تحقیق در پی شناسایی و کشف این عوامل می‌باشد. نمونه‌ها و الگوهای پیاده‌سازی ارتقای دانش در سازمان‌های گوناگون به‌خصوص ابزارهای آن برای نیاز سازمانی و مطابق با ساختار و تشکیلات اداری آن طراحی می‌شوند و مزیت‌های رقابتی آینده در شکل توانایی سازمان‌های امنیتی در ارتقای دانش سایبری و برتری اطلاعاتی سایبرمحور جلوه‌گر خواهد بود. براین اساس دغدغه پژوهشگر این است

که عوامل مؤثر بر ارتقای دانش سایبری سازمان‌های امنیتی را شناسایی نماید تا بتوان در پیشگیری، کشف و خنثی‌سازی تهدیدات سایبری به صورت اثربخش عمل نمود.

۱-۲. اهمیت و ضرورت تحقیق

الف. اهمیت تحقیق

پرداختن به موضوع حاضر از آن جهت که به تقویت و توسعه زمینه مطالعات ایجابی در حوزه اطلاعات و امنیت در کشور کمک می‌نماید، دارای اهمیت است. افزون بر اینکه طرح این دیدگاه می‌تواند به فهم بهترسیاست‌های اطلاعاتی و امنیتی بازیگران در عصر حاضر کمک نموده و از این منظر نیز دارای اهمیت است.

از سوی دیگر باید اذعان نمود ارتقای دانش می‌تواند کارکنان را در جهت توانمندسازی و اجرای راهبردهای عملیاتی- اجرایی سازمان یاری دهد و سطح آموزش و انگیزش افراد را ارتقا داده و تمایل آنان را در جهت واگذاری برخی از مسؤلیت‌ها فراهم کند. به‌دلیل گستردگی خدمات اطلاعاتی، پویایی فعالیت‌ها و تنوع تهدیدهای ملی، منطقه‌ای و فرامنطقه‌ای و نقش راهبردی سازمان‌های امنیتی در مبارزه با این تهدیدات، ارتقای دانش سایبری می‌تواند تأثیر مثبت قابل توجهی در انجام رسالت و مأموریت‌ها داشته باشد و به‌منظور آگاهی مسؤلین و مدیران از مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری در بهبود عملکرد کارکنان نقش بارزی ایفا نماید.

ب. ضرورت تحقیق

مطالعات انجام شده در زمینه اطلاعات و امنیت گسترده بوده و شامل مباحث فنی، رفتاری، مدیریتی، فلسفی و خط‌مشی‌های سازمانی می‌شود که به حفظ اطلاعات و همچنین کاهش تهدیدها علیه دارایی‌های اطلاعاتی می‌پردازد(زافار و کلارک، ۲۰۰۹). بررسی ادبیات موجود نشان می‌دهد که تمرکز مطالعات بیشتر بر جنبه فنی حفظ اطلاعات بوده است و کمتر به جنبه انسانی و به‌ویژه آموزش نیروی انسانی توجه شده است؛ نیروی انسانی که مهم‌ترین نقش را در سازمان‌های امنیتی ایفا می‌کند. کارکنان ضعیف در یک سازمان امنیتی می‌توانند خسارات غیرقابل جبرانی را بر سازمان تحمیل نمایند. نبود نیروی انسانی آموزش

دیده و ماهر در سازمان‌های امنیتی عامل اصلی شکست‌ها بوده است. بر این اساس و با درنظر گرفتن اهمیت فراوان کارکنان سازمان‌های امنیتی باید گفت اگر می‌خواهیم نیروی انسانی در پیچیدگی‌های فرایند امنیتی زبردست باشد و در تولید اطلاعات اثربخش شود، باید به ارتقای دانش ایشان توجه نمود و در دنیای کنونی که دانش سایبری تعیین‌کننده است، عنایت ویژه‌ای به این موضوع شود. براین اساس شناخت عوامل موثر بر ارتقای دانش سایبری نیروی انسانی این سازمان‌ها امری ضروری است.

۱-۳. پیشینهٔ تحقیق

۱. بناهان و دیگران (۱۳۹۹) در پژوهشی با عنوان «مقایسه تطبیقی مؤلفه‌های تربیت شهروندی در فضای مجازی و حقیقی با نگاهی بر فرصت‌ها و تهدیدها»، به این نتیجه رسیدند که شهروند مطلوب در فضای مجازی علاوه بر کسب سواد رسانه‌ای و اطلاعاتی به مؤلفه‌هایی همچون آگاهی، پایبندی به ارزش‌ها و هنجارهای فرهنگی، قانون‌مداری، عدالت محوری، مشارکت‌پذیری و مسؤلیت‌پذیری آگاهانه نیازمند است. تربیت شهروند فضای مجازی به پرورش شهروند نقاد و تقویت میل به یادگیری مادام‌العمر کمک می‌کند تا با بهره گیری از ویژگی‌های متمایز فضای مجازی در جهت آموزش، پژوهش، گذران اوقات فراغت با کیفیت بالا، برای مشارکت فعال در امور اجتماعی راهگشا باشد. بنابراین به منظور کاهش تهدیدها و بهره‌مندی هرچه بیشتر از فرصت‌ها، شناخت مؤلفه‌های خاص تربیت شهروندی در فضای مجازی ضروری است.

۲. محمودزاده و اسماعیلی (۱۳۹۷) در پژوهشی با عنوان «الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح»، الگوی راهبردی صیانت امنیتی را در سه بعد شامل الف- بعد عوامل اصلی فضای سایبر نیروهای مسلح با مؤلفه‌هایی چون: داده‌ها و اطلاعات، کاربران، شبکه و زیرساخت، خدمات و نرم‌افزار؛ ب- بعد اهداف امنیتی فضای سایبر نیروهای مسلح با مؤلفه‌های محرمانگی، احراز هویت، یکپارچگی و صحت، دسترسی‌پذیری، انکارناپذیری و حفاظت از حریم خصوصی سازمان؛ و ج- بعد اقدامات و

راهکارهای صیانت امنیتی فضای سایبر نیروهای مسلح با مؤلفه‌های شناسایی منابع و دارایی‌های سایبری، محافظت، تشخیص و کشف، تحلیل، پاسخ و واکنش، بازیابی، بازدارندگی، مقابله موثر، نوآوری و تحول تدوین و معرفی نمودند.

۳. جان‌پرور و صالح‌آبادی (۱۳۹۵)، در پژوهشی با عنوان «توسعه سواد سایبری گامی در راستای حفاظت سایبری در عرصه پدافند غیرعامل کشور»، توسعه سواد سایبری را به‌عنوان گامی در راستای حفاظت سایبری در عرصه پدافندغیرعامل کشور جهت کاهش آسیب‌ها و تهدیدات فضای سایبر چه در حوزه جنگ‌های نظامی و چه در حوزه جنگ‌های نوین نظیر جنگ الکترونیکی مطرح می‌کنند. نتایج نشان‌داده که با افزایش آگاهی در میان افراد، جامعه، کارکنان سازمان‌ها و نهادهای دولت، نیروهای نظامی و انتظامی می‌توان تا حدود زیادی بستر لازم برای کاهش تاثیرات آسیب‌های سایبری در قالب حفاظت سایبری در عرصه پدافند غیرعامل کشور فراهم آورد.

۴. نایب‌پور و موسوی (۱۳۹۵) در پژوهشی با عنوان «تبیین نقش آموزش مبتنی بر تعلیم و تربیت اسلامی در پیشگیری از آسیب‌های فردی-روانی فضای سایبری»، به این نتیجه رسیدند که آموزش به‌عنوان راهکار پیشنهادی برای پیشگیری از آسیب‌های فضای سایبری می‌باشد. به‌سامان رساندن آموزش با استفاده از اصول اساسی تعلیم و تربیت اسلامی می‌تواند موجب ورود علاقه‌مندان به حوزهٔ فناوری برپایهٔ اندیشه‌های اسلامی و پیشگیری بهتر از آسیب‌پذیری شود که بهترین شکل این فرآیند در همکاری بین حوزهٔ علمیه، والدین و رسانه‌های تبلیغاتی با آموزش و پرورش صورت می‌گیرد.

۵. نظامی‌پور و مزینانی (۱۳۹۱)، در پژوهشی با عنوان «پارادایم‌شناسی فعالیت‌های پنهان سازمان‌های اطلاعاتی در فضای سایبری»، به این نتیجه رسیدند که نوع فعالیت‌های سازمان‌های اطلاعاتی تحت تاثیر فناوری‌های اطلاعات و ارتباطات ـ فضای سایبر ـ دچار تحول پارادایمی شده است و فعالیت‌های آشکار و پنهان این سازمان‌ها از عملیات اطلاعاتی محصول‌محوری و کسب حداکثر اخبار، به سمت‌وسوی عملیات اطلاعاتی تاثیرمحور و تولید و تبادل هدفمند اطلاعات سوق یافته است و جهت‌گیری آنها را به

سرمایه‌گذاری در حوزه‌های شناختی و عاطفی، هوشمندی اطلاعات و شبکه‌ای شدن آن، خارج شدن محصول اطلاعات از انحصار سازمان‌های اطلاعاتی (واسطه‌زدایی) تکیه بر مدیریت دانایی محور، اهمیت یافتن مجدد و مضاعف نقش نیروی انسانی، مجازی‌سازی فعالیت‌های اطلاعاتی، برونسپاری ماموریت‌های اطلاعاتی و تولید و توزیع اطلاعات نافذ با هدف تاثیرمحوری تبدیل نموده است.

بررسی پیشینه‌های تحقیق، نشانگر آن است که در چند دهه اخیر در مورد نقش دانش در توسعه پایدار، حقوق شهروندی و هم‌چنین عوامل موثر بر ارتقا اثربخشی آموزشی، مطالعات خوبی صورت گرفته است ولیکن به مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری پرداخته نشده است و شناسایی و تعیین این مؤلفه‌ها به‌ویژه در سازمان‌های امنیتی با توجه به ویژگی‌های خاص این سازمان‌ها مغفول مانده است. بنابراین شناخت مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری در سازمان‌های امنیتی برای اولین بار در این حوزه کاری صورت گرفته و با توجه به ویژگی‌های خاص سازمان‌های امنیتی، کاری نو و بدیع است. بر همین اساس با عنایت به نبود نظریه و الگویی متناسب با موضوع در مطالعات گذشته، به خبرگان فن مراجعه شد و با هدایت صاحبنظران، مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی در سه حوزه سرمایه انسانی، ساختار آموزشی و فناوری آموزشی دسته‌بندی شدند.

۱-۴. سؤال‌های تحقیق

۱-۴-۱. سوال اصلی

مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی ج.ا.ایران کدامند؟

۱-۴-۲. سوال‌های فرعی

(۱) مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی در حوزه سرمایه انسانی کدامند؟

(۲) مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی در حوزه ساختار آموزشی کدامند؟

(۳) مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی در حوزه فناوری آموزشی کدامند؟

۱-۵. هدف‌های تحقیق

۱-۵-۱. هدف اصلی

شناسایی مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی ج.ا.ایران.

۱-۵-۲. هدف‌های فرعی

(۱) شناسایی مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی در حوزه سرمایه انسانی؛

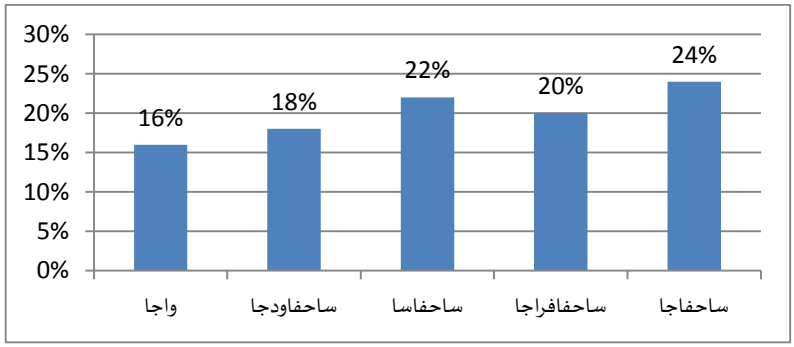
(۲) شناسایی مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی در حوزه ساختار آموزشی؛

(۳) شناسایی مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی در حوزه فناوری آموزشی.

۱-۶. روش شناسی تحقیق

پژوهش حاضر برحسب هدف کاربردی و بر اساس شیوه گردآوری داده‌ها، کمی از نوع تحلیلی توصیفی است. جامعه آماری این پژوهش، شامل افرادی از جامعه امنیتی (واجا، ساحفاودجا، ساحفاسا، ساحفافراجا و ساحفاجا به شرح نمودار ۱) که نسبت به دانش سایبری اشرافیت داشته و درک مناسبی از موضوع پژوهش داشته باشند به تعداد ۵۰ نفر برآورد شده است. به‌دلیل محدود بودن جامعه آماری، حجم نمونه به‌صورت تمام‌شمار درنظر گرفته شده است. برای گردآوری اطلاعات پژوهش از روش مطالعات کتابخانه‌ای (برای تدوین مبانی نظری و پیشینه پژوهش) و مطالعات میدانی (مصاحبه با صاحب‌نظران و

پرسشنامه پژوهشگر ساخته) استفاده شده است. برای انجام مصاحبه میدانی پژوهش با استفاده از روش گلوله برفی از بین جامعه آماری، نمونه‌هایی که دارای بیشترین اشرافیت و تخصص و سابقه لازم به قلمرو موضوع پژوهش را داشتند انتخاب و با ۱۲ نفر تا مرحله رسیدن به اشباع نظری، مصاحبه انجام پذیرفت. با استفاده از داده‌های حاصل از مطالعات انجام شده و مصاحبه عمیق حضوری در چندین نوبت با تعدادی از خبرگان اطلاعاتی- امنیتی در حوزه سایبر اقدام به پیاده‌سازی متن شد و متن پیاده شده، کدگذاری و شاخص‌های آن استخراج گردید. در ادامه پس از مشخص شدن مقوله‌های اصلی و فرعی، نتایج به‌دست آمده با استفاده از تجمیع، تقلیل و حذف برخی از شاخص‌های کم تعداد و همچنین ادغام برخی از شاخص‌ها در یکدیگر، مورد پالایش مجدد قرار گرفت و در نهایت شاخص‌های مورد نیاز بومی‌سازی گردید. روایی پرسشنامه به‌روش صوری و با مراجعه به خبرگان تائید شد و میزان پایایی آن با استفاده از ضریب آلفای کرونباخ مقدار (۹۷۵/.) به‌دست آمد، بنابراین پرسشنامه از ضریب اعتماد یا مطلوبی برخوردار بود. پرسشنامه نهایی بین جامعه آماری توزیع و تعداد ۴۵ پرسشنامه معتبر به‌دست آمد. برای تجزیه‌وتحلیل کمی داده‌ها از روش‌های آماری توصیفی و استنباطی و از نرم‌افزار SPSS استفاده شد. در قسمت آمار توصیفی از آماره‌هایی همچون فراوانی، میانگین، انحراف معیار، چولگی و کشیدگی و در بخش آمار استنباطی از آزمون کای‌مربع و برای رتبه‌بندی شاخص‌ها از آزمون فریدمن استفاده شد.



نمودار ۱- توزیع آماری جامعه نمونه

۲. ادبیات و مبانی نظری تحقیق

۲-۱. سازمان‌های امنیتی

سازمان امنیتی به سازمان‌ها، نهادها و ساختارهای اداری که وظیفه انجام فعالیت‌های امنیتی و تولید اطلاعات را دارند و به‌طور تخصصی برای جمع‌آوری اطلاعات پنهان سازمان یافته‌اند، اطلاق می‌شود (مکلین،۱۳۸۷: ۴۸۱). در این پژوهش سازمان‌های امنیتی شامل واجا، ساحفاودجا، ساحفاسا، ساحفافراجا و ساحفاجا می‌باشد. سازمان‌های امنیتی به‌عنوان ضرورتی حیاتی برای هر کشور در عرصه فعالیت‌های امنیتی، نقشی اساسی در پیشگیری از ناامنی، شناخت و خنثی‌نمودن تهدیدات، مقابله هدفمند با عوامل ناامنی و بهره‌برداری از فرصت‌ها دارند که فقدان کارکردهای اثربخش این سازمان‌ها، موجبات ضعیف‌شدن نهادهای حاکمیتی را فراهم خواهد نمود. داخلی‌ترین لایه ساختار امنیتی هر نظام سیاسی، سازمان امنیتی آن نظام است. زیرا هر نظام یا سازمانی با توجه به موضوع فعالیت، در معرض یک سری آسیب‌ها و تهدیداتی قرار دارد و این ساختار امنیتی است که ضمن شناسایی تهدیدات و آسیب‌پذیری‌ها، موجب اقتدار و اعتلای آن نظام یا سازمان خواهد شد(کلاهچیان و رحمتی نیا، ۱۳۹۶: ۷۲). با توجه به حساسیت و مهم بودن سنگر امنیت و خطری که همیشه از ناحیه نفوذ اطلاعاتی دشمن در کشور وجود دارد، رهبری معظم انقلاب این سازمان‌ها را بسیار مهم ارزیابی می‌نمایند.

۲-۲. فضای سایبر

فضای سایبر با فناوری جذاب و اغواگر خود، هژمونی را در حال پدیدآوردن است که مبتنی بر دانش و اطلاعات درونی، فضای تفوق و برتری نوینی را شکل داده است. فضای سایبر محیطی است مجازی و غیرملموس در فضای شبکه‌های بین‌المللی (این شبکه‌ها ازطریق شاهراه‌های اطلاعاتی مثل اینترنت به هم وصل هستند) که در این محیط تمام

اطلاعات راجع به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها و به طور کلی هر آن چه در کره خاکی به‌صورت فیزیکی و ملموس وجود دارد (به‌صورت نوشته، تصویر، صوت، سند) در یک فضای مجازی به‌شکل دیجیتالی وجود داشته و قابل استفاده و دسترس کاربران بوده و از طریق رایانه، اجزاء آن و شبکه‌های بین‌المللی به هم مرتبط می‌باشند(اشرافی مهابادی و توبی، ۱۳۹۶: ۱۰۷). در این مطالعه هرگونه استفاده از انواع فناوری‌های الکترونیکی و مخابراتی برای تبادل یا ارسال و دریافتِ اطلاعات، به‌منزله به‌کارگیری فضای سایبر است. سایبرنتیک علم مطالعه و کنترل مکانیزم‌ها در سیستم‌های انسانی- ماشینی (وکامپیوترها) است. فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. سند راهبردی پدافند سایبری کشور فضای سایبر را چنین تعریف نموده است: شبکه‌های وابسته به یکدیگر، از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده(جاگذاری شده)، کنترلگرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات می‌باشد. این فضا، ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه شده باشد(کمیته دائمی پدافندغیرعامل کشور، ۱۳۹۴: ۴).

۲-۳. مؤلفه‌های مؤثر در ارتقای دانش سایبری کارکنان در مبانی نظری و از دید صاحب‌نظران

بر اساس نظر خبرگان و صاحبنظران، مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی در سه حوزه «سرمایه انسانی»، «ساختار آموزشی» و «فناوری‌های آموزشی» دسته‌بندی شدند. در ادامه ضمن اشاره مختصری به مبانی نظری، دیدگاه صاحب‌نظران نیز در هر حوزه ارائه می‌گردد.

۱-۶-۲. سرمایه انسانی

سرمایه انسانی به میزان شایستگی‌ها و قابلیت‌های کارکنان اشاره دارد (ویگ، ۱۹۹۷). برخی اندیشمندان نیز آن را به دانش، مهارت‌ها، قابلیت‌ها، تعهد، دانش ضمنی، ایده‌ها و سلامت کارکنان نسبت می‌دهند (اسنل و بوهلاندر، ۲۰۰۷). چن و همکاران(۲۰۰۴) نیز سرمایه انسانی را به‌عنوان مبنای سرمایه فکری می‌دانند که به عواملی مانند دانش، مهارت، قابلیت، و نگرش کارکنان اشاره دارد و به بهبود عملکرد و افزایش سودآوری می‌انجامد (خلعتبری و دیگران، ۱۳۹۴: ۵۵). دانش به‌عنوان منبع نوآوری مستمر از راه نظرهای جدید، بهبود فرآیند و منبع واقعی مزیت رقابتی پایدار عمل می‌کند. بنابراین، توانایی به‌طور مؤثر مهار دانش مانند ایجاد دانش جدید و اشتراک آن درون سازمان، زمینه مدیریت دانش را تشکیل می‌دهد(میلار، لوکت و ماهون[۱] ۲۰۱۶: ۲). کاربرد دانش از راه تشویق، مهارت‌های خلاقانه و نوآورانه سرمایه انسانی کارکنان را تقویت می‌کند (بیراسنوا و رانگکار، ۲۰۰۸: ۱۱۶).

در فرایند مصاحبه، صاحب‌نظران اذعان نموده‌اند که همگام با رشد و تحول تهدیدات و آسیب‌پذیری‌های فضای سایبر، سازمان نیازمند نیروهای کارآمد در حوزه سایبر می‌باشد. به‌جهت این‌که در درجه اول این نیروها لازم است از سرمایه‌های سازمان محافظت نمایند و همچنین خود نیروها نیز از تهدیدات به‌روز با افزایش مهارت‌های لازم محفوظ بمانند. سرمایه انسانی می‌تواند ازطریق مهارت‌افزایی و افزایش انگیزش، استمرار و ارتقا یابد. وجود نیروی انسانی متعهد، متخصص، دلسوز، باتجربه و علاقه‌مند در حوزه سایبری و بهره‌گیری آنان در راستای مأموریت‌های محوله و همچنین به‌کارگیری آنان در بخش‌های مأموریتی و غیرمأموریتی می‌تواند باعث به‌جریان افتادن خون فنی سایبری در رگ‌های سازمان و ارتقای دانش سایبری سایر کارکنان گردد. در ادامه مهم‌ترین مواردی که صاحب‌نظران در حوزه سرمایه انسانی به‌آنها اشاره داشته‌اند ارائه می‌گردد:

۱. دسته‌بندی نیروی انسانی تحت آموزش بر اساس پارامترهایی نظیر سطح دانش فعلی، نوع مأموریت، میزان انگیزه برای یادگیری و سن.

۱ Millar, Lockett, & Mahon

۲. پیش‌بینی گزینه‌های تشویقی برای ارتقای سطح دانش سایبری کارکنان.

۳. ایجاد شرایط مختلف برای ارتقای سطح دانش سایبری کارکنان مانند: اعزام به دوره‌های آموزش مرتبط، بورس‌های تحصیلی و تشکیل جلسات گروهی برای ارایه ایده‌های جدید توسط کارکنان و طرح فناوری‌های نوین سایبری.

۴. جذب افراد هوشمند، خبره و خلاق در زمینه سایبری.

۵. فراهم کردن شرایط یادگیری کارکنان از یکدیگر.

۶. حمایت از پژوهش‌های حوزه سایبری کارکنان.

۷. احساس نیاز از سوی افراد.

۸. کیفیت سرمایه انسانی جذبی از نظر پایبندی به ارزش‌ها، علم و سطح تحصیلات.

۹. همدلی و همیت نیروی انسانی در رشد سازمان به لحاظ سایبری.

۱۰. وجود انگیزه در نیروی انسانی برای ارتقای دانش سایبری.

۱۱. تلاش نیروی انسانی برای مطالعه و مداقه در دانش سایبری روز.

۱۲. تلاش نیروی انسانی برای استفاده از دانش سایبری در اقدامات اطلاعاتی.

۱۳. تلاش هم‌افزای سرمایه انسانی در گفتمان‌سازی سایبر در سطح سازمان.

۱۴. توجه جدی به معیشت و حقوق و مزایای نیروی انسانی.

۲-۶-۲. ساختار آموزشی

ساختار سازمانی رابطه حاکم بر افراد و گروه‌هایی است که در جهت کسب اهداف تلاش می‌کنند و به دو بُعد ساختاری (رسمیّت، پیچیدگی، تمرکز) و محتوایی (اندازه، فناوری، محیط، استراتژی) تقسیم می شود. ابعاد ساختاری بیانگر ویژگی‌های درونی سازمان هستند و مبنایی به‌دست می‌دهند که می‌توان به‌کمک آنها سازمان‌ها را اندازه‌گیری یا با یکدیگر مقایسه کرد. ابعاد محتوایی مُعرِف کل سازمان و اهداف آن است که بر ابعاد ساختاری اثر می‌گذارد. بر همین اساس ساختار سازمانی باید به‌گونه‌ای طراحی شود که اطلاعات مناسب و به‌موقع در اختیار مدیران قرار گیرد (محمدی پیراسته و دیگران، ۱۳۹۱: ۲۰۴). هانگ و جیم وو (۲۰۱۰)، در مطالعه خود که در صنعت تایوان انجام دادند به این نتیجه

رسیدند که بین بهره‌وری دانش نیروی کار و ساختار سازمانی رابطه مثبت و معناداری وجود دارد (هوانگ و جیم، ۲۰۱۰: ۵۸۶). توجه به نوع ساختار حاکم بر سازمان و اصلاح آن در جهت افزایش بهره‌وری دانش ضرورت می‌یابد؛ در نتیجه بنا بر نقش ساختار سازمانی در ابعاد رفتاری و عملکردی نیروی انسانی، تحلیل نقش میانجی‌گر آن در رابطه با کار و بهره وری دانش نیروی کار اهمیّت می‌یابد تا جایی که ممکن است علت نداشتن کارکنان با انگیزه و بهره‌ور، نداشتن ساختار سازمانی مناسب باشد (اکبریان نسب و اسدی، ۱۳۹۹: ۲۳۶).

صاحب‌نظران در فرایند مصاحبه، اذعان نموده‌اند که در نظام آموزش ساختار، نقش اساسی و اصلی دارد. این قسمت در واقع هماهنگ‌کننده همه زیرمجموعه‌ها و گروه‌های وابسته در سازمان می‌باشد؛ در این حوزه سازمان باید بر اساس نیاز هر یک از کارکنان و با توجه به اولویت‌های مورد نظر ساختار آموزشی در سطح سازمان ترسیم گردد و همه کارکنان با توجه به آن ساختار در آموزش‌های سایبری شرکت نمایند. ساختار آموزشی به عنوان بستر ارتقای دانش سایبری می‌تواند مطرح باشد. پیش‌بینی ساختار آموزشی مناسب و متناسب با مأموریت‌های سازمانی از بدو ورود فراگیران و کارآموزان به مراکز آموزشی و پیش‌بینی محورها، سرفصل‌ها و مبانی آموزشی با تخصص سایبری در تمامی دوره‌ها، گروه‌ها، رشته‌ها و تمامی مقاطع تحصیلی در این مراکز می‌تواند مثمرثمر باشد. در ادامه اهم مواردی که صاحب‌نظران در حوزه ساختار آموزشی متذکر شده‌اند ارائه می‌شود:

۱. شناسایی نیازهای آموزش سایبری با توجه به نوع مأموریت، جامعه هدف و فناوری‌های سایبری موجود.

۲. طراحی دوره‌های کوتاه مدت و بلند مدت داخلی سازمانی.

۳. اعزام به دوره‌های برون سازمانی.

۴. تهیه محتوای آموزشی متناسب و مناسب برای دوره‌ها و دروس مختلف.

۵. طراحی دوره‌های مجازی و از راه دور .

۶. تصحیح روندها و بازخوردگیری.

۷. ایجاد زمینه‌های لازم برای افزایش دانش سایبری.

۸. ایجاد برنامه پیگیری لازم برای ارتقای دانش سایبری کارکنان از طریق پیگیری‌ها و بازدیدها.

۹. تدوین برنامه‌ها و سرفصل‌های آموزش برای سهولت دستیابی به هدف مورد نیاز.

۱۰. پیش‌بینی ضرورت‌های مورد نیاز برای آموزش سایبری کارکنان.

۱۱. هماهنگی و همکاری با نهادها و مؤسسات آموزشی برای ورود به علوم جدید سایبری به سازمان.

۱۲. تهیه متون و منابع مورد نیاز برای بهره‌برداری آموزشی کارکنان.

۱۳. سازماندهی و تعریف بوروکراسی لازم در حوزه سایبری.

۳-۶-۲. فناوری‌های آموزشی

تکنولوژی آموزشی تجزیه‌وتحلیل مسائل و شیوه‌های یادگیری و طراحی، توسعه، پیاده‌سازی، ارزیابی و مدیریت فرایندها و منابع آموزشی و غیرآموزشی به‌منظور بهبود یادگیری و عملکرد در مراکز مختلف آموزشی، محیط‌های آموزشی ویژه و مراکز شغلی است (پلویی و فرهادیان، ۱۳۹۹). پژوهش‌ها در این راستا نشان داده‌اند میزان اثربخشی نظام آموزشی مبتنی بر تکنولوژی‌های آموزشی به‌مراتب بیشتر از سیستم یادگیری سنتی بوده است (گورایا و عبدالله، ۲۰۲۰). استفاده از فناوری اطلاعات و ارتباطات سبب پیشرفت تحصیلی یادگیرندگان می‌شود (دائی‌زاده و دیگران، ۱۳۹۸؛ آنجلی و همکاران، ۲۰۱۷).

در فرایند مصاحبه صاحب‌نظران اظهار داشته‌اند که در عصر رقابتی حاضر که عدم بهره‌گیری مؤثر از فناوری‌های آموزشی، موجب پیشی گرفتن رقبا می‌گردد و یکی از حوزه‌هایی که با بهره‌گیری از فناوری دچار تحول بنیادین شده است، حوزه آموزش است. فناوری‌های آموزشی یکی از بسترهای ارتقای دانش سایبری است که از طریق طراحی نرم‌افزارها و برنامه‌های امن در بستر شبکه‌های داخلی نقش مؤثری در این زمینه خواهد داشت. فناوری‌های آموزشی واسطه انتقال مفاهیم، ابزار درک صحیح‌تر محتوای آموزشی و عامل اساسی در تسهیل یادگیری و در نتیجه تحقق اهداف آموزش است. بنابراین می‌توان آن را به‌عنوان یکی از مؤلفه‌های اصلی تأثیرگذار در ارتقای دانش سایبری کارکنان به‌شمار

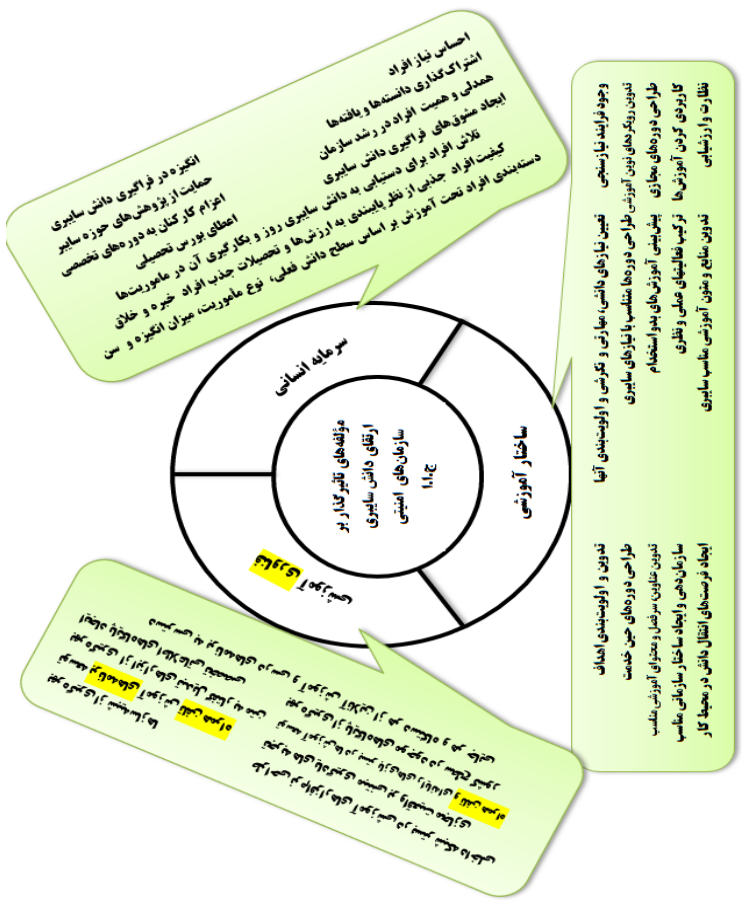
آورد. کاربرد این فناوری در آموزش سبب شده است تا محیط آموزشی به‌سوی مجازی شدن سوق پیدا کند. به‌دلیل این‌که در محیط یادگیری الکترونیکی، امکان تبادل اطلاعات و تعامل یادگیرندگان با هم و با یاددهنده در سطح بسیار بالایی است، یادگیری جذاب‌تر بوده و فرد ارزش آن چیزی را که یاد می‌گیرد چون منطبق با نیازهای اطلاعاتی اوست به‌خوبی درک می‌نماید. از انواع آموزش و یادگیری مبتنی بر فناوری اطلاعات می‌توان به مواردی چون: خود یادگیری، یادگیری از راه‌دور، کلاس مجازی، یادگیری گروهی و... اشاره نمود. در ادامه مهم‌ترین مواردی که صاحب‌نظران در حوزه فناوری‌های آموزشی برای ارتقای دانش سایبری به‌آنها تاکید نموده‌اند ارائه می‌گردد:

۱. ایجاد پایگاه‌های اطلاعاتی در دسترس.
۲. ایجاد فضای لازم برای شبیه‌سازی محیط‌های سایبری مورد نیاز.
۳. توسعه برنامه‌های آموزشی تلفن همراه.
۴. دسترسی به برنامه‌های آموزشی از هر دستگاه و هر جایی.
۵. توسعه و استفاده از ابزارهای تبدیل گفتار به متن.
۶. ارائه تجربیات یادگیری مبتنی بر واقعیت مجازی.
۷. ترغیب کارکنان به استفاده هر چه بیشتر از دانش سایبری.
۸. سرعت‌بخشی به فرآیند انتقال دانش سایبری با تکیه بر فناوری‌های نوین.
۹. ایجاد بستر و فضای مناسب برای استفاده بیشتر از فضای سایبر در پیشبرد مأموریت‌ها.

۲-۷. چارچوب مفهومی

با عنایت به نو بودن موضوع مورد مطالعه و نیافتن نظریه و الگویی متناسب با موضوع پژوهش در مطالعات گذشته، با مراجعه به خبرگان فن و با هدایت صاحبنظران، مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی در سه حوزه سرمایه انسانی، ساختار آموزشی و فناوری آموزشی دسته‌بندی شدند. پس از بررسی و مطالعه ادبیات موجود در

این سه حوزه، مصاحبه عمیق حضوری در چندین نوبت با ۱۲ نفر از خبرگان اطلاعاتی – امنیتی مشرف به حوزه‌های سایبری صورت گرفت. پس از پیاده‌سازی متن مصاحبه‌ها، نسبت به کدگذاری متن پیاده‌شده اقدام و شاخص‌های آن استخراج گردید. در ادامه پس از مقایسه با ادبیات نظری موجود در سه حوزه سرمایه انسانی، ساختار آموزشی و فناوری آموزشی، نتایج به‌دست آمده با استفاده از تجمیع، تقلیل و حذف برخی از شاخص‌های کم‌تعداد و همچنین ادغام برخی از شاخص‌ها در یکدیگر، مورد پالایش مجدد قرار گرفت و در نهایت نسبت به بومی‌سازی مؤلفه‌ها در حوزه‌های سرمایه انسانی، ساختار آموزشی و فناوری آموزشی اقدام شده است. سوال‌های پرسشنامه بر مبنای شاخص‌های این چارچوب طراحی شده است.



شکل ۱- چارچوب مفهومی پژوهش

۳. یافته‌های تحقیق و تجزیه‌وتحلیل آن‌ها

در این بخش فرآیندی تحلیلی بر داده‌های حاصل از سوال‌های پرسشنامه مستخرجه از چارچوب مفهومی که مبتنی بر بستر نظری و نتایج حاصل از مصاحبه صاحب‌نظران می‌باشد، انجام شده؛ به این ترتیب که در ابتدا با روش‌های آمار توصیفی و در ادامه با استفاده از تکنیک‌های آمار استنباطی به تحلیل متغیرهای تحقیق پرداخته‌ایم. در زیر برای نمونه ابتدا تجزیه‌وتحلیل توصیفی یکی از سؤال‌های مربوط به متغییرهای تحقیق ارائه و در ادامه تجزیه‌وتحلیل استنباطی و رتبه‌بندی عوامل مؤثر بر ارتقای دانش سایبری با استفاده از آزمون فریدمن پرداخته شده است.

۳-۱. تجزیه‌وتحلیل توصیفی

تاثیر احساس نیاز افراد بر ارتقای دانش سایبری

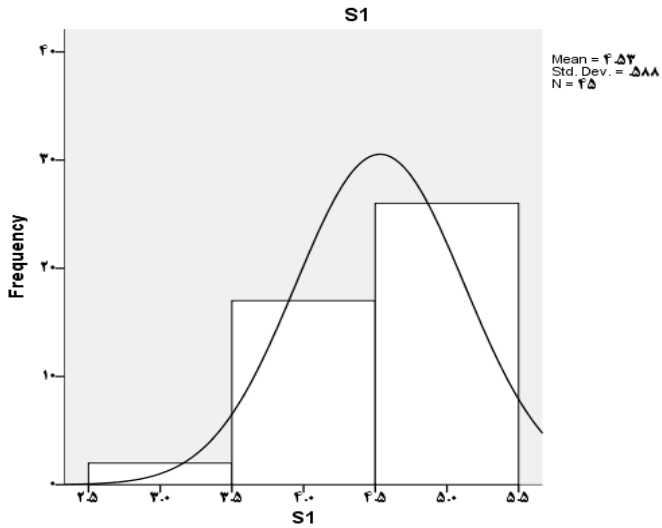
جدول۱- توزیع فراوانی «احساس نیاز افراد»

	Frequency	Percent	Cumulative Percent
متوسط	۲	۴/۴	۴/۴
زیاد	۱۷	۳۷/۸	۴۲/۲
خیلی زیاد	۲۶	۵۷/۸	۱۰۰
Total	۴۵	۱۰۰	

جدول۲- شاخصه‌های آماری «احساس نیاز افراد»

N	**Valid**	۴۵
	Missing	۰
Mean		۴/۵۳
Std. Error of Mean		۰/۰۸۸
Median		۵
Mode		۵
Std. Deviation		۰/۵۸۸
Variance		۰/۳۴۵
Skewness		-۰/۸۳۷
Std. Error of Skewness		۰/۳۵۴

Kurtosis	-۰/۲۳۳
Std. Error of Kurtosis	۰/۶۹۵
Sum	۲۰۴



نمودار۲- فراوانی شاخص «احساس نیاز افراد»

شاخصه‌های آماری (داده‌های جدول۲) بیانگر آن است که میانگین ۴/۵۳، میانه ۵ و انحراف استاندارد ۰/۵۸۸ است. توزیع از چولگی منفی برخوردار بوده و در نقطه اوج خود دارای پخی است. داده‌های جدول۱ توزیع فراوانی نشان می‌دهد که ۹۵/۶ درصد از پاسخ‌دهندگان در حد زیاد و خیلی زیاد معتقد هستند احساس نیاز کارکنان به فراگیری دانش سایبر تأثیر زیادی در ارتقای دانش سایبری ایشان دارد.

۲-۳. تجزیه‌وتحلیل استنباطی

در پژوهش حاضر، مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی در سه حوزه سرمایه انسانی، ساختار آموزشی و فناوری آموزشی دسته‌بندی شده‌اند. در ادامه

پس از تجزیه‌وتحلیل استنباطی شاخص‌های هر حوزه با آزمون کای‌مربع، به رتبه‌بندی شاخص‌های هر حوزه با استفاده از آزمون فریدمن پرداخته شده است.

۱-۲-۳. تجزیه‌وتحلیل مؤلفه‌های موثر بر ارتقای دانش سایبری سازمان‌های امنیتی حوزه سرمایه انسانی با استفاده از آزمون کای مربع

جدول ۳- آزمون کای مربع شاخص‌های حوزه سرمایه انسانی

	F1
Chi-Square	۳۶/۱۵۶a
df	3
Asymp. Sig.	۰/۰۰۰

F1	Observed N	Expected N	Residual
کم	۲	۱۱/۳	-۹/۳
متوسط	۵	۱۱/۳	-۶/۳
زیاد	۲۸	۱۱/۳	۱۶/۸
خیلی زیاد	۱۰	۱۱/۳	-۱/۳
Total	۴۵		

داده‌های جدول آزمون کای‌مربع بیانگر آن است که ارزش خی‌دوی مشاهده شده (۳۶/۱۵۶) در درجه آزادی ۳ معنی‌دار است، بنابراین بین فراوانی‌های مشاهده شده تفاوت معنی‌داری وجود دارد. در دو حوزه ساختار و فناوری آموزشی نیز نتایج آزمون کای‌مربع بیانگر وجود تفاوت معنی‌داری بین فراوانی‌های مشاهده شده بود که بواسطه محدودیت‌های موجود از آوردن جداول خودداری می‌شود.

۲-۲-۳. رتبه‌بندی مؤلفه‌های موثر بر ارتقای دانش سایبری سازمان‌های امنیتی حوزه سرمایه انسانی با استفاده از آزمون فریدمن

از میان شاخص‌های حوزه سرمایه انسانی ، «احساس نیاز افراد» با میانگین ۸/۶ و «حمایت از پژوهش‌های حوزه سایبر» با میانگین ۴/۵۱ به‌ترتیب بیشترین و کمترین میانگین

رتبه‌ای را به خود اختصاص داده‌اند. سایر ارزش‌های مربوط به میانگین رتبه‌ای متغیرها در جدول ۴ درج شده است.

جدول۴- اولویت‌بندی شاخص‌های حوزه سرمایه انسانی با آزمون فریدمن

Friedman Test

	Mean Rank
احساس نیاز افراد	۸/۶۰
انگیزه افراد در فراگیری دانش سایبری	۷/۶۷
تلاش افراد برای دستیابی به دانش سایبری روز و به‌کارگیری آن در ماموریت‌ها	۷/۵۲
کیفیت افراد جذبی از نظر پایبندی به ارزش‌ها و تحصیلات	۷/۲۳
جذب افراد خبره و خلاق	۶/۸۴
ایجاد مشوق‌های فراگیری دانش سایبری	۶/۶۱
اشتراک‌گذاری دانسته‌ها و یافته‌ها	۶/۳۳
همدلی و همیت افراد در رشد سازمان	۶/۳۱
اعزام کارکنان به دوره‌های تخصصی	۵/۷۷
اعطای بورس تحصیلی	۵/۴۲
دسته‌بندی افراد بر اساس سطح دانش فعلی، نوع مأموریت، میزان انگیزه و سن	۵/۲۷
حمایت از پژوهش‌های حوزه سایبر	۴/۵۱

Test Statisticsa

N	45
Chi-Square	۷۰/ 388
df	11
Asymp. Sig.	000/0

با توجه به این که ارزش خی‌دوی مشاهده شده ۷۰/۳۸۸ در درجه آزادی ۱۱ معنی‌دار است، بنابراین تفاوت بین میانگین‌های رتبه‌ای شاخص‌های حوزه سرمایه انسانی معنی‌دار است.

۳-۲-۳. رتبه‌بندی مؤلفه‌های موثر بر ارتقای دانش سایبری سازمان‌های امنیتی حوزه ساختار آموزشی با استفاده از آزمون فریدمن

از میان شاخص‌های حوزه ساختار آموزشی، «کاربردی کردن آموزش‌ها» با میانگین ۱۱/۳۹ و «طراحی دوره‌های مجازی» با میانگین ۵/۶۶ به‌ترتیب بیشترین و کمترین میانگین رتبه‌ای را به خود اختصاص داده‌اند. سایر ارزش‌های مربوط به میانگین رتبه‌ای متغیرها در جدول ۵ درج شده است.

جدول۵ – اولویت‌بندی شاخص‌های حوزه ساختار آموزشی با آزمون فریدمن

	Mean Rank
کاربردی کردن آموزش‌ها	۱۱/۳۹
ایجاد فرصت‌های انتقال دانش در محیط کار	۱۱/۲
ترکیب فعالیتهای عملی و نظری	۱۱/۱۱
طراحی دوره‌ها متناسب با نیازهای سایبری	۱۰/۹۷
تدوین عناوین، سرفصل و محتوای آموزشی مناسب	۱۰/۹۶
تعیین نیازهای دانشی، مهارتی و نگرشی و اولویت‌بندی آنها	۹/۳۳
تدوین منابع و متون آموزشی سایبری مناسب	۸/۷۹
نظارت و ارزشیابی و بهینه‌سازی شیوه‌های آموزش	۸/۵۹
وجود فرایند نیازسنجی	۸/۵۴
تدوین و اولویت‌بندی اهداف	۸/۵۱
سازماندهی و ایجاد ساختار آموزشی مناسب	۸/۴۳
طراحی دوره‌های حین خدمت	۸/۳۶
تدوین رویکردهای نوین آموزشی	۷/۹۰
پیش‌بینی آموزش‌های بدو استخدام	۷/۵۳
طراحی دوره‌های مجازی	۷/۴۱

Test Statisticsa

N	۴۵
Chi-Square	۱۰۱/ 381
df	۱۴
Asymp. Sig.	۰/۰۰۰

با توجه به این که ارزش خی‌دوی مشاهده شده ۱۰۱/۳۸۱ در درجه آزادی ۱۴ معنی‌دار است، بنابراین تفاوت بین میانگین‌های رتبه‌ای شاخص‌های حوزه ساختار آموزشی معنی‌دار است.

۴-۲-۳. رتبه‌بندی مؤلفه‌های موثر بر ارتقای دانش سایبری سازمان‌های امنیتی حوزه فناوری آموزشی با استفاده از آزمون فریدمن

از میان شاخص‌های حوزه فناوری‌های آموزشی، «طراحی نرم‌افزارهای آموزشی در بستر شبکه داخلی» با میانگین ۶/۶۸ و «بهره‌گیری از ابزارهای تبدیل گفتار به متن» با میانگین ۴/۳۷ به‌ترتیب بیشترین و کمترین میانگین رتبه‌ای را به خود اختصاص داده‌اند. سایر ارزش‌های مربوط به میانگین رتبه‌ای متغیرها در جدول ۶ درج شده است.

جدول۶- اولویت‌بندی شاخص‌های حوزه فناوری‌های آموزشی با آزمون فریدمن

	Mean Rank
طراحی نرم‌افزارهای آموزشی در بستر شبکه داخلی	6/68
توسعه آموزش‌ها در بستر بازی‌های رایانه‌ای و تلفن همراه	6/57
توسعه برنامه‌های آموزش تلفن همراه	6/42
دسترسی به برنامه‌های درسی و آموزش برخط از هر دستگاه و هر جایی	6/12
بهره‌گیری از شبیه‌سازها	5/68
ایجاد پایگاه‌های اطلاعاتی تخصصی	5/32
بهره‌گیری از پایگاه‌های موجود در سطح کشور	5/07
تجربه‌های یادگیری مبتنی بر واقعیت مجازی	4/63
بهره‌گیری از ابزارهای تبدیل گفتار به متن	4/37

Test Statisticsa

N	۴۵
Chi-Square	۴۰/ 725
df	۸
Asymp. Sig.	۰/۰۰۰

با توجه به این که ارزش خی‌دوی مشاهده شده ۴۰/۷۲۵ در درجه آزادی ۸ معنی‌دار است، بنابراین تفاوت بین میانگین‌های رتبه‌ای شاخص‌های حوزه فناوری‌های آموزشی معنی‌دار است.

۵-۲-۳. اولویت‌بندی مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی با آزمون فریدمن

مقایسه مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی، نشان‌دهنده آن است که حوزه «سرمایه انسانی» با میانگین رتبه‌ای ۲/۱۸ نسبت نسبت به حوزه «ساختار آموزشی» (۱/۹۴) و حوزه «فناوری‌های آموزشی» (۱/۸۸) از اولویت بیشتری برخوردار است.

جدول۷- اولویت‌بندی مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری با آزمون فریدمن

Ranks

	Mean Rank
f1	۲/ 18
f2	۱/ 94
f3	۱/ 88

Test Statistics[a]

N	۴۵
Chi-Square	۴/ 467
df	۲
Asymp. Sig.	۰/۱۰۷

۴. نتیجه‌گیری

۴-۱. جمع‌بندی

در این پژوهش تلاش گردید که با گردآوری اطلاعات نظری مورد نیاز، مراجعه به خبرگان و تحلیل آماری آنها، با استفاده از روش علمی به شناسایی و معرفی مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی پرداخته شود، تا بتوان گامی بلند در

راستای جلوگیری از غافلگیری در برابر دشمنان، تسهیل در امر تصمیم‌گیری، رفع ابهامات احتمالی در فعالیت‌ها، ارتقای درک افراد از محیط عملیاتی دشمن و پیش‌بینی شیوه و شگردهای حریف، برداشته و با کنترل تهدیدات و اشراف بر محیط اطلاعاتی و عملیاتی نسبت به تنظیم برنامه‌های پیشگیرانه و مقابله‌ای خود در مقابل تهدیدات اقدام نمود. آنچه روند پژوهش نشان می‌دهد دستیابی به اهداف پژوهش حاصل شده است.

در پاسخ به سوال اول یعنی «مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی در حوزه سرمایه انسانی کدامند؟» یافته‌های تحقیق نشان از آن دارد که عواملی همچون: «جذب افراد خبره و خلاق»، «کیفیت افراد جذبی از نظر پایبندی به ارزش‌ها و سطح تحصیلات»، «احساس نیاز از سوی افراد»، «انگیزه افراد در فراگیری دانش سایبری»، «اشتراک‌گذاری دانسته‌ها و یافته‌ها»، «همدلی و همیت افراد»، «تلاش افراد برای دستیابی به دانش سایبری روز و به‌کارگیری آن در ماموریت‌ها»، «ایجاد مشوق‌های فراگیری دانش سایبری»، «اعطای بورس تحصیلی»، «اعزام کارکنان به دوره‌های تخصصی»، «حمایت از پژوهش‌های حوزه سایبر» و «دسته‌بندی افراد تحت آموزش بر اساس عواملی چون سطح دانش فعلی، نوع مأموریت، میزان انگیزه برای یادگیری و سن» بر ارتقای دانش سایبری سازمان‌های امنیتی تاثیرگذارند.

در پاسخ به سوال دوم یعنی «مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی در حوزه ساختار آموزشی کدامند؟» باید اذعان نمود که عواملی مانند: «وجود فرایند نیازسنجی»، «تعیین نیازهای دانشی، مهارتی و نگرشی و اولویت‌بندی آنها»، «تدوین و اولویت‌بندی اهداف آموزشی»، «طراحی دوره‌ها متناسب با نیازهای سایبری»، «طراحی دوره‌های حین خدمت»، «طراحی دوره‌های مجازی»، «پیش‌بینی آموزش‌های بدو استخدام»، «تدوین عناوین، سرفصل و محتوای آموزشی مناسب»، «کاربردی کردن آموزش‌ها»، «ترکیب فعالیت‌های عملی و نظری»، «تدوین رویکردهای نوین آموزشی»، «تدوین منابع و متون آموزشی سایبری مناسب»، «نظارت و ارزشیابی»، «سازمان‌دهی و ایجاد ساختار آموزشی

مناسب» و «ایجاد فرصت‌های انتقال دانش در محیط کار» بر ارتقای دانش سایبری سازمان‌های امنیتی تاثیرگذار هستند.

و در نهایت در پاسخ به سوال سوم یعنی «مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی در حوزه فناوری‌های آموزشی کدامند؟»، نتایج نشان دادند که عواملی همچون: «طراحی نرم‌افزارهای آموزشی در بستر شبکه داخلی»، «توسعه آموزش‌ها در بستر بازی‌های رایانه‌ای و تلفن همراه»، «توسعه برنامه‌های آموزش تلفن همراه»، «دسترسی به برنامه‌های درسی و آموزش برخط از هر دستگاه و هر جایی»، «بهره‌گیری از شبیه‌سازها»، «ایجاد پایگاه‌های اطلاعاتی تخصصی»، «بهره‌گیری از پایگاه‌های موجود در سطح کشور»، «تجربه‌های یادگیری مبتنی بر واقعیت مجازی» و «بهره‌گیری از ابزارهای تبدیل گفتار به متن» در این حوزه بر ارتقای دانش سایبری سازمان‌های مؤثرند.

در میان شاخص‌های حوزه «سرمایه انسانی» ، سه شاخص «احساس نیاز از سوی افراد»، «انگیزه افراد در فراگیری دانش سایبری» و «تلاش افراد برای دستیابی به دانش سایبری روز و به‌کارگیری آن در ماموریت‌ها» به‌ترتیب بیشترین میانگین رتبه‌ای را به خود اختصاص داده‌اند و از اهمیت بیشتری برخوردارند.

در میان شاخص‌های حوزه «ساختار آموزشی»، سه شاخص «کاربردی کردن آموزش‌ها»، «ایجاد فرصت‌های انتقال دانش در محیط کار» و «ترکیب فعالیتهای عملی و نظری» به‌ترتیب بیشترین میانگین رتبه‌ای را به خود اختصاص داده‌اند، به‌این مفهوم که در ارتقای دانش سایبری سازمان‌های امنیتی جایگاه بالاتری را کسب نموده‌اند.

در میان شاخص‌های حوزه «فناوری‌های آموزشی» نیز، سه شاخص «طراحی نرم‌افزارهای آموزشی در بستر شبکه داخلی»، «توسعه آموزش‌ها در بستر بازی‌های رایانه‌ای و تلفن همراه»، «توسعه برنامه‌های آموزش تلفن همراه» به‌ترتیب بیشترین میانگین رتبه‌ای را به خود اختصاص داده‌اند و دارای اهمیت بیشتری هستند.

در مجموع با مقایسه مؤلفه‌های تاثیرگذار بر ارتقای دانش سایبری سازمان‌های امنیتی، شاهد بالاتر بودن میانگین رتبه‌ای شاخص‌های حوزه «سرمایه انسانی» نسبت به

شاخص‌های حوزه «ساختار آموزشی» و حوزه «فناوری‌های آموزشی» بوده که بیانگر اهمیت ویژه «سرمایه انسانی» می‌باشد.

۴-۲. پیشنهادهای اجرایی

با عنایت به نتایج حاصل شده، در راستای ارتقای دانش سایبری سازمان‌های امنیتی پیشنهاد می‌گردد موارد زیر مورد توجه و اقدام قرار گیرند:

۱. با توجه به جایگاه و ارزش بالای «سرمایه انسانی» به این عامل و شاخص‌های این حوزه عنایت ویژه‌ای گردد؛ در این زمینه پیشنهاد می‌گردد:

الف. با برگزاری جلسات توجیهی و جلب توجه کارکنان به اهمیت موضوع، احساس نیاز به فراگیری دانش سایبری در وجود افراد شعله‌ور گردد و با اولویت نسبت به اجرایی شدن این مهم در راستای نیازمندی سازمانی اقدام شود.

ب. با هر روش ممکن به صورت هدفمند انگیزه افراد در فراگیری دانش سایبری تقویت و از تلاش‌های ایشان در راستای دستیابی به دانش سایبری روز و به‌کارگیری آن در ماموریت‌ها تقدیر شود.

ج. نهایت تلاش معطوف به جذب افراد خبره و خلاق شده و به کیفیت افراد جذبی از نظر پایبندی به ارزش‌ها و اعتقادات و همچنین سطح تحصیلات و تخصص افراد در این زمینه توجه شود.

د. با ایجاد مشوق‌های لازم نسبت به فراگیری دانش سایبری و اشتراک‌گذاری دانسته‌ها و یافته‌ها در این حوزه اقدام و جو صمیمیت، همدلی و همیت افراد تقویت گردد.

۲. در حوزه «ساختار آموزشی» پیشنهاد می‌گردد:

الف. ضمن ایجاد ساختار آموزشی مناسب و تدوین فرایند نیازسنجی نسبت به تهیه و اولویت‌بندی اهداف آموزشی اقدام و نیازهای دانشی، مهارتی و نگرشی تعیین و اولویت‌بندی گردند.

ب. افزون بر پیش‌بینی آموزش‌های بدو استخدام نسبت به طراحی دوره‌های حین خدمت به‌صورت حضوری و همچنین مجازی متناسب با نیازهای سایبری اقدام شود.

ج. در تدوین عناوین، سرفصل و محتوای آموزشی مناسب و همچنین تدوین منابع و متون سایبری مناسب ضمن ترکیب فعالیت‌های عملی و نظری، به کاربردی بودن محتوی توجه ویژه شده و نظارت و ارزشیابی همیشه مورد توجه قرار گیرد.

د. فرصت‌های انتقال دانش در محیط کار فراهم گردد.

۳. در حوزه «فناوری‌های آموزشی» نیز پیشنهاد می گردد:

الف. با استفاده از ظرفیت بومی نسبت به طراحی نرم‌افزارهای آموزشی در بستر شبکه داخلی اقدام نمود.

ب. توجه ویژه‌ای به توسعه آموزش‌ها در قالب بازی‌های رایانه‌ای و تلفن همراه گردد.

ج. شرایط برای دسترسی به برنامه‌های آموزشی برخط از هر دستگاه و در هر مکانی فراهم گردد و همچنین توسعه برنامه‌های آموزشی تلفن همراه در دستور کار قرار گیرد.

د. برای کاهش هزینه‌های آموزش عملی، از شبیه‌سازها بهره‌برداری شود.

هـ. برای داشتن اشرافیت اطلاعاتی ضمن ایجاد پایگاه‌های اطلاعاتی تخصصی از ظرفیت پایگاه‌های اطلاعاتی سطح کشور نیز بهره‌برداری شود.

در پایان به‌نظر می‌رسد، بیشتر مؤلفه‌های اشاره شده در این پژوهش برای سازمان‌های خصوصی و انتفاعی هم مفید و کارساز باشد ولیکن مؤلفه‌هایی همچون «کیفیت افراد جذبی از نظر پایبندی به ارزش‌ها» به‌دلیل کمرنگ شدن اعتقادات به‌ویژه در سازمان‌های خصوصی، «طراحی نرم‌افزارهای آموزشی در بستر شبکه داخلی با استفاده از ظرفیت بومی» به‌دلیل بالا بودن هزینه طراحی و ساخت نرم‌افزارهای بومی و «بهره‌برداری از ظرفیت پایگاه‌های اطلاعاتی سطح کشور ضمن ایجاد پایگاه‌های اطلاعاتی تخصصی برای داشتن اشرافیت اطلاعاتی» به‌دلیل عدم دسترسی برای سازمان‌های غیرامنیتی قابل استفاده نخواهد بود.

۴-۳. پیشنهادهایی برای پژوهش‌های آتی

۱. هر یک از مؤلفه‌های شناسایی شده موثر بر ارتقای دانش سایبری سازمان‌های امنیتی می‌تواند در پژوهش مستقلی بررسی شوند. به‌عنوان نمونه، « تأثیر بوروکراسی سازمانی بر ارتقای دانش سایبری سازمان»؛ «تأثیر طراحی دوره‌های مجازی بر ارتقای دانش سایبری»؛ « سازوکار طراحی سامانه نظارت و ارزشیابی مؤثر بر ارتقای دانش سایبری کارکنان» و ... .

۲. همچنین با توجه به تفاوت‌های موجود در نوع ماموریت سازمان‌های امنیتی با سازمان‌های خصوصی، انتفاعی و حتی نظامی می‌توان تحقیق مشابهی در این سازمان‌ها انجام داد.

*****

فهرست منابع

الف. منابع فارسی

۱. اشرافی مهابادی، محمود و توبی، فرنوش(۱۳۹۶)، **پیشگیری وضعی از جرم جاسوسی سایبری**، فصلنامه مطالعات حقوق، پاییز۱۳۹۶، شماره ۱۴.

۲. اکبریان نسب، الهام و اسدی، حسین (۱۳۹۹)، بررسی ارتباط مثبت در کار و بهره وری دانش نیروی کار با نقش میانجی ساختار سازمانی (مطالعه موردی :شرکت خطوط لوله و مخابرات نفت خوزستان)، همایش بهبود و بازسازی سازمان ها و کسب و کارها، تابستان ۹۹، دوره ۱.

۳. بناهان، مریم، داوودیان، لیلا و ستاری، علی (۱۳۹۹)، **مقایسه تطبیقی مؤلفه‌های تربیت شهروندی در فضای مجازی و حقیقی با نگاهی بر فرصت‌ها و تهدیدها**، مجله اندیشه های نوین تربیتی، زمستان ۱۳۹۹، دوره شانزدهم، شماره ۴.

۴. پلوئی، لیلا و فرهادیان، فائزه،۱۳۹۹،**کاربرد مؤلفه های تکنولوژی آموزشی در منابع اصلی برنامه ریزی درسی**، https://civilica. com/doc/1024912

۵. جان‌پرور، احمد وصالح آبادی، ریحانه(۱۳۹۵)، **توسعه سواد سایبری گامی در راستای حفاظت سایبری در عرصه پدافند غیرعامل کشور**، فصلنامه پدافند غیر عامل و امنیت، پاییز ۱۳۹۵، سال پنجم – شماره ۱۶.

۶. خلعتبری معظم، مریم، امیری، حامد، اسکندری، ابراهیم و روزبهانی، علی(۱۳۹۴)، **نقش سرمایه انسانی در توسعه ظرفیت خلق دانش سازمانی**، فصلنامه مطالعات منابع انسانی، سال پنجم، زمستان ۹۴، شماره ۱۸.

۷. دائی‌زاده، حسین، حسین زاده، بابک و غزنوی، محمدرضا (۱۳۹۸)، **بررسی نقش(ICT) بر عملکرد تحصیلی دانش آموزان دوره متوسطه**، فصلنامه رهبری و مدیریت آموزشی دانشگاه آزاد اسلامی واحدگرمسار، زمستان ۱۳۸۹، سال چهارم، شماره ۴.

۸. سهیلی، حمیدرضا و حسین خضرلو، (۱۳۹۷)، **درک تهدیدات موجود در فضای سایبری**، فصلنامه ترجمان نظامی، دانشگاه افسری امام علی (ع)، شماره ۱۶، تهران، دانشگاه افسری امام علی (ع).

۹. صالحی‌نژاد، سیدحسین، (۱۳۷۹)، نقش آموزش در افزایش بهره‌وری نیروی انسانی، انتشارات پیام دریا، شماره ۴۵.

۱۰. عاملی، سید سعیدرضا (۱۳۹۰)، **رویکرد قضایی به آسیب‌ها، جرائم و قوانین و سیاست‌های فضای مجازی**، انتشارات امیرکبیر، چاپ اول.

۱۱. فتحی واجارگاه، کورش، درآمدی بر برنامه‌ریزی آموزش ضمن خدمت کارکنان، (۱۳۷۶)، تهران، انتشارات سرآمد کاوش.

۱۲. کلاهچیان، محمود و رحمتی نیا، روح اله (۱۳۹۶)، تبیین پدیده فلاتزدگی شغلی در کارکنان سازمانهای امنیتی، فصلنامه علمی پژوهشی پژوهش‌های حفاظتی-امنیتی، دانشکده امام هادی (ع) دانشگاه جامع امام حسین سال ششم، شماره ۲۲، ۵۵-۹۰.

۱۳. کمیته دائمی پدافندغیرعامل کشور، (۱۳۹۴)، سند راهبردی پدافند سایبری کشور.

۱۴. مردعلی، محسن و صالحی، محمود، ملاحظات پدافند غیرعامل فاوا، (۱۳۸۹)، سازمان فناوری اطلاعات ایران.

۱۵. محمدی پیراسته، سید محمدباقر، جلیلیان، حمیدرضا و میرزایی، حبیب (۱۳۹۱)، **رابطه سرمایه فکری و بهره‌وری در صنعت بانکداری (مطالعه موردی :بانک های استان لرستان)**، فصلنامه پول و اقتصاد، شماره ۷.

۱۶. محمودزاده، ابراهیم و اسماعیلی، کیوان (۱۳۹۷)، **الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح**، مجله امنیت ملی، زمستان ۱۳۹۷، سال هشتم، شماره ۳۰.

۱۷. مک‌لین، این (۱۳۸۷)، فرهنگ علوم سیاسی آکسفورد، ترجمه حمید احمدی، تهران، نشر میزان.

۱۸. نایب‌پور، علی و موسوی، سیدمحمدرضا (۱۳۹۵)، **تبیین نقش آموزش مبتنی بر تعلیم و تربیت اسلامی در پیشگیری از آسیب‌های فردی-روانی فضای سایبری**، فصلنامه پژوهش‌های اطلاعاتی و جنایی، تابستان ۱۳۹۵، سال یازدهم، شماره ۲.

۱۹. نظامی‌پور، قدیر و مزینانی، احمد (۱۳۹۱)، **پارادایم شناسی فعالیت‌های پنهان سازمان‌های اطلاعاتی در فضای سایبری**، فصلنامه پژوهش‌های حفاظتی و امنیتی، پاییز ۱۳۹۱، شماره ۳.

ب. منابع انگلیسی

۱. Angeli, C. , Howard, S. K. , Ma, J. , Yang, J. , & Kirschner, P. A. (2017). Data mining in

۲. Birasnav, M. and Rangnekar, S. (2008), "A conceptual model of human capital creation", in Chundawat, D. S. , Saxena, K. and Bhadu, S. S. (Eds), Managing Global ompetition: A Holistic Approach, Macmillan India, New Delhi.

۳. educational technology classroom research: Can it make a contribution?. Computers & Education, 113, 226-242. https://doi. org/10. 1016/j. compedu. 2017.

۴. Guraya, S. Y. , & Abdalla, M. E. (2020). Determining the effectiveness of peer-assisted learning in medical education: A systemic review and meta-analysis. Journal of Taibah University Medical Sciences. https://doi. org/10. 1016/j. jtumed. ۲۰۲۰.

۵. Huang, Y. , Jim Wu, Y. , 2010. Intellectual capital and knowledge productivity: The Taiwan biotech industry. Management Decision, 48(4.

۶. Millar-Schijf, C. C. , Lockett, M. , & Mahon, J. F. (2016). Knowledge Intensive Organisations: On the Frontiers of Knowledge Management: Guest Editorial. *Journal of Knowledge Management*, *20*(5).

۷. Snell, S. A. and Bohlander, G. W. (2007), Human Resource Management, Thomson South-Western, Mason, OH.

۸. Wiig, K. M. (1997), "Integrating intellectual capital and knowledge management", Long Range Planning, Vol. 30 No. 3.

۹. www. trendone. Com.

۱۰. Zafar H, Clark JG (2009) Current state of information security research in IS. Communications of the Association for Information Systems.