## چکیده

**نیروی کار متخصص یکی از مهم‌ترین سرمایه‌های امنیت فناوری اطلاعات به شمار می‌رود که امروزه بخش خصوصی و دولتی در سرتاسر دنیا در حال رقابت برای جذب این افراد هستند. کشور ما نیز مطابق نظر کارشناسان با کمبود نیروی متخصص امنیت سایبر مواجه است که می‌تواند موجب بروز آسیب‌های مختلف و خطرناکی شود. پژوهش حاضر در تلاش است که برای رویارویی با این مشکل در کشور راهکارهایی ارائه دهد.**

**برای یافتن راهکارها بعد از مطالعه منابع مرتبط با کارشناسان حوزه امنیت سایبر مصاحبه نیمه ساخت‌یافته صورت پذیرفته و نتایج با روش تحلیل مضمون استقرایی تحلیل شد. بدین ترتیب ۲۱ راهکار و ۵ راهبرد شناسایی شدند سپس راهبردهای به دست آمده به وسیله روش‌های تحلیل سلسله مراتبی فازی و راهکارها به وسیله تحلیل اهمیت-عملکرد اولویت‌بندی شدند.**

**مطابق نتایج به‌دست‌آمده، راهبردهای حفظ و نگهداری نیرو، ارتقای دوره‌های آموزشی از اولویت بیشتری نسبت به سایر راهبردها برخوردار هستند. همچنین با توجه به وضعیت فعلی کشور، توجه به طرح‌های ترکیبی آموزشی-استخدامی، اجرای طرح‌های ارزیابی و استعدادیابی، برگزاری رویدادهای مرتبط با حوزه امنیت سایبر، اجرای طرح‌های با مخاطب دانش‌آموزی، قانون‌گذاری مناسب و ارتقای سطح الزامات امنیتی از موارد دارای اهمیت بیشتر ارزیابی شده است.**



کلید واژه:

***کمبود متخصص امنیت سایبر، توسعه نیروی کار، روش تحلیل سلسله مراتبی فازی، تحلیل اهمیت- عملکرد***


*بررسی راهکارهای مقابله با کمبود نیروی متخصص امنیت فضای سایبر در کشور*


***محمد فتحیان(نویسنده مسئول)***
***استاد، گروه تجارت الکترونیکی، دانشکده مهندسی صنایع، دانشگاه علم وصنعت ایران، تهران، ایران***
*fathian@iust.ac.ir*

***مهدی عبدالحمید***
***استادیار، گروه مدیریت و فلسفه علم و فناوری، دانشکده مهندسی پیشرفت، دانشگاه علم و صنعت ایران، تهران، ایران***
*mahdi.abdolhamid@gmail.com*

***محمدرضا رفیعی***
***دانشجوی کارشناسی ارشد مدیریت فناوری اطلاعات، دانشکده مهندسی پیشرفت، دانشگاه علم و صنعت ایران، تهران، ایران***
*rafiei_m@pgre.iust.ac.ir*



***تاریخ ارسال:۹۹/۰۸/۰۱***
***تاریخ پذیرش:۹۹/۱۱/۳۰***


## مقدمه

امروزه با گسترش فناوری اطلاعات به حوزه‌های مختلف زندگی بشر ازجمله اقتصاد، کسب‌وکار، حکمرانی و غیره، لزوم توجه به امنیت این فناوری، افزایش یافته است. گزارشات موجود در سرتاسر دنیا مؤید این موضوع است که عدم توجه به امنیت سایبر خطرات متعددی را متوجه جوامع مختلف کرده است. کارشناسان معتقدند کمبود نیروی کار متخصص امنیت سایبر، یکی از مهم‌ترین مشکلاتی است که کشورها برای تأمین امنیت سایبری خود با آن روبرو هستند.

نیروی متخصص امنیت سایبر، کسی است که توانایی به‌کارگیری دانش پیشرفته و مهارت‌ها را در شرایط سخت یا جدید کاری دارا می‌باشد [۱]. به عبارت دیگر این افراد کسانی هستند که از دانش پیشرفته و تجربه عملی در به‌کارگیری امنیت برخوردار هستند و می‌توانند راه‌حل‌هایی که در منابع نیستند را اولویت‌بندی و به کار ببندند [۲]. به دلیل چند تخصصی بودن و ماهیت مفاهیم این حوزه، تربیت یک متخصص امنیت سایبر بنا بر نظر کارشناسان امری زمان‌بر و پرهزینه است و در برخی از حوزه‌ها نیازمند داشتن ویژگی‌های خاص شخصیتی در افراد نیز می‌باشد. این دشواری در ساخت تا جایی است که برخی معتقدند متخصصین برجسته کسانی هستند که چندان ساختنی نیستند و باید سراغ راهکارهای مناسبی برای یافتن این افراد رفت. این افراد کسانی هستند که حتی از الگوهای متفاوت رضایت شغلی نسبت به نیروهای عادی امنیت سایبر پیروی می‌کنند [۳].

اگرچه توسعه تکنولوژی و تولید ابزارهای خودکار موجب کاهش ریسک‌های امنیتی شده است اما متخصصین در حوزه امنیت با توانایی بالا هستند که کلید مقابله، تشخیص و بازیابی در برابر حملات

هستند [۳]. این افراد در واقع ارزشمندترین دارایی امنیت سایبر هستند و هرچه اهمیت امنیت فضای سایبر بیشتر می‌شود، میزان توجه به این دارایی نیز بیشتر می‌شود [٤].

اهمیت توسعه نیروی کار امنیت سایبر تا آنجاست که در اسناد حاکمیتی برخی از کشورها، مانند آمریکا، انگلستان و فرانسه، به این موضوع به صراحت اشاره شده است، برای نمونه در سند استراتژی ملی سایبر ایالات‌متحده [٥] که در سال ۲۰۱۸ به امضای رئیس‌جمهور این کشور رسیده است، برنامه‌های توسعه نیروی کار سایبر به عنوان یکی از راهبرهای کلان مطرح شده است و برای آن اولویت‌های اقدامی تعریف شده است.

این موضوع در اسناد بالادستی کشور ما نیز مطرح شده است. در سند راهبردی پدافند سایبر کشور در ذیل بخش "مأموریت پدافند سایبری کشور"، "آموزش و تربیت سرمایه‌های انسانی در حوزه سایبری" از مأموریت‌های پدافند سایبری کشور شمرده شده است و همچنین " آموزش، تربیت و توانمندسازی سرمایه‌های انسانی کارآمد متناسب با اقتضائات حال و آینده پدافند سایبری" از "اهداف کلان در افق چشم‌انداز پدافند سایبری کشور" به حساب آمده است. همچنین در بخش "موضوعات اساسی راهبردی پدافند سایبری کشور"، " ایجاد تناسب و کفایت سرمایه‌های انسانی" نیز از موضوعات اساسی برشمرده شده است.

در حال حاضر بخش خصوصی و دولتی در سرتاسر جهان بر سر منابع محدود متخصصان امنیت در بین نیروی کار جهانی در حال رقابت هستند [٤]. این موضوع هم از بررسی‌های بازار کار جهانی، هم از گزارش‌ها و هم از حقوق بالای متخصصان امنیت سایبر قابل دریافت است. مطابق گزارشی که کنسرسیوم[۱] (ISC)[۲] در سال ۲۰۱۹ منتشر کرده است میزان کمبود نیروی امنیت سایبر در سطح جهانی به عدد ٤،۰۷ میلیون نفر رسیده است [٦]. کارشناسان در داخل کشور نیز بر این موضوع تأکید دارند که کشور ما نیز با کمبود نیروی متخصص امنیت سایبر مواجه است. وزیر ارتباطات و فناوری اطلاعات در سال ۹٦ در هفته نکوداشت پدافند غیرعامل با اشاره به روبرو بودن کشور با تهدیدات سایبر به اهمیت امنیت سایبر برای اقتصاد و امنیت کشور پرداخت. او بیان کرد که تا سال ۲۰۲۵ فناوری‌های اینترنت اشیا، کلان داده و واقعیت افزوده گسترده‌تر خواهند شد و می‌توانند مسائل متعددی ایجاد کنند. او از تلاش برای تربیت ۱۰ هزار نیروی متخصص سایبری در کشور برای مقابله با تهدیدات خبر داد و افزود: "تربیت این نیروها با هدف افزایش توانمندی در بخش دفاع سایبری در دستور کار قرار گرفته است" [۷].

پژوهش حاضر تلاش دارد که راهکارها و راهبردهایی برای مواجهه با کمبود نیروی متخصص امنیت سایبر ارائه کند و سپس آن‌ها را با توجه با شرایط کشور اولویت‌بندی کند. در همین راستا در مرحله اول با کارشناسان این حوزه مصاحبه صورت گرفت و بعد از تحلیل مضمون راهکارها و معیارهای ارزیابی آن‌ها استخراج شد. با توجه به فراگیری مشکل و وجود مقالات و تجربیاتی در زمینه راهکارهای پاسخ‌گویی به این مشکل در سایر کشورها، از مقالات و گزارشات موجود برای جمع‌آوری اولیه راهکارها استفاده شد. مجموع راهبردها و راهکارهای حاصله از مصاحبه‌ها و مطالعات کتابخانه‌ای در دو دسته راهبردها و راهکارها دسته‌بندی شدند. برای اولویت‌بندی راهبردها از روش تحلیل سلسله مراتبی فازی[۲] استفاده شد. معیارهای مورد استفاده در این روش نیز از مصاحبه‌ها و مطالعات کتابخانه‌ای استخراج شدند. برای ارزیابی و اولویت‌بندی راهکارها نیز از روش تحلیل اهمیت-عملکرد[۳] استفاده شد. در روش تحلیل سلسله مراتبی فازی از نظر ٥ کارشناس و در روش تحلیل اهمیت-عملکرد از نظر ۱۱ کارشناس استفاده شد. در بخش‌های پیش روی ابتدا مبانی نظری و پیشینه تحقیق مرور می‌شود. در بخش سوم روش جمع‌آوری اطلاعات و تحلیل نتایج پژوهش توضیح داده شده است. یافته‌های به دست آمده از پژوهش و جمع‌بندی آن‌ها در بخش‌های ٤ و ٥ آورده شده است.

## ۱. مبانی نظری و پیشینه تحقیق

مطابق مرجع [۱] "امنیت سایبر به تکنیک‌ها و فناوری‌هایی اشاره می‌کند که از اطلاعات و سیستم‌ها در مقابل دزدی و حمله محافظت می‌کند."

بنا بر تعریف سازمان ملی استاندارد و تکنولوژی ایالات متحده، در سند چهارچوب نیروی کار ابتکار ملی برای آموزش امنیت سایبر که از اسناد معتبر و پر ارجاع در این کشور است، نیروی کار امنیت سایبر، "نیروی کاری است که نقش‌های کاری آن بر روی توانایی سازمان برای محافظت از داده، سیستم‌ها و عملیات، اثرگذار است [۸]."

در این پژوهش نیز همین تعریف از نیروی امنیت سایبر در نظر گرفته شده است. این سند نیروی کار امنیت سایبر را نه تنها شامل حوزه‌های فنی مرتبط می‌داند بلکه تخصص‌های مرتبط دیگر، مانند حقوق و مدیریت را نیز در بر می‌گیرد.

داشتن دانش پیشرفته درزمینه‌های مرتبط با امنیت و توانایی به‌کارگیری آن در حل مشکلات جدید دو قسمت اصلی در تعاریف نیروی کار متخصص است. در مستندی که توسط وزارت امنیت ملی ایالات‌متحده در مورد توسعه نیروی کار امنیت سایبر منتشر شده است [۱]، تخصص در این زمینه به صورت"توانایی به‌کارگیری دانش پیشرفته و مهارت‌ها در شرایط پیچیده، سخت یا جدید کاری" تعریف شده است.

لیبسکی[٤] و همکاران طی مصاحبه‌هایی که با افراد مختلف داشته‌اند، ویژگی‌های یک نیروی امنیت رده‌بالا را شامل موارد زیر می‌دانند [۹]:

- توانایی در تشخیص نقاط آسیب‌پذیر یا علائم ظریف نفوذ را دارد.
- استعداد فنی خود را با تجربه‌های کسب‌وکاری و سازمانی ترکیب می‌کند
- اینگونه افراد معمولاً در دهه سوم زندگی خود هستند.

با ظهور اقتصاد دیجیتال، اقتصاد جهانی دچار یک دگرگونی گسترده شده است، مرزها برداشته شده و مهارت‌های جدیدی برای تولید محصولات، مورد توجه قرار گرفته است. یکی از این مهارت‌ها که درخواست رو به رشدی دارد، مهارت‌های مرتبط با تهدیدات سایبری است [۱۰]. در حال حاضر بخش خصوصی و دولتی در سرتاسر جهان بر سر منابع محدود متخصصان امنیت در بین نیروی کار جهانی در حال رقابت هستند [٤] و سرعت افزایش درخواست از سرعت افزایش عرضه بیشتر است. به نظر می‌رسد که عمده دلیل افزایش تقاضا افزایش رایانه‌ها و گستردگی ارتباطات است. با گستردگی ارتباطات و رایانه‌ها، داده‌های بیشتری ذخیره می‌شود و فرآیندهای بیشتری وابسته به این تکنولوژی‌ها می‌شود و درنتیجه از بین رفتن امنیت آن‌ها مخاطرات بیشتری ایجاد می‌کند، بنابراین باید محافظت بیشتری از آن‌ها به عمل آید. دیجیتالی شدن و گستردگی ارتباطات همچنان رو به رشد به نظر می‌رسد بنابراین باید کماکان منتظر افزایش تقاضا باشیم. در گزارشی که مرکز مطالعات راهبردی و بین‌المللی آمریکا در سال ۲۰۱۹ با عنوان خلق نیروی کار امنیت سایبر منتشر کرد، بیان کرده است که در حال حاضر آمریکا با مشکل کمبود جدی نیروی کار مواجه است و تعداد موقعیت‌های کاری پر نشده در این حوزه افزایش پیدا کرده است. این نیاز تقریباً در تمامی جایگاه‌های این حوزه وجود دارد اما نیازهای حادتر برای کارکنان فنی بسیار متخصص است. این گزارش تأکید دارد که بعد از گذشت ۹ سال از گزارش CSIS در سال ۲۰۱۰ [۱۱]، هنوز خلأ ذکرشده برای نیروی امنیت سایبر وجود دارد [۱۲]. در بین منابع، تخمین‌های متعددی برای میزان نیاز نیروی کار در آینده و کمبود آن در شرایط فعلی وجود دارد. بنا بر گزارش کنسرسیوم (ISC)[۲]، خلأ نیروی کار در زمینه امنیت سایبر در سال ۲۰۱۹ به عدد ٤ میلیون نفر رسیده است [۱۳].

تخمین‌ها نشان می‌دهد که میزان نیاز همچنان رو به افزایش خواهد بود [۱۰].

کشور ما نیز مطابق نظر کارشناسان با کمبود نیروی متخصص امنیت سایبر مواجه است. رئیس کمیسیون افتای سازمان نظام صنفی رایانه‌ای (نصر) در سال ۱۳۹٤ در مصاحبه با روزنامه ایران بیان می‌کند که امروز فناوری اطلاعات و امنیت اطلاعات نقش حیاتی در کشورها ایفا می‌کند و باید امنیت اقتصاد دانش‌بنیان و امنیت بومی و ملی در اولویت‌های کشور قرار گیرد. در آن مقطع کشور در دوران پس از برجام بوده است و در این مصاحبه ورود نرم‌افزارهای مختلف و اجرای پروژه‌ها جدید نیازمند تأمین ملاحظات امنیتی دانسته شده است که نیازمند متخصصان امنیت فناوری اطلاعات است. لکن کشور دچار کمبود در این زمینه بوده است. [۱٤]. مدیر یک شرکت دانش‌بنیان حوزه فناوری اطلاعات نیز در خرداد سال ۹۷ در مصاحبه با روزنامه همشهری بیان می‌کند در سال‌های اخیر کاربرد فضای مجازی در ادارات استان به‌طور چشمگیری افزایش پیدا کرده است و در صورت رعایت نکردن ملاحظات امنیتی می‌تواند پیاده‌سازی دولت الکترونیکی را دچار مشکل کند. این کارشناس راه تأمین امنیت دستگاه‌های اجرایی را آموزش نیروهای کارآمد و استفاده از مشاوران دارای صلاحیت می‌داند [۱۵].

کارشناسان معتقدند که کمبود نیروی متخصص امنیت سایبر مهم‌ترین یا یکی از مهم‌ترین چالش‌هایی است که سازمان‌ها و کشورها برای رویارویی با مخاطرات و تهدیدات روزافزون سایبری، پیش رو دارند. آن‌ها معتقدند که اگرچه توسعه ایمن محصولات و افزایش تکنولوژی‌های امنیت سایبر می‌تواند منجر به کاهش این نیازمندی شود اما همچنان نیاز به نیروی کار امنیت سایبر به‌ویژه نیروی متخصص امنیت سایبر باقی خواهد بود.

در واقع منابع انسانی همیشه ارزشمندترین دارایی امنیت سایبر است و هر میزان که اهمیت امنیت فضای سایبر بالاتر می‌رود، میزان توجه به این دارایی نیز افزایش پیدا می‌کند. مسئله اینجاست که کمبود متخصص امنیت سایبر مشکلی است که تأثیرات بسیار قابل‌توجهی در امنیت ملت‌ها می‌گذارد، بنابراین دسترسی به افراد بااستعداد تبدیل به یک عامل حیاتی این حوزه شده است [٤]. توسعه نیروی انسانی عموماً یکی از راهبردهای کلان در اسناد راهبردی کشورها در رابطه با امنیت سایبر است. در سند استراتژی ملی سایبر ایالات‌متحده که در سال ۲۰۱۸ به امضای رئیس‌جمهور این کشور رسید، بیان شده است که رقبای آمریکا در حال استفاده از برنامه‌های توسعه نیروی کار امنیت سایبر هستند و ازاین‌رو یکی از راهبردهای کلان را توسعه نیروی کار امنیت سایبر عنوان کرده است و برای آن اولویت‌های اقدامی تعریف شده است که در این سند مورد بررسی قرار گرفته‌اند [٥]. راهبرد ملی امنیت سایبر انگلیس ۲۰۱٦-۲۰۲۱ که در سال ۲۰۱٦ توسط رئیس خزانه وقت دولت انگلیس امضا و ابلاغ شد، سه راهبرد اساسی برای دست یافتن به آرمانی که در این سند توصیف شده، در نظر گرفته است که شامل دفاع، بر حذر داشتن و توسعه است [۱٦]. در این سند ذیل دو راهبرد کلی بر حذر داشتن و توسعه به این مهم توجه شده است. در استراتژی کلی بر حذر داشتن، به منظور ایجاد یک قدرت بازدارنده، توسعه نیروی کار امنیت در حوزه تهاجمی

مورد توجه قرار گرفته است تا جایی که برای ارزیابی میزان دستیابی برنامه در این راهبرد به اهدافش، دو معیار در نظر گرفته شده است: کشور انگلیس در ظرفیت‌های تهاجمی سایبری، رهبری دنیا را داشته باشد و کشور یک مسیر توسعه از مهارت‌ها و تخصص‌ها ایجاد کرده باشد که بتواند تسلط این کشور را در حوزه امنیت تهاجمی حفظ و توسعه دهد.

استراتژی ملی امنیت دیجیتال فرانسه در تاریخ ۱۵ اکتبر سال ۲۰۱۵ توسط، نخست‌وزیر وقت فرانسه ابلاغ شد که

دارای ۵ هدف اصلی است که یکی از این اهداف، "افزایش آگاهی، آموزش اولیه و ادامه تحصیل" است که در ذیل آن به موضوعات مرتبط با توسعه نیروی کار امنیت سایبر، مانند ادغام آموزش امنیت سایبری در آموزش عالی در رشته‌های شامل فناوری اطلاعات اشاره شده است [۱۷].

در اسناد کلان داخلی نیز به اهمیت تربیت نیروی کار امنیت سایبر توجه شده است. برای نمونه در سند پدافند سایبری کشور در ذیل بخش "مأموریت پدافند سایبری کشور"، "آموزش و تربیت سرمایه‌های انسانی در حوزه سایبری" را از مأموریت‌های پدافند سایبری کشور می‌داند و همچنین "آموزش، تربیت و توانمندسازی سرمایه‌های انسانی کارآمد متناسب با اقتضائات حال و آینده پدافند سایبری" از "اهداف کلان در افق چشم‌انداز پدافند سایبری کشور" به حساب آورده شده است. همچنین در بخش "موضوعات اساسی راهبردی پدافند سایبری کشور"، " ایجاد تناسب و کفایت سرمایه‌های انسانی" نیز از موضوعات اساسی ذکر شده است.

در این قسمت به بررسی پیشینه تحقیقات مرتبط می‌پردازیم. ساولا[۵] در مقاله خود با اشاره به اهمیت موضوع نیاز به متخصصین امنیت به توسعه متریک برای بررسی اطلاعات موجود برای بررسی میزان سطح رقابت برای متخصصان امنیت در کشور فنلاند پرداخته است [٤].

کب[٦] در مقاله خود با اشاره به وجود یک شکاف بین نیازمندی و میزان فعلی نیروی امنیت متخصص ضرورت توجه به این موضوع را بیان می‌کند. او ذکر می‌کند که بیشتر تحقیقات انجام‌شده در این مورد است که چگونه نیروها را آموزش دهیم و نگهداری کنیم که بر یک فرض استوار است که نیروی کارا و با استعداد کافی برای طی کردن این مسیر وجود دارد. در نهایت او نتیجه می‌گیرد که تعداد گزینه‌های دارای پتانسیل رسیدن به سطح معقول تخصص، کمتر از میزانی است که این شکاف را پر کند. مگر اینکه میزان تقاضا کاهش پیدا کند [۱۸].

توه[۷] در مقاله خود بیان می‌کند که با وجود تغییرات گسترده حاصل از ظهور اقتصاد دیجیتالی تهدیداتی بروز کرده است که نیازمندی به نیروی‌های متخصص امنیت سایبر را بیشتر کرده است. او در این تحقیق بیان می‌کند که این نیاز در سال ۲۰۲۱ به ۳,۵ میلیون نفر خواهد رسید. نگارنده در این مقاله تلاش‌های صورت گرفته توسط ۹ کشور برتر اقتصاد دیجیتال برای توسعه نیروی کار متخصص سایبر را مورد بررسی قرار داده است. او در مقاله خود ٦ عامل آگاهی، کارآموزی، گواهی‌های فنی، تحصیلات بالاتر، همکاری و ادغام در سیستم آموزشی را از عناصر توسعه نیروی انسانی امنیت سایبر بر می‌شمارد [۱۰].

بشیر[۸] و همکاران در مقاله خود ابتدا به موضوع حمله کره شمالی به شرکت سونی پیکچر و پس از آن برنامه‌های ایالات متحد برای ارزیابی و توسعه نیروی امنیت سایبر می‌پردازند. آن‌ها در این مقاله به بررسی رقابت‌های سالانه‌ای که در این کشور انجام می‌شود پرداخته‌اند و از زاویه دید انسانی به آن نگاه کرده‌اند [۱۹].

برلی[۹] و همکاران در مقاله خود به این سؤال پاسخ می‌دهند که نقش حرفه‌ای‌گری در بهبود ظرفیت‌های امنیت سایبر چیست؟ اساساً نگارندگان معتقدند که نگاه به امنیت سایبر به عنوان یک حرفه غلط است. ممکن است در بخش‌هایی وضعیت به‌گونه‌ای باشد که نیاز به یک حرفه‌ای گری باشد لکن در تمامی این بخش‌ها نوع نگاه حرفه محوری می‌تواند باعث عدم پاسخگویی به نیازها شود [۲۰].

کمیسیون CSIS برای امنیت سایبر، در گزارشی که در سال ۲۰۱۰ منتشر کرد، برای هر راهبردی که برای مقابله با مشکل کمبود نیروی امنیت سایبر تنظیم می‌شود، داشتن ٤ عنصر را ، ضروری می‌داند [۱۱]:

۱- ارتقا و حمایت از توسعه برنامه‌های دقیق تحصیلی در مدارس

۲- پشتیبانی از توسعه و به‌کارگیری گواهی‌های حرفه‌ای دقیق که دارای اجزای عملیاتی مناسب هستند

۳- به‌کارگیری ترکیبی از به دست آوردن، استخدام و آموزش منابع، برای افزایش سطح صلاحیت کسانی که سیستم‌های دولتی را می‌سازند، عملیاتی می‌کنند و دفاع می‌کنند

٤- اطمینان حاصل کردن از وجود یک مسیر شغلی مناسب، مانند سایر رشته‌ها، برای نگهداشت و بزرگداشت کسانی که سطوح بالایی از توانایی را دارند

لیبسکی و همکاران با اشاره به موضوع کمبود نیروی انسانی متخصص امنیت سایبر در آمریکا ، به بررسی وضعیت فعلی بازار متخصصین امنیت سایبر در کشور آمریکا پرداخته‌اند. در این کتاب در ابتدا به مطالعه ادبیات موضوع پرداخته شده است و سپس یک مصاحبه نیمه ساخت‌یافته با مدیران، مربیان و متخصصین امنیت سایبر انجام شده است و درنهایت پیشنهادات اقتصادی را برای بازار نیروی کار متخصص امنیت سایبر ارائه کرده است. در این کتاب به مفهوم متخصص امنیت سایبر نیز پرداخته شده است و از منظر اقتصادی به موضوع نگاه شده و مدل عرضه و تقاضا و تفاوت‌هایی که رفتار بازار نیروی کار از خود نشان داده است، نیز بررسی شده است. در نهایت برای روبرو شدن با این مشکل راه‌حل‌هایی ارائه شده است مانند[۹]:

- تغییر در قوانینی که از استخدام نیروی‌های متخصص امنیت سایبر جلوگیری می‌کند
- ادامه به خدمت گرفتن نیروی‌های متخصص توسط دولت از راه‌های مختلف
- بهسازی تست‌ها برای شناسایی افرادی که احتمالاً در این مسیر حرفه‌ای موفق می‌شوند
- در طولانی‌مدت، توسعه روش‌هایی برای ورود بانوان به حرفه امنیت سایبر

کشتری[۱۰] در مقاله خود به بررسی وضعیت نگرانی کسب‌وکارها در کشور هند می‌پردازد. او بیان می‌کند که علاوه بر مشکلات قانون‌گذاری و حقوقی و تکنولوژی، کشور هند نیز مانند سایر کشورها از مشکل کمبود نیروی متخصص فناوری اطلاعات رنج می‌برد [۲۱].

کلی[۱۱] در تحقیق خود به دنبال این سؤال است که چه میزان سرمایه‌گذاری در بخش امنیت سایبر، شرایط را در وضعیت متعادل قرار می‌دهد [۲۲].

در کتابی که شورای تحقیقات ملی در زمینه حرفه‌ای گری در امنیت سایبر منتشر کرده است، به بررسی موضوع نیروی کار از دریچه حرفه‌ای‌گری پرداخته است. در این کتاب بیان می‌شود که امنیت سایبر حوزه جوانی است و با تغییرات گسترده‌ای همراه است. این موجب می‌شود که تنها آموختن دانش‌های ویژه ای برای متخصص شدن در این حوزه کافی نباشد. در این کتاب بیان می‌شود که حرفه‌ای شدن چه نقشی در ظرفیت و قابلیت‌های نیروی کار امنیت سایبر دارد و تصمیم گیران در دولت‌ها و بخش خصوصی باید چه سیاست‌هایی را برای حرفه‌ای شدن در نظر بگیرند. همچنین بیان می‌شود که امنیت سایبر دارای وسعت زیادی است و در نظر گرفتن آن به عنوان یک تخصص مناسب نیست و برای داشتن نیروی کار مناسب باید افرادی از زمینه‌های مختلف را برای این حرفه در نظر گرفت [۲۳].

در گزارشی که CISI در سال ۲۰۱۹ با عنوان خلق نیروی کار امنیت سایبر منتشر کرد، بیان شده است که تعداد زیادی از کارفرمایان از سطح آموزش‌ها ناراضی هستند به علاوه کارفرمایان معمولاً متوجه می‌شوند که فارغ‌التحصیلان امنیت سایبر فاقد مهارت‌های نرم؛ مانند کار تیمی، حل مسئله و ارتباطات هستند. این گزارش بیان می‌کند که آموزش‌ها باید دروس پایه‌ای مانند معماری کامپیوتر، رمزنگاری، شبکه، قواعد برنامه‌نویسی امن و غیره را در نظر بگیرد تا فارغ‌التحصیلان بتوانند با تغییرات تکنولوژی و مسیر شغلی همگام شوند. یکی دیگر از مشکلات برای کارفرمایان، تجربه ناکافی است. یکی از راه‌حل‌های کمبود مهارت‌های عملی در فارغ‌التحصیلان سایبری، گسترش کارآموزی، ارائه خدمات کار-تحصیل برای دانش آموزان و همراه ساختن آموزش‌ها با چالش‌های عملی، برگزاری مسابقات و شبیه‌سازی‌های محیط واقعی است [۱۲].

تیملین[۱۲] و ردر[۱۳] به این موضوع پرداخته‌اند که افراد با توانایی بالا، کلید تشخیص و بازیابی در برابر حملات هستند. این گزارش به بررسی عوامل مؤثر در استخدام و نگهداشت این افراد پرداخته است. می‌توان نتایج این تحقیق را در موارد زیر خلاصه کرد [۳]:

۱- از نظر نیروهای متخصص؛ چالشی بودن کار، اثرگذاری بالای نقش فرد متخصص، داشتن ساعت منعطف حضور در محل کار و ادامه دار بودن آموزش برای آن‌ها، مواردی هستند که مهم‌تر و اساسی‌تر از میزان پرداختی به آن‌ها است

۲- افراد متخصص علاقه دارند با کسانی کار کنند که به کار آن‌ها احترام می‌گذارند و پیوسته می‌توانند از آن‌ها یاد بگیرند

۳- افراد متخصص گواهی‌های بیشتر و متفاوتی دریافت می‌کنند

گزارش کارس[۱۴] و همکاران به بررسی وضعیت بازار کار امنیت سایبر، علی‌الخصوص در ایالت کالیفرنیا آمریکا پرداخته است. در این گزارش نیز علاوه بر بررسی وضعیت کمبود نیروی امنیت سایبر با توجه به عرضه و تقاضا در دسته‌های مختلف حوزه امنیت سایبر به بررسی خروجی طرح‌های آموزشی و استراتژی‌های مقابله با این چالش توسط کارفرمایان نیز پرداخته است [۲٤].

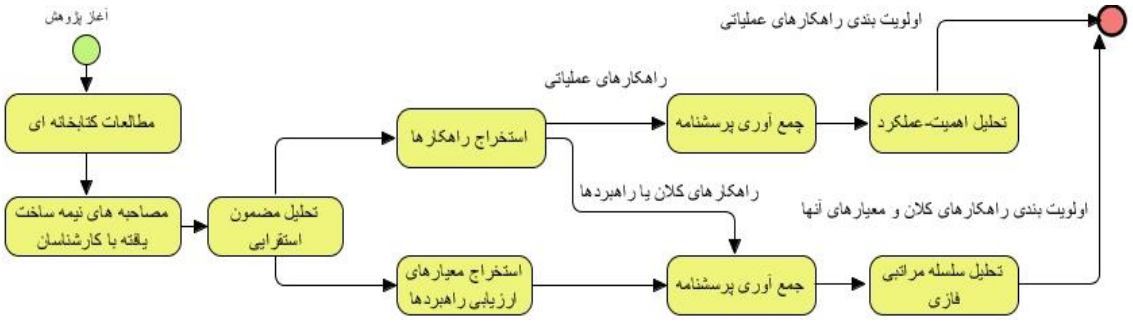
با توجه به اهمیت موضوع پژوهش‌های مختلفی در این حوزه انجام شده است که هر یک به جنبه‌ای از این موضوع پرداخته‌اند. برخی به ریشه‌های کمبود پرداخته‌اند، برخی به بررسی میزان یا ماهیت کمبود پرداخته‌اند و تعدادی از پژوهش‌ها نیز به ارائه راهکارها یا ارزیابی راهکارها پرداخته‌اند. مطالعه ادبیات موضوع و پیشینه تحقیق مبین آن است که در ارتباط با شناسایی حوزه‌های کمبود نیروی انسانی متخصص امنیت فناوری اطلاعات و ارائه راهکارهای اولویت‌بندی شده در داخل کشور کار چندانی انجام نشده است.

## ۲. روش تحقیق

با توجه به هدف پژوهش حاضر برای کاربردی کردن یافته‌هایش در پاسخ به مشکل کمبود نیروی متخصص امنیت این پژوهش از نوع کاربردی است. اما از این جهت که به بررسی وضع موجود می‌پردازد و به تبیین مشکلات و شرایط نیروی‌های کار امنیت سایبر می‌پردازد از نوع توصیفی است.

پژوهش حاضر به دلیل پیچیدگی موضوع از روش‌های تحقیقات کیفی و کمی به صورت همزمان استفاده کرده است. در این پژوهش برای یافتن راه‌حل‌ها از روش‌های کیفی استفاده می‌کند و برای اولویت‌بندی راهکارها به سراغ روش‌های کمی رفته است.

در این پژوهش ابتدا با انجام مصاحبه‌های نیمه ساخت‌یافته اقدام به شناسایی یافته‌ها می‌شود. سپس با استفاده از روش تحلیل محتوای کیفی، یافته‌ها تحلیل خواهند شد و خروجی مجموعه‌ای از راه‌حل‌ها، راهبردها و معیارها خواهد بود. معیارها و راهبردها، ورودی روش تصمیم‌گیری چندمعیاره فرآیند تحلیل سلسله مراتب فازی خواهند بود که درنتیجه اولویت‌بندی راهبردها صورت می‌پذیرد و از روش تحلیل عملکرد – کیفیت برای اولویت‌بندی راهکارها استفاده می‌شود. فرآیند پژوهش به صورت خلاصه در شکل ۱ آمده است.




شکل ۱ نمودار فرآیند انجام پژوهش

جامعه آماری

جامعه آماری موردبررسی در این تحقیق، کارشناسان حوزه امنیت هستند که در حال حاضر در این حوزه فعالیت دارند و نقش‌ها و اعمال آن‌ها بر روی اتفاقات حوزه امنیت مؤثر است وآن‌ها می‌توانند وضعیت فعلی بازار کار امنیت سایبر را تبیین کنند و همچنین می‌توانند راهکارهای برون‌رفت از مشکل کمبود نیروی متخصص امنیت فناوری اطلاعات ارائه نمایند. با توجه به این هدف عموماً فعالینی که سابقه حضور بیش از ۳ سال در این حوزه را دارا هستند مورد توجه قرار گرفته‌اند.

نمونه‌گیری

در این پژوهش از نمونه‌گیری هدفمند با استراتژی "نمونه‌برداری با حداکثر گوناگونی" استفاده شده است. یکی از ویژگی‌های این راهبرد این است که می‌تواند پیچیدگی‌های دنیای مورد ارزیابی را وارد تحقیق کند. این روش زمانی مناسب است که افراد موردنظر ما از لحاظ برخی خصیصه‌ها با هم متفاوت هستند [۲۵].

برای نمونه‌گیری دسته‌بندی زیر در نظر گرفته شد:

- مدیران دولتی
- مدیران شرکت‌ها
- اساتید دانشگاه یا موسسه‌های آموزشی
- متخصصین فعال در این حوزه

در این پژوهش از جامعه آماری کارشناسان حوزه امنیت سایبر ۹ مصاحبه به عمل آمده است که با تحلیل مضمون مشخص شد که اشباع داده نیز رخ داده است. همچنین در مرحله تحلیل نتایج به وسیله تحلیل سلسله مراتبی فازی از نظرات ۵ کارشناس استفاده شد و برای تحلیل عملکرد اهمیت از نظرات ۱۱ کارشناس استفاده شده است.

ابزارهای جمع‌آوری داده

در این پژوهش داده‌ها از طریق مطالعه منابع و مصاحبه و پرسشنامه بدست آمده است. با استفاده از اسناد و مطالعات پیشینه موضوع، ابعاد مفهومی موضوع و راهکارهای مشابه در کشورهای مختلف جمع‌آوری شده است و همچنین جمع‌آوری راهکارهای جدید در قالب مصاحبه نیمه ساخت‌یافته انجام شده است. در برخی موارد به جای مصاحبه از پرسشنامه کیفی استفاده شده است.

روش تحلیل محتوای کیفی

از آنجایی که این پژوهش ماهیتی اکتشافی دارد و هدف فهم علل کمبود و یافتن راهکارهای مقابله با این مشکل و معیارهای ارزیابی آن در ذهن کارشناسان بوده است، بنابراین از رویکرد استقرایی و روش تحلیل داده کیفی استفاده شده است.

فرآیند تحلیل سلسله مراتبی فازی

برای تعیین اولویت راهبردها بر اساس معیارها از روش تحلیل سلسله مراتبی فازی استفاده شده است. برای انجام روش تحلیل سلسله مراتبی فازی از توسعه‌های مختلفی استفاده می‌شود. در این پژوهش از توسعه چانگ [۲۶] استفاده شده است. همچنین به منظور تعیین نرخ ناسازگاری از روش گوگوس و بوچر [۲۷] استفاده شده است. همچنین برای تعیین برآیند نظرات کارشناسان از میانگین هندسی استفاده شده است.

روش تحلیل عملکرد-اهمیت

این روش اولین بار توسط مارتیلا[۱۵] به عنوان یک ابزار توسعه راهبردهای مدیریتی در یک شرکت به کار برده شد [۲۸]. در این راستا موارد اندازه‌گیری شده در یک موضوع از حیث عملکرد و اهمیت در یک نمودار دوبعدی نمایش داده شد که این موضوع به خاطر سهولت تفسیر و استخراج پیشنهادهای عملی بوده است. [۲۹]. در واقع تأکید بر روی سهلت به‌کارگیری و نمایش جذاب داده‌ها و پیشنهاد راهبردها از جمله عواملی است که موجب پذیرش گسترده این روش شده است [۲۸].

در این پژوهش برای بررسی و اولویت‌بندی راهکارهای ارائه شده در مراحل قبلی از نظر ۱۱ کارشناس استفاده شده و در نهایت از میانگین هندسی پاسخ‌های آنان استفاده شد.

## ۳. یافته‌های تحقیق

در این قسمت نتایج مصاحبه‌ها، تحلیل سلسله مراتبی فازی و تحلیل اهمیت-عملکرد ارائه می‌شود.

نتایج تحلیل مضمون مصاحبه‌ها

در طی فرآیند تحلیل مضمون، ۸۱ یک مضمون پایه در مصاحبه‌ها شناسایی شد که طی اعمال فرآیندهای انتزاعی سازی در نهایت و در بالاترین سطح در قالب ۷ مضمون سازمان دهنده دسته‌بندی شد. مصاحبه‌ها در این قسمت به صورت عمده شامل بررسی وضع موجود، بررسی مشکلات و راهکارهای برون‌رفت از مشکل بوده است.

همان‌طور که در جدول ۱ مشاهده می‌شود در این مرحله با ۹ کارشناس در حوزه امنیت سایبر که دارای سوابق بالایی هستند مصاحبه شده است. در اینجا تلاش شده است که این افراد از دسته‌های گوناگونی باشند که نوع نگاه‌های مختلفی مورد ارزیابی قرار بگیرد. در این بخش مصاحبه‌شوندگان شامل مدیر ارشد و میانی در حوزه امنیت سایبر، کارشناس فنی، مدرس دانشگاهی و غیردانشگاهی می‌باشند.

جدول ۱ ویژگی‌های افراد مصاحبه شده از جامعه کارشناسان

| کارشناس | شغل / سمت مصاحبه شونده |
|---|---|
| P1 | مسئول تیم امنیت سایبر یک شرکت هواپیمایی، کارشناس امنیت سایبر، ارزیاب شرکت‌های دانش‌بنیان در حوزه امنیت سایبر، کارشناس و مدیر در حوزه امنیت سایبر |
| P2 | مدیر پروژه تست نفوذ در یکی از شرکت‌های حوزه امنیت سایبر، کارشناس در حوزه امنیت سایبر |
| P3 | ریاست یکی از معاونت‌های سازمان فناوری اطلاعات ایران، کارشناس و مدیر در حوزه امنیت سایبر |
| P4 | کارشناس در حوزه امنیت سایبر |
| P5 | مدیر یکی از مؤسسات فعال در حوزه آموزش برنامه‌نویسی و امنیت سایبر، مدیر و کارشناس امنیت سایبر |
| P6 | عضو هیئت‌علمی دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر، کارشناس در حوزه امنیت سایبر |
| P7 | کارشناس حوزه امنیت سایبر |
| P8 | پژوهشگر، مدرس و مشاور حوزه امنیت سایبر |
| P9 | کارشناس حوزه امنیت سایبر |

**Error! Reference source not found.** مبین روند اشباع داده در فرآیند تحلیل مضمون با توجه به نظرات کارشناسان مختلف است. عبارت P۱ در ستون اول برای مضمون پایه تأیید کمبود نیروی کار متخصص امنیت سایبر به این معنا است که اولین بار این مضمون در مصاحبه با کارشناس P۱ بیان شده است. همان‌طور که در این جدول قابل‌مشاهده است در مصاحبه با کارشناس P۹ که آخرین کارشناس است، تنها یک مضمون پایه به مضامین پایه این بخش اضافه شد و هیچ مضمون سازمان دهنده‌ای نیز اضافه نشده است. در مورد کارشناس ماقبل آخر یا همان P۸ نیز تنها ۲ مضمون پایه اضافه شده است. بنابراین می‌توان گفت که تعداد مصاحبه‌ها درباره این موضوع به اشباع رسیده است.

موضوع بعدی که در مضامین پایه مورد بررسی قرار گرفت، تعداد تکرار آن‌ها بوده است. همان‌طور که در جدول ۲ قابل مشاهده است، تقریباً تمامی کارشناسان وجود نوعی از کمبود را تأیید کرده‌اند. در اینجا تعداد ٦ نفر از کارشناسان بر روی مشکل ضعف دانش مدیران و اثر آن در موضوع کمبود امنیت سایبر پرداخته‌اند و ٤ نفر از کارشناسان معتقد بوده‌اند که نحوه پرداخت دروس دانشگاهی به حوزه امنیت بسیار ضعیف است و چه بسیار دانشجویان رشته‌های فناوری اطلاعات هستند که دوره کارشناسی را طی می‌کنند ولی چیزی در مورد مفاهیم پایه‌ای امنیت سایبر نشنیده‌اند.

جدول ۲ تعداد تکرار مضامین پایه در مصاحبه با کارشناسان

| مضمون سازمان دهنده | مضمون پایه | P1 | P2 | P ۳ | P ٤ | P ٥ | P ٦ | P ۷ | P ۸ | P ۹ | مجموع |
|---|---|---|---|---|---|---|---|---|---|---|---|
| کمبود نیروی امنیت سایبر | تأیید کمبود نیروی کار متخصص امنیت سایبر | ۱ | ۱ | ۱ | | ۱ | | | | ۱ | ٥ |
| | روی آوردن شرکت به آموزش امنیت سایبر | ۱ | ۱ | | | | | | | | ۲ |
| | تأیید کمبود کیفی نیروی متخصص امنیت سایبر | | ۱ | ۱ | ۱ | | | ۱ | ۱ | | ٥ |
| | تأیید کمبود کمی نیروی متخصص امنیت سایبر | | ۱ | ۱ | ۱ | | | | ۱ | | ٤ |
| | صعودی بودن کمبود نیروی متخصص امنیت سایبر | | ۱ | | | | | | | | ۱ |
| | وجود استعداد فراوان در کشور | | | ۱ | | ۱ | | | | | ۲ |
| | کمبود نیروی کیفی در بخش دولتی | | | ۱ | | | | | | | ۱ |
| ویژگی‌های نیروی کار امنیت سایبر | سخت بودن ارزیابی نیروی امنیت سایبر | ۱ | | | | | | | | | ۱ |
| | حقوق بالای نیروی‌های متخصص | ۱ | | | | | | | | ۱ | ۲ |
| | وجود مهارت زبان انگلیسی در متخصصین امنیت سایبر | ۱ | | | | | | | | | ۱ |
| | عوامل دلسردی نیروی‌های متخصص | ۱ | | | | | | | | | ۱ |
| | لزوم داشتن استعداد کافی برای تبدیل شدن به متخصص امنیت سایبر | | | | | ۱ | | | | ۱ | ۲ |
| ماهیت امنیت سایبر | ماهیت غیر کارکردی امنیت | ۱ | | ۱ | | | | | | | ۲ |
| | چند تخصصی بودن حوزه امنیت سایبر | ۱ | | | | | | | | | ۱ |
| | زمان‌بر بودن آموزش امنیت | ۱ | | | | | | | | ۱ | ۲ |
| | سختی تربیت نیروی متخصص | ۱ | | | | | | | | ۱ | ۲ |
| | هزینه‌بر بودن آموزش امنیت سایبر | ۱ | | | | | | | | ۱ | ۲ |
| | مخاطب‌های دولتی بخش امنیت سایبر | | | | | ۱ | | | | | ۱ |
| مشکلات و علل | ضعف دانش مدیران | ۱ | | ۱ | | ۱ | | ۱ | ۱ | ۱ | ٦ |
| | مهاجرات زیاد کارشناسان امنیت سایبر | ۱ | ۱ | | | | | | ۱ | | ۳ |
| | پروژه‌های بی‌کیفیت | ۱ | | | | | | | | | ۱ |
| | مشکل در برنامه‌ریزی استراتژیک | ۱ | | | | | | | | | ۱ |
| | مشکل عملی نبودن آموزش‌ها | ۱ | | | ۱ | | | ۱ | | | ۳ |
| | فقدان بستر مناسب برای رشد متخصص امنیت سایبر | | ۱ | | | | | | | | ۱ |
| | کم شدن علاقه افراد به حوزه امنیت سایبر | | ۱ | | | | | | | | ۱ |
| | پرداخت کم و غیر جذاب به حوزه امنیت سایبر در دانشگاه‌ها | | ۱ | | | | | | | | ۱ |
| | کمرنگ شدن آپاهای[۱۶] دانشگاهی | | ۱ | | ۱ | | ۱ | | | | ۳ |
| | مشکل در نگهداری نیروی‌های امنیت سایبر در شرکت‌ها | | ۱ | | | | | | | | ۱ |
| | مشکل در آگاهی بخشی عمومی امنیت سایبر | | ۱ | | | | | | | | ۱ |
| | مشکل مالی در شرکت‌های خصوصی امنیتی | | ۱ | | | | | | | | ۱ |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | مشکل در مسیر شغلی امنیت سایبر در داخل کشور | | ۱ | | | | | | | | | ۱ |
| | وضعیت نامناسب بازار امنیت سایبر در داخل کشور | | ۱ | | | | | | | | | ۱ |
| | مشکل نظارت نامناسب نهادهای مربوطه | | ۱ | | | | | | | | | ۱ |
| | مشکل عدم ثبات در سیاست‌گذاری | | ۱ | | | | | | | | | ۱ |
| | مشکل استفاده کم از نیروی‌های متخصص در سمت‌های حاکمیتی | | ۱ | | | | | | | | | ۱ |
| | به‌روز نبودن آموزش‌های امنیت سایبر | | | ۱ | | | | | | | | ۱ |
| | وجود تهدیدات نامتعارف امنیتی در داخل کشور | | | ۱ | | | | | | | | ۱ |
| | مشکل کمبود منابع در بخش امنیت سایبر | | | ۱ | | | | | ۱ | ۱ | ۱ | ۳ |
| | تفکیک و پرداخت ضعیف دروس عمومی دانشگاهی و آموزشگاهی به امنیت سایبر | | | ۱ | ۱ | ۱ | | | | | ۱ | ٤ |
| | مشکل در ارزیابی‌های تخصصی امنیت سایبر | | | | ۱ | ۱ | | | | | | ۲ |
| | مشکل عدم برگزاری رویدادهای امنیت سایبر | | | | | ۱ | | | | | | ۱ |
| | مشکل طرح‌های آموزشی ناقص | | | | | ۱ | | | | | | ۱ |
| | مشکل عدم ارائه مطلوب مسیر شغلی امنیت سایبر | | | | | ۱ | | | | | | ۱ |
| | عدم وجود دغدغه کافی در نهادهای دخیل در امر منابع انسانی | | | | ۱ | | | | | | | ۱ |
| | مشکل تعداد کم ورودی‌های رشته تخصصی امنیت فناوری اطلاعات در دانشگاه‌ها | | | | | | | | ۱ | | | ۱ |
| | متمرکز نبودن اساتید تخصص‌های امنیت سایبر بر روی این حوزه | | | | | | | | ۱ | | | ۱ |
| | مشکل ارتباط صنعت با دانشگاه | | | | | | | | ۱ | | | ۱ |
| بایدهای آموزش اثربخش امنیت سایبر | لزوم توجه به مباحث پایه‌ای در آموزش امنیت | ۱ | ۱ | | | | | | | | | ۲ |
| | لزوم آموزش مراجعه به منابع در دوره‌های آموزشی | ۱ | | | | | | | | | | ۱ |
| | لزوم توجه به کارآموزی در آموزش‌های امنیت سایبر | ۱ | | | | | | | | | | ۱ |
| | توجه به معیارهای سنجش عملی | ۱ | | | | | | | | | | ۱ |
| بایدهای راهکارهای کلان | وابسته نبودن راهکارها به نقش‌های دولتی | | ۱ | ۱ | | | | | | | | ۲ |
| | داشتن نتایج زودبازده | | | ۱ | | | | | | | | ۱ |
| | توجه به همه رده‌های نیروی کار امنیت سایبر | | | ۱ | | | | | | | | ۱ |
| | اثربخشی طرح‌ها | | | | ۱ | | | | | | | ۱ |
| | در نظر گرفتن منافع نیروی انسانی در طرح‌ها | | | | | ۱ | | | | | | ۱ |
| | توجه طرح‌ها به شرایط کشور | | | | | ۱ | | | ۱ | | | ۲ |
| | توجه به هزینه‌ها | | | | | | | | ۱ | | | ۱ |
| | توجه به روند گسترش فناوری در طرح‌ها | | | | | | | | ۱ | | | ۱ |
| راهکار | طراحی نقشه مسیر برای طرح درس‌های آموزشی | ۱ | | | | | | | | | | ۱ |
| | لزوم توجه به طرح‌های ترکیبی آموزش و استخدام | ۱ | | | | | | | | | ۱ | ۲ |
| | تجربه محور کردن دروس دانشگاهی | ۱ | | | | | | | | | | ۱ |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | لزوم اصلاح مسیر شغلی | | | ۱ | | | | | | | ۱ |
| | لزوم توجه به آپاهای دانشگاهی | | | | ۱ | ۱ | | | | | ۲ |
| | لزوم استعدادیابی فعالانه دستگاه‌های کشور در حوزه امنیت سایبر | | | | ۱ | ۱ | | | | | ۲ |
| | لزوم تدوین استانداردهای الزام‌آور حاکمیتی | | | | | ۱ | | | | | ۱ |
| | لزوم آگاهی بخشی به مدیران درباره اهمیت امنیت سایبر | | | | | ۱ | | | | | ۱ |
| | لزوم تشکیل نهادهای مستقل در حوزه امنیت | | | | | ۱ | | | | | ۱ |
| | لزوم اجرای طرح‌های آموزشی امنیت سایبر با مخاطب دانش‌آموزی | | | | ۱ | | | | | | ۱ |
| | لزوم توجه به برگزاری رویدادهای امنیت سایبر | | | | ۱ | | | | | ۱ | ۲ |
| | لزوم توجه به آموزش نیروی‌های نظامی برای حضور در بخش امنیت | | | | ۱ | | | | | | ۱ |
| | لزوم آگاهی بخشی به مردم در مورد کمبود نیروی امنیت سایبر | | | | | ۱ | | | | | ۱ |
| | لزوم وجود یک نهاد مستقل برای پایش مستمر وضعیت نیروی کار امنیت سایبر و کیفیت آموزش‌های آن | | | | | | ۱ | | | | ۱ |
| | لزوم توسعه برنامه‌های جدید آموزشی | | | | | | ۱ | | | | ۱ |
| | لزوم توجه به دوره‌های بازآموزی | | | | | | ۱ | | | | ۱ |
| | لزوم بهبود گواهی‌های استاندارد امنیت | | | | | | ۱ | | | | ۱ |
| | لزوم وجود مؤسساتی آموزشی غیردانشگاهی با کیفیت بالا | | | | | | ۱ | | | | ۱ |
| | ارتقای دوره‌های دانشگاهی فعلی | | | | | | ۱ | | | | ۱ |
| | لزوم تخصیص بودجه مناسب | | | | | | | | ۱ | | ۱ |
| | لزوم توجه به شبکه‌های حرفه‌ای | | | | | | | ۱ | | | ۱ |

راهکارهای به دست آمده از مصاحبه‌ها و مطالعات کتابخانه‌ای، که در بخش قبلی ذکر شد، مطابق جدول ۳ در ۵ راهبرد کلی دسته‌بندی می‌شوند.

جدول ۳دسته‌بندی راهکارها

| | |
|---|---|
| جذب افراد به مسیر شغلی امنیت سایبر | توجه به برگزاری رویدادها و چالش‌های امنیت سایبر |
| | آگاهی بخشی به مردم در مورد کمبود نیروی امنیت سایبر |
| | اجرای طرح‌های آموزشی امنیت سایبر با مخاطب دانش آموزی |
| حفظ و نگهداری نیرو | اصلاح مسیر شغلی امنیت سایبر |
| | تولید ابزارهای استاندارد برای مدیریت مؤثر نیروی انسانی در سازمان‌ها |
| توسعه و آموزش نیروهای جدید | ارتقای دوره‌های دانشگاهی |
| | تخصیص بودجه مناسب برای توسعه نیروی امنیت سایبر |
| | طرح‌های ترکیبی آموزشی-استخدامی و یا کارآموزی‌ها |
| | توسعه مراکز آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری) دانشگاهی |
| | وجود نهادها یا سازمانهایی برای پایش مستمر وضعیت نیروی کار امنیت سایبر و کیفیت آموزش‌های آن |
| | ایجاد مؤسسات آموزشی غیر دانشگاهی با کیفیت بالا |
| | استفاده از کهنه سربازها |
| | طرح‌های افزایش حضور بانوان در حوزه امنیت سایبر |
| | استفاده از بورس‌های تحصیلی |
| | توجه به راهکارهای استفاده از نیروی‌های فعال در حوزه‌های نزدیک به امنیت سایبر |
| | ایجاد شبکه‌های حرفه‌ای در حوزه امنیت سایبر |
| جذب و به کارگیری استعدادهای کشف نشده | توسعه طرح‌های ارزیابی و استعدادیابی |
| بهبود بازار حوزه امنیت سایبر | بهبود فضای امنیت سایبر از طرق قانون گذاری و افزایش سطح الزامات امنیتی |
| | توسعه واژگان مشترک و چهارجوب های نیروی کار امنیت سایبر |
| | آگاهی بخشی مدیران درباره اهمیت امنیت سایبر |
| | کم کردن تقاضا به وسیله افزایش امنیت سامانه‌ها و آموزش‌های عمومی |

بنابراین با دسته‌بندی راهکارها، ۵ راهبرد کلان برای مقابله با کمبود نیروی متخصص امنیت سایبر به دست آمد که عبارت است از:

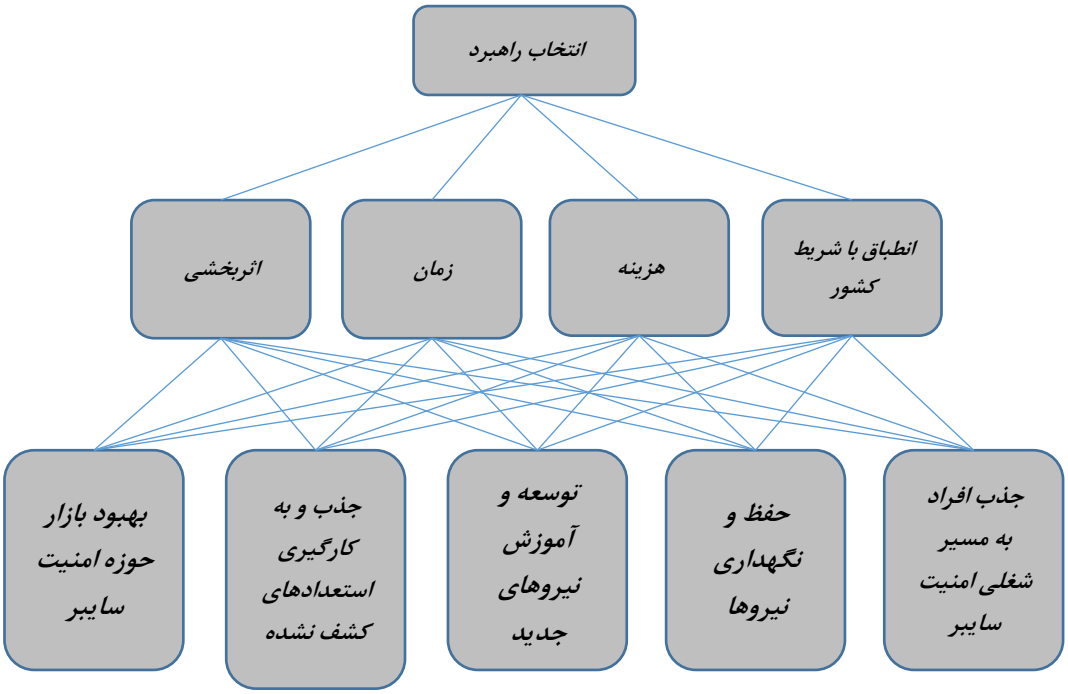
- جذب افراد به مسیر شغلی امنیت سایبر
- حفظ و نگهداری نیرو
- توسعه و آموزش نیروهای جدید
- جذب و به کارگیری استعدادهای کشف نشده
- بهبود بازار حوزه امنیت سایبر

همچنین با توجه به مطالعات کتابخانه‌ای و تحلیل مضمون مصاحبه‌ها برای ارزیابی راهبردها، ٤ معیار به صورت زیر تعیین می‌شود:

- انطباق با شرایط کشور
- هزینه اجرا
- زمان اجرا
- اثربخشی

نتایج حاصل از تحلیل سلسله مراتبی فازی

برای انجام تحلیل سلسله مراتبی فازی در مرحله اول نمودار سلسله مراتبی مطابق شکل ۲ ترسیم شد.




تصویر ۲ مدل درختی تحلیل سلسله مراتبی

سپس به تعداد ٥ نفر از کارشناسان و پژوهشگران مرتبط این حوزه پرسشنامه ارائه شد. ویژگی‌های این افراد به صورت مختصر در جدول ٤ آمده است. همچنین جداول داده ای پر شده توسط این افراد در ادامه آورده شده است.

جدول ٤ ویژگی کارشناسان پاسخ‌دهنده به پرسشنامه تحلیل سلسله مراتبی فازی

| فرد | شغل /سمت |
|---|---|
| P10 | کارشناس حوزه فناوری اطلاعات و پژوهشگر حوزه امنیت سایبر |
| P11 | مدیر در حوزه امنیت سایبر |
| P12 | کارشناس حوزه فناوری اطلاعات و پژوهشگر حوزه امنیت سایبر |
| P13 | کارشناس حوزه امنیت سایبر |
| P14 | کارشناس حوزه امنیت سایبر |

بعد از جمع‌آوری پرسشنامه‌ها ، خانه‌های خالی که معکوس قرینه خود نسبت به قطر اصلی در ماتریس پاسخ‌ها بوده‌اند پر شدند و عبارت‌های کلامی به عدد معادل فازی تبدیل شدند. بعد از این مرحله نرخ ناسازگاری هر یک از جداول محاسبه شد و مواردی که دارای نرخ ناسازگاری بیشتر از ۰,۱ بودند دوباره با کارشناس مربوطه بازنگری شدند و در نهایت نرخ‌های ناسازگاری مطابق جدول ٦به دست آمدند:

جدول ٥ نرخ ناسازگاری پاسخ‌های کارشناسان به پرسشنامه تحلیل سلسله مراتبی فازی

| | جدول معیارها | جدول راه‌حل‌ها با معیار انطباق | جدول راه‌حل‌ها با معیار زمان | جدول راه‌حل‌ها با معیار هزینه | جدول راه‌حل‌ها با معیار اثربخشی |
|---|---|---|---|---|---|
| P۱۰ | (۰,۰۵۱– و ۰,۰٦۱) | (۰,۰۰۸– و ۰,۰۷٥) | (۰,۰۳۳ و ۰,۰۹۲) | (۰,۳ و ۰,۰۸٥) | (۰,۰۱۸ و ۰,۰۹٤) |
| P۱۱ | (۰,۰۲۳ و ۰,۰٦٤) | (۰,۰۲٥ و ۰,۰۷۳) | (۰,۰۰۷– و ۰,۰٥٤) | (۰,۰٤– و ۰,۰٤۷) | (۰,۰۰۷ و ۰,۲۲) |
| P۱۲ | (۰,۰۲٦ و ۰,۰۷۲) | (۰,۰۱۹ و ۰,۰٥) | (۰,۰۱٤ و ۰,۰۳۸) | (۰,۰۳۸– و ۰,۰٤۱) | (۰,۰۲۹ و ۰,۰۸۱) |
| P۱۳ | (۰,۱٥– و ۰,۰۷۷) | (۰,۰۱۹ و ۰,٥) | (۰,۰۱٤ و ۰,۰۳۸) | (۰,۱۰۷– و ۰,۰٤۱) | (۰,۰۲۹ و ۰,۰۸۱) |
| P۱٤ | (۰,۰۱۷ و ۰,۰٥۷) | (۰,۰۲۲– و ۰,۳۸) | (۰,۰۲٤ و ۰,۰٦۷) | (۰,۰۱۲– و ۰,۰۹۸) | (۰,۰۰٥ و ۰,۰۱٦) |

سپس از جداول متناظر در پاسخ‌نامه‌های مختلف میانگین هندسی گرفته شد و در گام بعدی بردار وزن راهکار و معیارها محاسبه شده و سپس نرمال گردید که نتایج در جدول ٦ و جدول ٧ قابل مشاهده است:

جدول ٦ بردار وزن نرمال شده جدول معیارها در روش تحلیل سلسله مراتبی فازی

| اثربخشی بیشتر | زمان کوتاه‌تر | هزینه کمتر | انطباق بیشتر با شرایط کشور |
|---|---|---|---|
| ۰,۵۵ | ۰,۰ | ۰,۰ | ۰,٤٥ |

جدول ٧ بردار وزن نرمال شده جداول راهکارها در روش تحلیل سلسله مراتبی فازی

| معیار/ راهکار | جذب افراد به مسیر شغلی امنیت سایبر | حفظ و نگهداری نیروها | توسعه و آموزش نیروهای جدید | جذب و به‌کارگیری استعدادهای کشف نشده | بهبود بازار حوزه امنیت سایبر |
|---|---|---|---|---|---|
| انطباق بیشتر | ۰,۲۰۷ | ۰,۲۷۳ | ۰,۲۳٤ | ۰,۰۹۹ | ۰,۱۸٦ |
| هزینه کمتر | ۰,۲۵۱ | ۰,۲۱۷ | ۰,۱٤۷ | ۰,۲۸۵ | ۰,۱۰۰ |
| زمان کمتر | ۰,۱٦۲ | ۰,٤۰۵ | ۰,۰ | ۰,۳۰۸ | ۰,۱۲۵ |
| اثربخشی بیشتر | ۰,۱۲۰ | ۰,۲۸۸ | ۰,۲۳۳ | ۰,۰۹۵ | ۰,۲٦۵ |

و در نهایت با ضرب ماتریس وزن هر راهکار، از جهت یک معیار، در وزن آن معیار، بردارد نهایی اولویت مشخص می‌شود. از آنجایی که در ماتریس اولویت‌ها، وزن زمان کوتاه‌تر و هزینه کمتر صفر به‌دست‌آمده طبعاً وزن معیارهای آن‌ها بی‌اثر می‌شود و اولویت راهکارهایی که از نظر اثربخشی و انطباق، وزن بیشتری داشتند به عنوان راهکارهای با اولویت انتخاب می‌شوند. در مورد معیار هزینه کمتر، خبرگان عموماً معتقد بودند که انتخاب راهکارهای با هزینه کمتر چندان دارای اولویت نخواهد بود، چرا که در صورت لزوم این امکان در داخل کشور وجود دارد که طرح‌های گران‌قیمت را هم اجرا کرد و نسبت به معیارهای دیگر از اهمیت کمتری برخوردار است. زمان کمتر در مقابل هزینه کمتر از اهمیت بیشتر برخوردار بوده است ولی به دلیل نوع محاسبات در روش تحلیل سلسله مراتبی فازی چانگ وزن هر دو معیار برابر صفر شده است. نتایج نهایی تحلیل سلسله مراتبی در جدول ۸ آمده است.

جدول ۸ بردار اولویت منتج از تحلیل سلسله مراتبی فازی

| | بهبود بازار حوزه امنیت سایبر | جذب و به‌کارگیری استعدادهای کشف نشده | توسعه و آموزش نیروهای جدید | حفظ و نگهداری نیروها | جذب افراد به مسیر شغلی امنیت سایبر |
|---|---|---|---|---|---|
| اولویت | ۰,۲۳ | ۰,۱۰ | ۰,۲۳ | ۰,۲۸ | ۰,۱٦ |

مطابق جدول ۹ کارشناسان به ترتیب به راهبردهای زیر اولویت داده‌اند:

- حفظ و نگهداری نیروها
- توسعه و آموزش نیروهای جدید
- بهبود بازار حوزه امنیت سایبر
- جذب افراد به مسیر شغلی امنیت سایبر
- جذب و به‌کارگیری استعدادهای کشف نشده

نتایج حاصل از تحلیل اهمیت-عملکرد

در این مرحله از تعداد ۱۱ کارشناس در حوزه امنیت سایبر نظرسنجی شد. برای جمع‌آوری پرسشنامه از یک روش برخط استفاده شد و شرکت‌کنندگان به صورت برخط در نظرسنجی شرکت کردند. مشخصات خبرگان در جدول ۹ آورده شده است. از آنجایی که پرسش به صورت محدود در اختیار افراد قرار داده شده است و همه دارای صفت کارشناس بوده‌اند، برای توضیحات این افراد نیز از لفظ کارشناس حوزه امنیت سایبر استفاده شده است.

جدول ۹ مشخصات مشارکت‌کنندگان در پرسشنامه بررسی راهکارها در روش تحلیل اهمیت-عملکرد

| مورد | سمت /شغل |
|---|---|
| P15 | کارشناس، پژوهشگر در حوزه امنیت سایبر |
| P16 | مدیر و کارشناس در حوزه امنیت سایبر |
| P17 | کارشناس حوزه امنیت سایبر |
| P18 | کارشناس منابع انسانی در یک شرکت فناوری اطلاعات |
| P19 | کارشناس حوزه امنیت سایبر |
| P20 | کارشناس و پژوهشگر حوزه امنیت سایبر |
| P21 | کارشناس حوزه امنیت سایبر |
| P22 | کارشناس حوزه امنیت سایبر |
| P23 | کارشناس حوزه امنیت سایبر |
| P24 | کارشناس و مدیر در حوزه امنیت سایبر |
| P25 | کارشناس و پژوهشگر حوزه امنیت سایبر |

بعد از جمع‌آوری پاسخ‌نامه‌ها میانگین هندسی پاسخ‌ها گرفته شد که نتایج آن در جدول ۱۰ قابل‌مشاهده است.

جدول ۱۰ میانگین پاسخ‌ها به پرسشنامه روش تحلیل اهمیت-عملکرد

| راهکارها | اهمیت | عملکرد |
|---|---|---|
| برگزاری رویدادها (مانند همایش‌ها) و چالش‌ها با موضوع امنیت سایبر | ۳،۸۹ | ۱،۹۰ |
| آگاهی بخشی به مردم در مورد کمبود نیروی امنیت سایبر | ۳،۲۹ | ۱،٦۱ |
| اجرای طرح‌های آموزشی امنیت سایبر با مخاطب دانش آموزی | ۳،٦۷ | ۱،۲۱ |
| اصلاح مسیر شغلی امنیت سایبر | ٤،۲۰ | ۲،٥٦ |
| تولید ابزارها استاندارد برای مدیریت مؤثر نیروی انسانی امنیت سایبر در سازمان‌ها | ۳،٦۰ | ۱،٤۸ |
| ارتقای دوره‌های دانشگاهی | ۳،۹۱ | ۲،٥۰ |
| تخصیص بودجه مناسب برای توسعه نیروی کار امنیت سایبر (چه در سطح سازمان‌ها و چه در سطح ملی و حاکمیتی) | ۳،۹۷ | ۲،۲٦ |
| طرح‌های ترکیبی آموزشی- استخدامی و یا کارآموزی‌ها | ٤،۱٤ | ۱،۹۷ |
| توسعه مراکز آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری) دانشگاهی | ۳،۳۰ | ۲،٥۹ |
| نهادها یا سازمان‌ها یا برنامه‌هایی برای پایش مستمر وضعیت نیروی کار امنیت سایبر و کیفیت آموزش‌های آن | ۳،۳٦ | ۱،٥٥ |
| مؤسسات آموزشی غیردانشگاهی | ٤،۱٤ | ۲،۳۲ |
| آموزش و استفاده از نیروهای فعلی و بازنشسته نظامی یا کهنه سربازها | ۲،۳۸ | ۱،۷۲ |
| حضور بانوان | ۲،٥۹ | ۲،۲۰ |
| بورس‌های تحصیلی در حوزه امنیت سایبر | ۳،٤۰ | ۱،۷۲ |
| آموزش و استفاده از نیروی کار فناوری اطلاعات که در حوزه‌هایی غیر از امنیت سایبر فعال | ٤،۱۲ | ۲،۳۲ |
| شبکه‌های حرفه‌ای در حوزه امنیت سایبر | ٤،۲۳ | ۲،٤۰ |
| طرح‌های ارزیابی و استعدادیابی در حوزه امنیت سایبر | ٤،۰٥ | ۱،۹۰ |
| قانون‌گذاری و سطح الزامات امنیت سایبری | ۳،۷٥ | ۱،۹۷ |
| توسعه واژگان مشترک و چهارچوب‌های نیروی کار امنیت سایبر | ۳،۲۷ | ۱،۸٥ |
| آگاهی مدیران درباره اهمیت امنیت سایبر | ٤،۲۳ | ۲،۲٦ |
| تقاضای نیروی کار امنیت سایبر به خاطر ضعف در تکنولوژی‌ها و امنیت سامانه‌ها و سیستم‌های اطلاعاتی | ۲،۷۳ | ۳،۳۳ |

سپس نتایج به وسیله نرم‌افزار SPSS به صورت یک نمودار دوبعدی ترسیم شد(به منظور نمایش بهتر، داده‌ها در عدد ثابت ۱۰ ضرب شدند).

همان‌طور که در تصویر ۳ قابل مشاهده است، مواردی که در بلوک نیازمند تمرکز بیشتر قرار گرفته‌اند شامل:

- طرح‌های ترکیبی آموزش–استخدام
- طرح‌های ارزیابی و استعدادیابی
- رویدادها و چالش‌ها در حوزه امنیت سایبر
- طرح‌های با مخاطب دانش‌آموزی
- تولید ابزارها استاندارد برای مدیریت مؤثر نیروی انسانی امنیت سایبر در سازمان‌ها
- قانون‌گذاری مناسب و ارتقای سطح الزامات امنیتی

که در بین آن‌ها طرح‌های با مخاطب دانش‌آموزی کمترین میزان عملکرد و طرح‌های ترکیبی و استعدادیابی دارای بیشترین میزان اهمیت بوده‌اند.

مواردی که در بلوک اهمیت زیاد و عملکرد بالا قرار گرفته‌اند شامل موارد زیر بوده است:

- بهبود مسیر شغلی
- شبکه‌های حرفه‌ای

- آگاهی مدیران
- مؤسسات آموزشی غیردانشگاهی
- استفاده از نیروی‌های دیگر حوزه‌های فناوری اطلاعات
- تخصیص بودجه مناسب
- ارتقای دوره‌های دانشگاهی

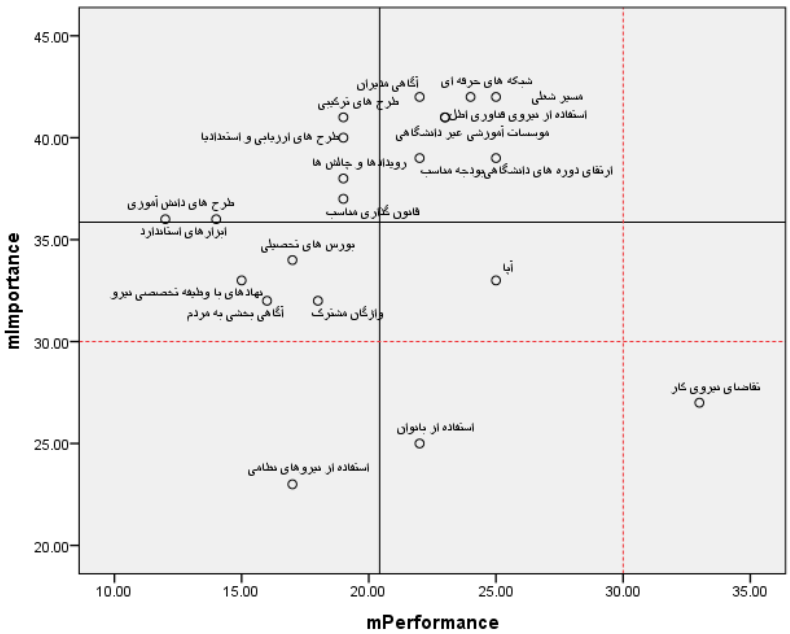
بلوک عملکرد پایین و اهمیت کم شامل موارد زیر شده است:

- بورس تحصیلی
- آگاهی‌بخشی‌های عمومی در مورد کمبود نیروی متخصص امنیت سایبر به مردم
- نهادهای با وظیفه تخصصی در حوزه امنیت سایبر
- توسعه واژگان مشترک و چهارچوب‌های نیروی کار امنیت سایبر
- استفاده از نیروهای فعلی یا بازنشسته نظامی

بلوک عملکرد بالا و اهمیت کم نیز شامل:

- آپاهای (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری) دانشگاهی
- استفاده از بانوان
- کاهش تقاضای نیروی کار از طریق بهبود تکنولوژی‌ها

مطابق روش تحلیل عملکرد–اهمیت برای خطوط میانی نمودار که مشخص‌کننده بلاک‌ها می‌باشد از روش میانگین‌گیری استفاده است. توجه به این نکته در اینجا ضروری به نظر می‌رسد که میانگین پاسخ‌ها در مورد میزان اهمیت، ۳,۶۳ بوده است که بیشتر از عدد میانه طیف لیکرت است و این به معنی این است که پاسخ‌دهندگان تعداد زیادی از راهکارها را مهم ارزیابی کردند و تعداد معدودی تنها از کمتر از ۳ ارزیابی شده‌اند. در مقابل میانگین برای میزان عملکرد، عدد ۲,۰۸ به دست آمده که نشان‌دهنده این موضوع است که پاسخ‌دهندگان در بیشتر این موارد ضعف عملکرد مشاهده کرده‌اند و در تنها یک مورد، کارشناسان به صورت میانگین عددی بالاتر از ۳ یعنی متوسط را انتخاب کرده‌اند. این موضوع در تصویر ۳ نیز آمده است. خطوط افقی و عمودی که به صورت نقطه‌چین هستند، بیانگر میانه طیف لیکرت پاسخ‌ها است. همانطور که قابل مشاهده است بیشتر راهکارها در بلوکی هستند که اهمیت بیشتر از میانه و عملکردی کمتر از میانه دارند. اما برای محسابات تحلیل اهمیت–علمکرد مطابق روش انجام آن برای بلوک‌بندی، از روش میانگین‌گیری استفاده شده است که در این حالت راهکارها را نسبت به یکدیگر بلوک‌بندی و بررسی می‌شوند.



تصویر ۳ نتایج تحلیل اهمیت-عملکرد

## ٤. تحلیل

بررسی‌های انجام شده حاکی ازآن است که یکی از مهم‌ترین مشکلات در این حوزه، ضعف آموزش‌های دانشگاهی و غیردانشگاهی در زمینه امنیت است. پرداخت ناقص یا عدم پرداخت در دانشگاه‌ها در رشته‌های مرتبط مانند مهندسی کامپیوتر و فناوری اطلاعات، به‌روز نبودن آن‌ها، ظرفیت پایین رشته‌های تخصصی امنیت و کیفیت پایین آموزش‌ها از جمله مشکلات اصلی مطرح شده در مصاحبه‌ها بوده است. در واقع به نظر می‌رسد که پرداختن به موضوع امنیت سایبر در دانشکده‌های کامپیوتر علی الخصوص در مقطع کارشناسی، تبدیل به یک موضوع کم اهمیت شده است که یا به آن پرداخته نمی‌شود و یا در نهایت در غالب یک درس ۳ واحدی ارائه می‌شود. در نتیجه مشاهده می‌شود که تعداد قابل توجهی از افرادی که از رشته‌های مرتبط فارغ التحصیل شده‌اند، با مفاهیم مرتبط با امنیت سایبر بیگانه هستند. از آنجایی که شناخت، مقدمه ایجاد علاقه و انتخاب یک مسیر حرفه‌ای است، بنابراین در حال حاضر این مقدمه در مورد بسیاری از دانشجویان اتفاق نمی‌افتد. حال که مطابق مشاهدات و نظرات کارشناسان این علاقه و زنده بودن امنیت در فضای دانشگاه رو به کاهش است و دانشگاه نیز بستر چندان مناسبی برای این ایجاد علاقه محیا نکرده است، به نظر می‌رسد که روند عرضه نیروی کار متخصص روند کاهشی نیز پیدا کند. کارشناسان البته در مجموع کیفیت آموزش‌ها در معدودی از دانشگاه‌های کشور در دوره‌های تخصصی امنیت در مقطع تحصیلات تکمیلی را خوب ارزیابی کرده‌اند، لیکن این موضوع در مورد همه دانشگاه‌های کشور صادق نیست. بنابراین یکی از راهبردهای ارائه شده توسط کارشناسان و همچنین تعدادی از راهکارها متوجه بهبود وضعیت آموزشی بوده است. ایجاد علاقه برای ورود به این مسیر حرفه‌ای تا جایی مهم است که برخی از راهکارها مانند طرح‌های آموزشی برای دانش آموزان، مستقلاً متوجه ایجاد شناخت و علاقه در مخاطبین پیش از ورود به دانشگاه بوده است و برخی از راهکارها مانند برگزاری رویدادها و رقابت‌ها به عنوان ابزاری موفق برای ایجاد شناخت و انگیزه در مخاطبین از گروه‌های مختلف سنی ارائه شده است.

بطور پیوسته حوزه امنیت سایبر از تصمیمات نهادهای حاکمیت و نقش‌آفرینی دولت‌ها متأثر بوده است که این اختصاص به کشور ما ندارد. بنابراین اگر این بازیگر به درستی ایفای نقش نکند می‌تواند اثرات بیشتری نسبت به سایر حوزه‌های مرتبط با فناوری اطلاعات داشته باشد. چراکه در اینجا دولت‌ها، خود نیز بخشی از خریداران عمده خدمات و محصولات امنیتی هستند تا جایی که در برخی موارد تبدیل به بزرگترین مخاطبین یا تنها مخاطبین می‌شوند. بنابراین ناآگاهی مدیران دولتی و سطح الزامات نامناسب امنیتی می‌تواند علاوه بر کاهش امنیت دارائی‌های اطلاعاتی کشور، موجب افت کیفیت پروژه‌های امنیت سایبر و کاهش تزریق منابع مالی به این حوزه شود که این خود می‌تواند موجب ضربه به بازار امنیت سایبر شود و همچنین موجب کاهش دستمزد این نیروها شود. این موضوع در نهایت موجب کم‌تر شدن علاقه افراد برای حضور یا ماندن در این حوزه می‌شود. بنابراین راهکارهایی متوجه افزایش سطح الزامات امنیتی، بهبود قانون‌گذاری و افزایش سطح آگاهی‌های مدیران شده‌اند و همچنین راهبرد بهبود بازار ناظر به این موضوع پرداخته است. شرایط محیطی کشور، مانند شرایط اقتصادی نیز علاوه بر موارد قبلی بنابر گزارش کارشناسان، منجر به افزایش نرخ مهاجرت نخبگان شده است. بنابراین برخی از راهبردها و راهکارها متوجه ایجاد عامل‌هایی برای نگهداشت نیروها در سازمان و کشور شده است. بنابراین اینکه کارشناسان مطابق نتایج به دست آمده، معتقد بودند که توجه به راهبردهای حفظ و نگهداری نیرو، ارتقای دوره‌های آموزش و بهبود بازار حوزه امنیت سایبر، از اولویت بیشتری نسبت به سایبر راهبردها برخوردار هستند، می‌تواند در کنار نگاه به عوامل کمبود یافت شده در مصاحبه‌ها، ارتباط معناداری ایجاد کند که در این جمع‌بندی سعی شد، به آن پرداخته شود. توجه به این راهبردها و راهکارها در نهادهای حاکمیتی مرتبط با امنیت سایبر مانند وزارت ارتباطات و فناوری اطلاعات و سازمان‌هایی که وظیفه توسعه نیروی کار متخصص و ماهر را برعهده دارند، مانند وزارت علوم، تحقیقات و فناوری، سازمان آموزش‌های فنی و حرفه ای و کلیه نهادهای مرتبط با برنامه ریزی و توسعه نیروی کار متخصص امنیت سایبر می‌تواند موجب کاهش کمبود متخصصین امنیت سایبر در داخل کشور شود.

## نتیجه‌گیری

هدف پژوهش حاضر ارائه مجموعه‌ای از راهکارها و راهبردها با نگاه ملی بوده است تا از این طریق بتواند شکاف موجود بین عرضه و تقاضای نیروی متخصص امنیت سایبر در داخل کشور را کاهش دهد. به همین جهت به سازمان‌ها، شرکت‌ها و نهادهای مرتبط با حوزه امنیت سایبر پیشنهاد می‌شود که به حمایت و پشتیبانی از رویدادها و مسابقات امنیت سایبر بپردازند. همچنین این سازمان‌ها باید تلاش کنند که با برگزاری نشست‌های تخصصی و هم‌اندیشی در دانشگاه‌ها به رواج علاقه‌مندی به امنیت سایبر در بین دانشجویان کمک کنند. توجه به این موارد می‌تواند باعث شهرت برند این شرکت‌ها یا سازمان‌ها نیز بشود. این شرکت‌ها همچنین باید به راهکارهای مرتبط با راهبرد حفظ و نگهداری نیروها بیشتر توجه کنند.

باید طرح درس‌های دانشگاهی به گونه‌ای تغییر یابد که میزان پرداخت به دروس امنیت سایبر، به صورت دروس جداگانه یا به صورت طرح مباحث مربوط به امنیت هر مبحث در سایر دروس، افزایش یابد. همچنین به نظر می‌رسد که این سازمان‌ها باید به همراه سایر سازمان‌ها و شرکت‌های خصوصی و دولتی مرتبط با امنیت سایبر اقدام به تشکیل سازمان یا کارگروهی کنند که وظیفه پایش مستمر بازار کار و نیازمندی‌های حوزه امنیت سایبر را به عهده داشته باشند و پیوسته برای به روزرسانی دروس دانشگاهی مرتبط با امنیت سایبر اقدام کنند.

ضعف قوانین موجود در حوزه امنیت سایبر یکی از مشکلات حائز اهمیت است که وزارت ارتباطات و فناوری اطلاعات باید در ارتقای سطح قوانین و الزامات امنیتی و همچنین سطح ارزیابی‌های امنیتی بیافزاید. با بهبود قانون‌گزاری در این حوزه، بازار حوزه امنیت می‌تواند بهبود قابل توجهی را تجربه کند که این امر در نهایت منجر به بهبود بازارکار این حوزه خواهد شد.

## منابع


***CYBERSECURITY WORKFORCE DEVELOPMENT TOOLKIT How to Build a Strong Cybersecurity Workforce, U.S.D.O.H. Security, Editor. 2016.***

***Mustaca, S. What is a security expert? 2015; Available from: https://blog.isc2.org/isc2_blog/2015/02/what-is-a-security-expert.html.***

***Timlin , K. and F. Reeder, Recruiting and retaining cybersecurity ninjas. 2016.***

***Savola, R.M. Current level of cybersecurity competence and future development: case Finland. in Proceedings of*** *۱۱th European Conference on Software Architecture: Companion Proceedings. ۲۰۱۷.the*

***NATIONAL CYBER STRATEGY, T.W. House, Editor. 2018.***

***Strategies for Building and Growing Strong Cybersecurity Teams (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2019.***

***تربیت ۱۰ هزار نیروی متخصص سایبری در اولویت است/خودداری از برخورد سلیقه‌ای با اپلیکیشن های بومی. ۱۳۹۶ ; دریافت شده از:***

***http://www.irna.ir/fa/News/82714471***

***Newhouse, W., S. Keith, B. Scribner and G. Witte , National initiative for cybersecurity education (NICE) cybersecurity workforce framework. NIST Special Publication, 2017.***

***Libicki, M.C., D. Senty, and J. Pollak, Hackers wanted: An examination of the cybersecurity labor market. 2014.***

***Teoh, C.S. and A.K. Mahmood, Cybersecurity Workforce Development for Digital Economy. The Educational Review, USA, 2018. 2(1): p. 136-146.***

***Evans, K. and F .Reeder, A human capital crisis in cybersecurity: Technical proficiency matters. 2010.***

***Crumpler, W. and J.A. Lewis, The Cybersecurity Workforce Gap. 2019: CSIS.***

***Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens - (ISC)² CYBERSECURITY WORKFORCE STUDY, 2018.***

***صادقی، کارشناسان افتا اعلام کردند***

***نیاز مبرم ایران به نیروی متخصص امنیت اطلاعات در پساتحریم. ۱۳۹۴، روزنامه ایران***

***کمبود نیروی متخصص در حوزه سایبری استان. ۱۳۹۷ ; دریافت شده از: http://newspaper.hamshahrionline.ir/id/17229/کمبود-نیروی-متخصص-حوزه-سایبری-استان.html***

***National Cyber Security Strategy 2016-2021. 2016, HM Government London.***

***French national digital security strategy, in French Republic. 2015.***

***Cobb, S. Mind this Gap: Criminal hacking and the global cybersecurity skills shortage, a critical analysis. in Virus Bulletin Conference. 2016 (pp. 1-8).***

***Bashir, M., A. Lambert, B. Guo, N. Memon and T. Halevi , Cybersecurity competitions: The human angle. IEEE Security & Privacy, 2015. 13(5): p. 74-79.***

*Burley, D.L., J. Eisenberg, and S.E. Goodman ,Would cybersecurity professionalization help address the cybersecurity crisis? Communications of the ACM, 2014. 57(2): p. 24-27.*

*Kshetri, N., Cybersecurity in India: Regulations, governance, institutional capacity and market mechanisms. Asian Research Policy, 2017. 8(1): p. 64-76..*

*Kelly, D. The economics of cybersecurity. in International Conference on Cyber Warfare and Security. 2017.*

*Council, N.R., Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making. 2013.*

*Carrese, J., M. Goss, A. Hermann, T. Bartel, K. Greaney, D. Fernandez, Cybersecurity: Labor Market Analysis and Statewide Survey Results.*

*Creswell, J.W., Educational Research Planning, Conducting, and Evaluating Quantitative and Qualitative Research ۴□□. ۲۰۱۲.*

*Chang, D.-Y., Applications of the extent analysis method on fuzzy AHP. European journal of operational research, ۱۹۹۶. 95(3): p. 649-655.*

*Gogus, O. and T.O. Boucher, Strong transitivity, rationality and weak monotonicity in fuzzy pairwise comparisons. Fuzzy Sets and Systems, 1998. 94(1): p. 133-144.*

*Martilla, J.A. and J.C. James, Importance-performance analysis. Journal of marketing,1977. 41(1): p. 77-79.*

*Oh, H., Revisiting importance–performance analysis. Tourism management, 2001. 22(6): p. 617-627.*

**پی نوشت:**

[۱] *(ISC)² :International Information System Security Certification Consortium*

[۲] *Fuzzy analytic hierarchy process (FAHP)*

[۳] *Importance-performance analysis (IPA)*

[۴] ***Libicki***

[۵] ***Savola***

[۶] ***Cobb***

[۷] ***Teoh***

[۸] ***Bashir***

[۹] ***Burley***

[۱۰] ***Kshetri***

[۱۱] ***Kelly***

[۱۲] ***Timlin***

[۱۳] ***Reeder***

[۱۴] ***Carrese***

[۱۵] ***Martilla***

[۱۶] *آگاهی‌رسانی، پشتیبانی و امداد*