دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۲، جلد ۲۱، شماره ۲ (۲۴-۳۲)
https://monadi.isc.org.ir

ارائه‌شده در بیستیمین کنفرانس بین‌المللی انجمن رمز ایران در سازمان پژوهش‌های علمی و صنعتی ایران، ۸ و ۹ شهریور ۱۴۰۲

تحلیل روندهای جهانی درارائه چارچوب‌های آموزشی برای تربیت متخصصان امنیت سایبری★

احمد راهداری[۱،۲] و محمدحسام تدین[۲،*]

[۱] دانشگاه شیراز، شیراز، ایران
[۲] پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
امنیت سایبری
آموزش رسمی
آموزش
مهارت
دانش
توانایی
نقش کاری
توسعه منابع انسانی
چارچوب نیروی کار امنیت سایبری آمریکا (NICE)
چارچوب مهارت‌های سایبری اروپا (ECSF)
چارچوب مهارت‌های سایبری استرالیا (ECSF)

dor: 20.1001.1.24763047.1402.12.2.3.9

نوع مقاله: پژوهشی

چکیده

آموزش امنیت سایبری در ایران با استانداردها و رویکردهای جهانی منطبق نیست و سه عامل، بخش آموزشی، متقاضیان آموزش و سازمان‌ها و شرکت‌های متقاضی کار شناخت مناسبی از تخصص‌ها و نقش‌های کاری مورد نیاز ندارند. تخصص‌های مختلف در زمینه‌های کاری امنیت سایبری، منطبق با پازل‌های بین‌المللی نیست و این امر حفره‌های امنیتی در زیست‌بوم فضای مجازی کشور ایجاد کرده است. افرادی که در حوزه سایبری فعالیت می‌کنند به ترکیبی از دانش ویژه حوزه، مهارت‌ها، توانایی‌ها و تخصص‌های دیگر نیاز دارند تا مانند فناوری‌هایی که با آن کار می‌کنند، قابل اعتماد و انعطاف‌پذیر باشند. در سطح بین‌المللی، چارچوب‌های متعددی برای آموزش و به‌کارگیری متخصصان امنیت سایبری طراحی و اجرا شده‌اند که از جمله مهم‌ترین آن‌ها می‌توان به چارچوب نیروی کار امنیت سایبری آمریکا (NICE)، چارچوب مهارت‌های سایبری اروپا (ECSF) و چارچوب مهارت‌های سایبری استرالیا (ASD) اشاره کرد. در این مقاله، هر کدام از این چارچوب‌ها به طور خلاصه معرفی و ویژگی‌های کلیدی آن‌ها، از جمله هدف، ساختار و اجزا بررسی و تحلیل می‌شود. همچنین اثربخشی آن‌ها در رسیدگی به چالش‌های سازمان‌های جهانی در ایجاد و توسعه منابع انسانی متخصص امنیت سایبری ارزیابی و تحلیل می‌شود. این بررسی نقاط قوت و ضعف هر چارچوب را برجسته می‌کند، قرابت یکی از چارچوب‌ها به فضای آموزشی و بازار کار ایران را نشان می‌دهد و توصیه‌هایی را برای طراحی یک چارچوب ملی آموزش و به‌کارگیری متخصصان امنیت سایبری ارائه می‌دهد که می‌تواند درس‌آموزی بزرگی برای کشور داشته باشد تا متولیان امر در اسرع وقت در این زمینه اقدامات لازم را انجام دهند.

۱ مقدمه

تهدیدهای سایبری یکی از مهم‌ترین چالش‌های پیش روی همه سازمان‌ها صرف نظر از حوزه فعالیتشان است. برای مقابله با این تهدیدها، سازمان‌ها روی فناوری‌های دفاعی سرمایه‌گذاری کرده و استانداردهایی را برای تضمین امنیت سیستم‌های اطلاعاتی پیاده‌سازی کرده‌اند. بنابراین، بردار اصلی حمله به سیستم‌های اطلاعاتی، نیروی انسانی درون یک سازمان شده است [۱]. آسیب‌پذیری‌های فناوری همراه با کمبود نیروی انسانی و شکاف مهارتی می‌توانند داده‌های سازمان را به خطر بیاندازند و/یا بر تصمیمات مدیریتی تأثیر بگذارند. از این رو در کنار ابعاد فنی، تحقق امنیت سایبری نیازمند توسعه منابع انسانی کارآمد است.

در سال‌های اخیر و همزمان با فراگیرشدن اینترنت، هوشمندسازی

★از کمیته علمی بیستمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول
آدرس‌های رایانامه: a.rahdari@hafez.shirazu.ac.ir (احمد راهداری)، tadayon@itrc.ac.ir (محمدحسام تدین)

و افزایش ضریب نفوذ فضای سایبر، بسیاری از کشورهای توسعه‌یافته به‌منظور محافظت از شهروندان و زیرساخت‌های خود در مقابل تهدیدهای سایبری، چارچوب‌ها و راهبردهایی را برای مدیریت فرآیندهای توسعه منابع انسانی امنیت سایبری طراحی و/یا بازطراحی کرده‌اند. با این وجود، مطابق آمارگیری‌های انجام‌شده بیشتر این کشورها هم‌چنان دچار شکاف‌های مهارتی و چالش کمبود نیروی انسانی متخصص هستند [۲].

افرادی که در حوزه سایبری فعالیت می‌کنند به ترکیبی از دانش خاص حوزه، مهارت‌ها، توانایی‌ها و ویژگی‌های دیگر نیاز دارند تا مانند فناوری‌هایی که با آن کار می‌کنند، قابل اعتماد و انعطاف‌پذیر باشند. بر همین اساس و با توجه به اهمیت موضوع در تقویت توان دفاع ملی در حوزه امنیت سایبری، این سؤال مطرح می‌شود که آیا «چارچوب و نظام جامعی برای آموزش و به‌کارگیری متخصصان امنیت سایبری در ایران وجود دارد؟» سؤالی که شواهد نشان از مغفول ماندن آن به دلایلی مانند عدم یکپارچگی مسئولیت‌ها و وظایف نهادهای متولی امنیت سایبری و یا سیار عوامل دارد.

پیشرفت فناوری‌های اطلاعات و ارتباطات و هوش مصنوعی به‌گونه‌ای شگرفت و فراگیر بوده که کشورهای پیشرفته بر آن شده‌اند به صورت سیستماتیک و نهادی در تمام زمینه‌های مورد تهدید امنیتی، از مهد کودک تا دانشگاه‌ها و از سازمان‌های کوچک تا دولت‌های فدرال را زیر چتر آموزش و تربیت نیروی انسانی قرار دهند. به این منظور به صورت کاملاً مطالعه‌شده پازل‌های لازم را طراحی کرده و به کار گرفته‌اند.

این مقاله بر اساس یک پروژه پژوهشی از مطالعه گسترده و عمیق مهم‌ترین چارچوب‌های بین‌المللی آموزش امنیت سایبری، یعنی چارچوب نیروی کار امنیت سایبری آمریکا (NICE [۱]) [۳]، چارچوب مهارت‌های سایبری اروپا (ECSF [۲]) [۴] و چارچوب مهارت‌های سایبری استرالیا (ASD [۳]) [۵] شکل گرفته است تا بر اساس درس‌آموزه‌های آن بتوان توصیه‌های لازم را برای کشور ارائه داد.

در ادامه این مقاله، در بخش‌های ۲، ۳ و ۴ به ترتیب هر کدام از این چارچوب‌های آمریکا، اروپا و استرالیا همراه با ویژگی‌های کلیدی آن‌ها، از جمله هدف، ساختار و اجزا بررسی و تحلیل می‌شوند. در بخش ۵، نقاط قوت و ضعف این چارچوب‌ها همراه با اثربخشی آن‌ها ارزیابی می‌شود. در انتها و در بخش ۶، نتیجه‌گیری مقاله همراه با توصیه‌های برای طراحی یک چارچوب ملی آموزش و به‌کارگیری متخصصان امنیت سایبری ارائه می‌شود.

۲ چارچوب نیروی کار امنیت سایبری آمریکا (NICE)

چارچوب نیروی کار امنیت سایبری آمریکا که به اختصار با عنوان «چارچوب NICE» شناخته می‌شود، در سال ۲۰۱۷ توسط مؤسسه ملی استاندارد و فناوری [۴] ایالات متحده آمریکا ارائه شده است و هدف آن «آماده‌سازی، رشد، و حفظ نیروی کار امنیت سایبری است که از امنیت ملی و رفاه اقتصادی حراست کند و آن را ارتقا دهد». این چارچوب، یک منبع ملی به منظور توسعه نیروی کار امنیت سایبری است و برای بخش‌های دولتی، خصوصی و دانشگاهی قابل استفاده است. چارچوب NICE، یک زبان مشترک ایجاد می‌کند که با استفاده از آن می‌توان به توصیف کارها و کارکنان امنیت سایبری پرداخت و ارتباطات مورد نیاز برای شناسایی، استخدام و توسعه استعدادهای امنیت سایبری را بهبود بخشید. در واقع با استفاده از این چارچوب سازمان‌ها می‌توانند: الف) به رشد و آموزش نیروی کار خود برای انجام کارهای امنیت سایبری بپردازند؛ ب) به تقاضاهای بازار برای افزایش جذب، استخدام و حفظ استعدادهای امنیت سایبری رسیدگی کنند؛ ج) موقعیت‌های شغلی را مناسب با نیازهای خود ایجاد کنند و نامزدهای متنوع را با استفاده از توضیحات چارچوب NICE استخدام کنند. یادگیرندگان می‌توانند: الف) کارهای امنیت سایبری را پیدا کنند و برای توسعه دانش، مهارت‌ها، و توانایی‌های خود در فعالیت‌های یادگیری مناسب شرکت کنند؛ ب) شایستگی‌های خود را از طریق مسابقات، دوره‌های کارآموزی، و سایر رویکردهای یادگیری مبتنی بر تجربه نشان دهند. همچنین مؤسسات دانشگاهی می‌توانند از این چارچوب برای توسعه برنامه‌های درسی، مدارک تحصیلی و گواهینامه‌های امنیت سایبری استفاده کنند. درنتیجه مخاطبان این چارچوب یا کسانی که از آن استفاده می‌کنند، کارفرمایان، کارکنان فعلی و آینده امنیت سایبری، مشاوران دانشگاهی و متخصصان نیروی انسانی، ارائه‌دهندگان آموزش و گواهینامه‌ها و ارائه‌دهندگان فناوری هستند.

چارچوب NICE از اجزای زیر تشکیل شده است:

دسته‌ها (۷ تا): عملکردهای سطح بالای امنیت سایبری و ساختار سازمانی فراگیر چارچوب NICE را ارائه می‌دهند و هر کدام از آن‌ها از حوزه‌های تخصص و نقش‌های کاری تشکیل شده‌اند. این ساختار سازمانی مبتنی بر تحلیل‌های شغلی گسترده است که کار و کارکنانی را که کارکردهای اصلی مشترک دارند، در کنار هم قرار می‌دهد.

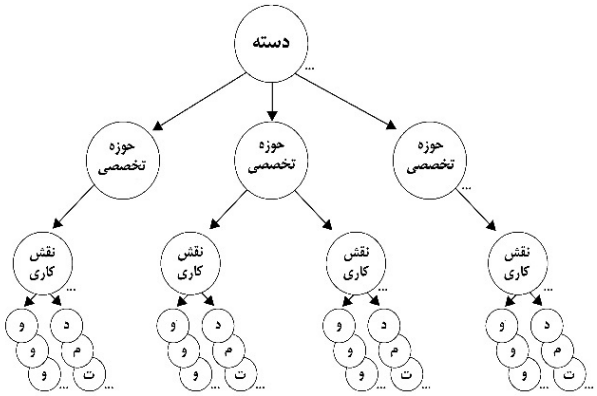
حوزه‌های تخصص (۳۳ تا): هر کدام از دسته‌ها شامل گروه‌هایی از کارهای امنیت سایبری هستند که به آن‌ها حوزه‌های تخصص می‌گویند. هر حوزه تخصصی شامل نقش‌های کاری است و نشان‌دهنده حوزه‌ای از کار یا عملکرد متمرکز در امنیت سایبری است.

نقش‌های کاری (۵۲ تا): موقعیت یا عملکرد نیروی کار سایبری هستند و جزئی‌ترین گروه‌بندی از امنیت سایبری و کارهای مرتبط را نشان می‌دهند.

هر کدام از نقش‌ها شامل فهرستی از ویژگی‌های مورد نیاز برای انجام آن نقش است که به آن «KSAT» یا به اختصار فارسی «دمتو» می‌گویند به معنی (د) دانش (K [۵])، (م) مهارت‌ها (S [۶])، (ت) توانایی‌ها (A [۷])

[1]National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [2]European Cybersecurity Skills Framework (ECSF) [3]Australian Signals Directorate (ASD) Cyber Skills Framework

[4]National Institute of Standards and Technology (NIST) [5]Knowledge [6]Skill [7]Ability



شکل ۱. اجزای چارچوب NICE و چگونگی ارتباط آن‌ها

و (و) وظایف (T [1]).

شکل ۱ اجزای چارچوب NICE و چگونگی ارتباط آن‌ها با یکدیگر را نشان می‌دهد و جدول ۱، ۷ دسته تعریف‌شده در این چارچوب را همراه با عناوین حوزه‌های تخصصی ذیل آن‌ها معرفی می‌کند.

برای توصیف هر نقش کاری در چارچوب NICE، اطلاعات زیر ارائه می‌شود: الف) نام نقش کاری؛ ب) حوزه تخصصی که نقش کاری در آن قرار دارد؛ پ) دسته‌ای که نقش کاری در آن قرار دارد؛ ج) شرح نقش کاری؛ د) فهرستی از وظایف که از یک فرد در آن نقش کاری انتظار می‌رود انجام دهد؛ و) فهرستی از دانش‌ها که از یک فرد در آن نقش کاری انتظار می‌رود درک کرده باشد؛ هـ) فهرستی از مهارت‌ها که از یک فرد در آن نقش کاری انتظار می‌رود برخوردار باشد؛ ی) فهرستی از توانایی‌ها که از یک فرد در آن نقش کاری انتظار می‌رود از خود نشان دهد.

هنگامی که سازمان‌ها الزامات امنیت سایبری خود را تعیین کردند (به‌عنوان مثال خودارزیابی داخلی انجام دادند)، می‌توانند به چارچوب NICE برای شناسایی نقش‌ها و وظایف کاری که به تحقق این الزامات کمک می‌کند، رجوع کنند. با شناسایی نقش‌های مورد نیاز و شناسایی شکاف بین دانش‌ها، مهارت‌ها و توانایی‌های مورد نیاز و موجود، سازمان‌ها می‌توانند نیازهای حیاتی برای مدیریت صحیح تهدیدهای امنیت سایبری فعلی و آینده را شناسایی کنند. از آن جایی که سازمان‌ها نیازهای حیاتی را شناسایی می‌کنند، تصمیم‌گیرندگان آموزش باید با در نظر گرفتن این نیازها و مطابق دانش، مهارت‌ها و توانایی‌های نقش‌ها در چارچوب NICE، مدارک تحصیلی و برنامه درسی را ارائه دهند تا یادگیرندگان بتوانند در فعالیت‌های یادگیری مناسب شرکت کنند.

۳ چارچوب مهارت‌های سایبری اروپا (ECSF)

چارچوب مهارت‌های سایبری اروپا که به اختصار با عنوان «چارچوب ECSF» شناخته می‌شود، در سال ۲۰۲۲ توسط آژانس امنیت سایبری اتحادیه اروپا (اِنیسا) ارائه شده است و هدف آن «تقویت فرهنگ امنیت سایبری اروپا از طریق ارائه یک زبان اروپایی مشترک در میان جوامع و

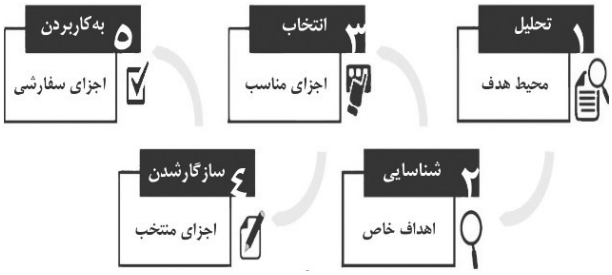
[1] Task

جدول ۱.

دسته	شرح دسته
تأمین ایمن (Securely Provision)	مفهوم‌سازی، طراحی، تهیه و یا ایجاد سیستم‌های فناوری اطلاعات ایمن با مسئولیت برای جنبه‌های توسعه سیستم و یا شبکه. این دسته شامل حوزه‌های تخصصی مدیریت رسیک، توسعه نرم‌افزار، توسعه سیستم‌ها، معماری سیستم‌ها، برنامه‌ریزی نیازمندی سیستم‌ها، تحقیق و توسعه فناوری، و آزمون و ارزشیابی است.
بهره‌برداری و نگهداری (Operate and Maintain)	فراهم کردن پشتیبانی، مدیریت و نگهداری لازم برای اطمینان از عملکرد و امنیت سیستم فناوری اطلاعات مؤثر و کارآمد. این دسته شامل حوزه‌های تخصصی خدمات مشتری و پشتیبانی فنی، مدیریت داده‌ها، مدیریت دانش، مدیریت سیستم‌ها، تحلیل سیستم‌ها و خدمات شبکه است.
نظارت و حاکمیت (Oversee and Govern)	رهبری، مدیریت، هدایت یا توسعه و حمایت تا سازمان بتواند به طور مؤثر کار امنیت سایبری را انجام دهد. این دسته شامل حوزه‌های تخصصی مدیریت امنیت سایبری، رهبری سایبری اجرایی، مشاوره حقوقی و وکالت، مدیریت برنامه/ پروژه و کسب، برنامه‌ریزی و سیاست استراتژیک، آموزش و آگاهی‌رسانی است.
محافظت و دفاع (Protect and Defend)	شناسایی، تحلیل و کاهش تهدیدها برای سیستم‌ها و یا شبکه‌های فناوری اطلاعات داخلی. این دسته شامل حوزه‌های تخصصی تحلیل دفاع سایبری، پشتیبانی از زیرساخت‌های دفاع سایبری، پاسخ به حادثه، و ارزیابی و مدیریت آسیب‌پذیری است.
تحلیل (Analyze)	بررسی و ارزیابی کاملاً تخصصی اطلاعات امنیت سایبری ورودی به منظور تعیین سودمندی آن‌ها برای سرویس‌های اطلاعاتی. این دسته شامل حوزه‌های تخصصی تحلیل همه منابع، تحلیل بهره‌برداری، تحلیل زبان، اهداف و تحلیل تهدید است.
جمع‌آوری و عملیات (Collect and Operate)	ارائه عملیات تخصصی ممانعت و فریب و جمع‌آوری اطلاعات امنیت سایبری که ممکن است برای توسعه اطلاعات مورد استفاده قرار گیرد. این دسته شامل حوزه‌های تخصصی عملیات مجموعه، برنامه‌ریزی عملیات سایبری و عملیات سایبری است.
بررسی (Investigate)	بررسی رویدادها یا جرایم امنیت سایبری مربوط به سیستم‌ها، شبکه‌ها و شواهد دیجیتال فناوری اطلاعات. این دسته شامل حوزه‌های تخصصی تحقیق سایبری و فارنزیک است.

برداشتن گامی اساسی به سمت آینده دیجیتالی اروپا» است. این چارچوب، ابزاری عملی برای شناسایی و بیان وظایف، شایستگی‌ها، مهارت‌ها، و دانش مرتبط با نقش‌های تخصصی امنیت سایبری اروپایی ارائه می‌دهد و یک درک مشترک میان افراد، کارفرمایان و ارائه‌دهندگان برنامه‌های آموزشی در سراسر کشورهای عضو اتحادیه اروپا ایجاد می‌کند. مخاطبان هدف این چارچوب تیم‌های رهبری سازمان‌ها، واحدهای منابع انسانی و امنیت سایبری، متخصصان امنیت سایبری، تازه‌واردان و علاقه‌مندان به سایبر، و همچنین ارائه‌دهندگان برنامه‌های یادگیری از همه نوع در محیط‌های دولتی و خصوصی، انجمن‌های بخش‌های مختلف صنعت، محققان بازار، و سیاست‌گذاران هستند.

چارچوب ECSF به گونه‌ای طراحی شده است که به اندازه کافی انعطاف‌پذیر باشد تا امکان سفارشی‌سازی را فراهم کند و به روشی ماژولار و انعطاف‌پذیر بر اساس نیازهای ذینفعان مختلف اعمال شود. استفاده



شکل ۲. راهنمای پنج مرحله‌ای مدولار برای اعمال چارچوب ECSF

خاص و کاربرد عملی به عوامل زیادی مانند دیدگاه بازار، اندازه سازمان، زمینه استفاده و هدف کلی بستگی دارد. به این ترتیب برای استفاده سفارشی از چارچوب در زمینه خاص مراحل شکل ۲ را باید انجام داد: الف) تحلیل وضعیت محیط مورد نظر؛ ب) شناسایی اهداف خاصی که باید به آن‌ها دست یافت؛ پ) انتخاب اجزای مناسب چارچوب؛ ج) تطبیق اجزای انتخاب‌شده با توجه به نیاز؛ د) اعمال اجزای سفارشی‌شده در محیط هدف.

چارچوب ECSF شامل مجموعه‌ای از ۱۲ نقش برای متخصصان امنیت سایبری است. هر نقش با استفاده از یک الگوی مشترک تعریف می‌شود که مجموعه‌ای از معیارهای کلیدی (یعنی عنوان، عنوان‌های جایگزین، شرح یا هدف اصلی نقش، مأموریت، وظایف اصلی، مهارت‌های کلیدی، دانش کلیدی، شایستگی‌های الکترونیکی) را در بر می‌گیرد. جدول ۲، ۱۲ نقش تعریف‌شده در این چارچوب را معرفی می‌کند.

در خصوص آموزش عالی، اِنیسا در این چارچوب یک فهرست تعاملی از مدارک امنیت سایبری در کشورهای منطقه اقتصادی اروپا ارائه داده است تا به نقطه مرجع اصلی برای همه شهروندان اروپایی تبدیل شود که به دنبال ارتقاء دانش و مهارت‌های امنیت سایبری خود از طریق مدرک تحصیلی عالی هستند. با این حال، به وضوح بیان می‌کند که «برای ایجاد یک چرخه که تطابق خوبی را بین عرضه نیروی کار و تقاضای بازار کار تضمین کند، به تلاش‌های بیشتری نیاز است و بخش دانشگاهی و کارفرمایان باید به طور کامل در توسعه نیروی کار امنیت سایبری ادغام شوند.»

۴ چارچوب مهارت‌های سایبری استرالیا (ASD)

از سال ۲۰۰۹، اداره سیگنال‌های استرالیا (ASD) از یک چارچوب داخلی استفاده می‌کرد که قابلیت‌هایی حرفه‌ای را در یک گروه شغلی گسترده و مربوط به یک حوزه مهارتی تعریف کرده بود. در سال ۲۰۱۸، چارچوب مذکور دوباره بررسی شد و در نتیجه این بررسی، چارچوب مهارت‌های سایبری استرالیا شکل گرفت که در سال ۲۰۱۹ منتشر شد. هدف این چارچوب «ایجاد یک دنیای برخط امن برای استرالیایی‌ها، کسب‌وکار آن‌ها و خدمات ضروری» است و به گونه‌ای طراحی شده که به عنوان یک سند راهنما مورد استفاده قرار بگیرد و در صورت نیاز، اجزای مختلف

جدول ۲. نقش‌ها در چارچوب ECSF

نقش	شرح نقش
مدیر ارشد امنیت اطلاعات (Chief Information Security Officer (CISO))	استراتژی امنیت سایبری سازمان و اجرای آن را مدیریت می‌کند تا اطمینان حاصل شود که سیستم‌ها، خدمات، و دارایی‌های دیجیتال به اندازه کافی امن هستند و محافظت می‌شوند.
پاسخگوی حوادث (Cyber Incident Responder)	بر وضعیت امنیت سایبری سازمان نظارت می‌کند و مسئول رسیدگی حوادث در طول حملات سایبری است.
مسئول حقوقی، سیاست و انطباق سایبری (Cyber Legal, Policy & Compliance Officer)	انطباق با استانداردهای مرتبط با امنیت سایبری، چارچوب‌های قانونی و نظارتی را بر اساس استراتژی و الزامات قانونی سازمان مدیریت می‌کند.
کارشناس اطلاعاتی تهدیدهای سایبری (Cyber Threat Intelligence Specialist)	جمع‌آوری، پردازش، تحلیل داده‌ها و اطلاعات برای تولید گزارش‌های اطلاعاتی عملی و انتشار آن‌ها برای ذینفعان هدف را برعهده دارد.
معمار امنیت سایبری (Cybersecurity Architect)	راه‌حل‌های امنیتی و کنترل‌های امنیت سایبری را برنامه‌ریزی و طراحی می‌کند.
حسابرس امنیت سایبری (Cybersecurity Auditor)	امنیت سایبری در اکوسیستم سازمان را ممیزی می‌کند و از انطباق با قوانین، مقررات، سیاست‌ها، الزامات امنیتی و استانداردهای صنعت اطمینان حاصل می‌کند.
مدرس امنیت سایبری (Cybersecurity Educator)	دانش امنیت سایبری، مهارت‌ها و شایستگی‌های انسان‌ها را بهبود می‌بخشد.
مجری امنیت سایبری (Cybersecurity Implementer)	راه‌حل‌های امنیت سایبری (سیستم‌ها، دارایی‌ها، نرم‌افزارها، کنترل‌ها و خدمات) را در زیرساخت‌ها و محصولات توسعه می‌دهد و/یا بهره‌برداری می‌کند.
پژوهشگر امنیت سایبری (Cybersecurity Researcher)	در حوزه امنیت سایبری پژوهش می‌کند و نتایج را در راه‌حل‌های امنیت سایبری می‌گنجاند.
مدیر ریسک امنیت سایبری (Cybersecurity Risk Manager)	ریسک‌های مرتبط با امنیت سایبری سازمان را در راستای استراتژی سازمان مدیریت می‌کند. فرآیندها و گزارش‌های مدیریت ریسک را توسعه، نگهداری و ابلاغ می‌کند.
بازرس فارنزیک دیجیتال (Digital Forensics Investigator)	اطمینان حاصل می‌کند که تحقیقات جرایم سایبری تمام شواهد دیجیتالی را برای اثبات فعالیت مخرب نشان می‌دهد.
آزمونگر نفوذ (Penetration Tester)	اثربخشی کنترل‌های امنیتی، آشکارسازی و استفاده از آسیب‌پذیری‌های امنیت سایبری و بحرانی‌بودن آن‌ها در صورت سوء استفاده توسط عوامل تهدید را ارزیابی می‌کند.

آن بتوانند برای برآورده کردن اهداف سازمانی و نیازهای نیروی کار پیاده‌سازی شوند.

اجزای اصلی چارچوب مهارت‌های سایبری استرالیا عبارتند از:

قابلیت‌ها و مهارت‌ها (۹ تا): قابلیت‌ها، گروه‌بندی گسترده مهارت‌های شغلی هستند. مهارت‌ها، دانش و تخصص‌های گروه‌بندی شده در یک

قابلیت هستند.

سطوح مهارت (۶ تا): سطح تسلط مورد انتظار برای انجام نقش یا مهارت هستند که عبارتند از: سطح ۱: فراگیر (دانش)؛ سطح ۲: مبتدی (فهم)؛ سطح ۳: کارورز (اجرا)؛ سطح ۴: کارورز ارشد (توانمندسازی)؛ سطح ۵: کارورز اصلی (مشاوره)؛ سطح ۶: کارورز متخصص (مبتکر و مطمئن).

نقش‌های سایبری (۹ تا): شغل، موقعیت یا عملکرد نیروی کار سایبری هستند. هر نقش با استفاده از یک الگوی مشترک تعریف می‌شود که مجموعه‌ای از قابلیت‌ها و مهارت‌ها و سطوح مورد انتظار آن‌هاست (که مطابق با سطح تسلط نقش متفاوت است).

مسیرهای شغلی دیجیتال (۴ تا): چگونگی استفاده از مهارت‌های فناوری اطلاعات و ارتباط در نقش‌های دیگر هستند و همچنین بیان می‌کنند که یک کارمند برای برتری در آن نقش‌ها به چه مهارت‌های جدیدی ممکن است نیاز داشته باشد. هدف مسیر شغلی دیجیتال، «انعطاف‌پذیر کردن گزینه‌های شغلی در داخل دولت با ارائه دیدی روشن به کارکنان از موقعیت شغلی خود و نحوه هدایت آینده بالقوه‌شان» است. در این مسیرها دو سؤال اصلی برای کاربران طراحی شده است: الف) چه مهارت‌ها و توانایی‌هایی دارید؟؛ ب) به چه مهارت‌ها و توانایی‌هایی نیاز دارید؟

مسیر رشد و یادگیری: راهنمایی‌هایی برای یادگیری مهارت‌های ارائه شده است که به منظور حمایت از رشد فنی و حرفه‌ای متخصصان سایبری طراحی شده است. این مسیر درکی از نتایج یادگیری و اهداف مورد نیاز برای توسعه مهارت‌ها در قابلیت‌های مختلف ارائه می‌کند و همچنین سطح تعریف شده مورد نیاز را شناسایی می‌کند تا با یادگیری رسمی و تجربی پیشنهادی تکمیل شود.

جدول ۳، قابلیت‌ها و مهارت‌ها و جدول ۴، نقش‌ها را در چارچوب مهارت‌های سایبری استرالیا معرفی می‌کند.

به طور کلی چارچوب مهارت‌های سایبری استرالیا، استخدام هدفمند متخصصان سایبری را امکان‌پذیر می‌سازد؛ مسیر رشد را برای کارکنان فعلی و آینده سایبری فراهم می‌کند؛ و مهارت‌ها، دانش‌ها، و ویژگی‌ها را با استانداردهای صنعتی ملی و بین‌المللی همسو می‌کند.

۵ ارزیابی و اثربخشی چارچوب‌های بین‌المللی آموزش و به‌کارگیری متخصصان امنیت سایبری

در چارچوب NICE، نقشه‌برداری بین نقش‌های کاری و مجموعه دانش، مهارت‌ها، توانایی‌ها و وظایف گسترده است. این چارچوب با تعریف ۵۲ نقش کاری، ۱۰۰۷ وظیفه، ۶۳۰ دانش و صدها مهارت و توانایی کامل‌ترین تصویر موجود از نیازهای حیاتی امنیت سایبری سازمان‌ها را ارائه می‌دهد. نقش‌های کاری، دانش و مهارت‌ها و سایر ویژگی‌های تعریف‌شده در چارچوب‌های ECSF و ASD به گستردگی چارچوب NICE

جدول ۳. قابلیت‌ها و مهارت‌ها در چارچوب ASD

قابلیت‌ها	مهارت‌ها
حکمرانی و استراتژی امنیت اطلاعات (Information Security Governance and Strategy)	حکمرانی؛ سیاست‌ها و استانداردها؛ استراتژی امنیت اطلاعات؛ تغییر رفتار؛ محیط قانونی و مقرراتی و انطباق؛ مدیریت شخص ثالث.
ارزیابی تهدید و مدیریت ریسک‌های اطلاعات (Threat Assessment and Information Risk Management)	هوش تهدید، ارزیابی و مدل‌سازی تهدید؛ ارزیابی ریسک؛ مدیریت ریسک اطلاعات.
توسعه و پیاده‌سازی سیستم‌ها (Systems Development and Implementation)	توسعه و مدیریت سیستم‌ها؛ طراحی سیستم‌ها؛ طراحی نرم‌افزار؛ برنامه‌نویسی/توسعه نرم‌افزار.
تضمین: حسابرسی، انطباق و آزمون (Assurance: Audit, Compliance and Testing)	حسابرسی داخلی و قانونی؛ نظارت بر انطباق و آزمون کنترل؛ ارزیابی امنیتی و آزمون عملکرد؛ آزمون نفوذ.
مدیریت امنیت عملیاتی (Operational Security Management)	مدیریت عملیات امن؛ عملیات امن و تحویل خدمات.
مدیریت حوادث، تحقیقات و فارنزیک (Incident Management, Investigation and Forensics)	تشخیص و تحلیل نفوذ؛ مدیریت حادثه، بررسی حادثه و پاسخ؛ فارنزیک.
تحقیق امنیت اطلاعات (Information Security Research)	تحقیق؛ تحقیق کاربردی.
مدیریت، رهبری، تجارت، و ارتباطات (Management, Leadership, Business and Communications)	پشتیبانی از استراتژی؛ به دست آوردن نتیجه؛ پشتیبانی از روابط کاری؛ یکپارچگی شخصیت؛ ایجاد ارتباط مستحکم.
مشاوره تخصصی (Specialist Advice)	مشاوره تخصصی.

نیست و حداقل‌های مورد نیاز را در نظر گرفته‌اند. چارچوب‌های اروپایی و استرالیایی، چارچوب NICE را به عنوان منبعی تکمیلی برای توسعه بیشتر معرفی و توصیه کرده‌اند. در واقع برای حالتی که نیروی کار امنیت سایبری گسترده است و نیاز به دانش و توانایی‌های جامع‌تری دارد، از چارچوب NICE کمک می‌گیرند.

اما آیا چاچوب NICE، به عنوان کامل‌ترین تصویر موجود می‌تواند همه نیازها را برطرف کند؟ محدودیت چارچوب NICE این است که از میان این همه دانش، مهارت و توانایی، کمتر از ۱۰ مورد، شایستگی اجتماعی یا کار گروهی را توصیف کرده است. این نشان می‌دهد که این چارچوب همچنان تصویر ناقصی از مهارت‌های نرم نیروی کار ترسیم می‌کند [۶، ۷]. یک فرآیند توسعه نیروی کار امنیت سایبری اگر جنبه اجتماعی رفتار انسانی در شبکه را نادیده بگیرد، بخش مهمی از حوزه سایبری را نادیده گرفته است. به عنوان مثال، پرورش استعداد در حوزه‌های سایبری مستلزم شناخت این موضوع است که افرادی که به این حوزه کشیده می‌شوند ممکن است دارای ویژگی‌ها و گرایش‌های روان‌شناختی اجتماعی متمایزی باشند که آن‌ها را به طور منحصربه‌فردی برای برتری در این فضا مناسب می‌سازد [۸، ۹]. علاوه بر این، درک رفتار انسان شامل نحوه معرفی ریسک به شبکه است و حملات سایبری اغلب مشروط به

جدول ۴. نقش‌ها در چارچوب ASD

نقش	شرح نقش
تحلیلگر تهدیدهای سایبری (Cyber Threat Analyst)	تحلیل دقیق رویدادهای سایبری، ارزیابی‌های اطلاعاتی و مشاوره حرفه‌ای و سیاستی را برای تهدیدهای سایبری شناسایی‌شده انجام می‌دهد.
تحلیلگر نفوذ (Intrusion Analyst)	برنامه‌ریزی، هماهنگی و انجام فعالیت‌های پیشگیرانه کشف تهدیدهای سایبری را بر اساس اطلاعات این تهدیدها برای شناسایی نفوذ بالقوه یا درک رفتار غیرعادی انجام می‌دهد.
تحلیلگر بدافزار (Malware Analyst)	عملکرد، منشاء و تأثیرات بالقوه بدافزار را از طریق مهندسی معکوس، توسعه و تحقیق سیستم‌های طراحی و اجزای نرم‌افزار تحلیل می‌کند تا از شبکه‌ها در برابر تهدیدهای مخرب دفاع کند.
پاسخگوی حوادث	به منظور اصلاح شبکه‌ها و ارائه توصیه‌هایی در جهت محافظت از امنیت سیستم‌ها، تحلیل و بررسی حوادث امنیت سایبری اغلب مخرب را انجام می‌دهد.
هماهنگ‌کننده عملیات (Operations Coordinator)	وظایف مرتبط با حوادث امنیت سایبری را در تیم‌های مختلف برای واکنش به حادثه و عملیات شکار، از جمله تعیین اولویت‌ها و تعامل با مشتریان، مدیریت می‌کند.
آزمونگر نفوذ	با استفاده از تحلیل فنی عمیق ریسک‌ها و آسیب‌پذیری‌ها، تهدیدهای سایبری را شبیه‌سازی می‌کند تا کاستی‌ها در کنترل‌های امنیتی فنی را شناسایی کند.
ارزیاب آسیب‌پذیری (Vulnerability Assessor)	سیستم‌های اطلاعاتی را برای آسیب‌پذیری‌های امنیتی واقعی یا بالقوه بررسی می‌کند، و تهدید انواع دستگاه‌های الکترونیکی را توضیح می‌دهد.
مشاور و ارزیاب امنیت سایبری	مشاوره و راهنمایی فنی، حرفه‌ای و سیاست دقیق در مورد کاربرد و عملکرد کنترل‌های امنیتی رویه‌ای ارائه می‌دهد.

بهره‌برداری از رفتار شناخته‌شده انسانی است [۱۰].

چارچوب NICE و ECSF، برخلاف چارچوب ASD، سطوح تخصص (مانند پایه، متوسط، پیشرفته) را تعریف نمی‌کنند و چنین ویژگی‌هایی را به منابع دیگر واگذار می‌کنند. ویژگی منحصربه‌فرد چارچوب ECSF، امکان سفارشی‌سازی و انعطاف‌پذیری بالای آن است (به دلیل آنکه برای سراسر کشورهای عضو اتحادیه اروپا تعریف شده است). این در حالی است که به عنوان مثال در چارچوب NICE، اگر چه برای پشتیبانی از اهداف جدید، می‌توان نقش کاری جدید تعریف کرد اما درباره تغییر نام و شرح یک نقش کاری موجود به کاربران هشدار داده شده چرا که ممکن است منجر به ناهماهنگی شود [۳].

برای بررسی اثربخشی این چارچوب‌های بین‌المللی می‌توان به شاخص‌ها و آمارهای جهانی رجوع کرد. بر اساس شاخص جهانی امنیت سایبری [1] در سال ۲۰۲۰، ایالت متحده آمریکا با ۱۰۰ امتیاز از مجموع ۱۰۰ امتیاز در رتبه اول، استرالیا با ۹۷/۴ امتیاز در رتبه دوازدهم و تعدادی از کشورهای عضو اتحادیه اروپا از جمله استونی، اسپانیا و فرانسه در میان ده رتبه برتر قرار گرفته‌اند [۱۱]. شاخص جهانی امنیت سایبری

[1] Global Cybersecurity Index (GCI)

جدول ۵. برآورد نیروی کار امنیت سایبری [۲]

	۲۰۱۹	۲۰۲۰	۲۰۲۱	۲۰۲۲
ایالات متحده آمریکا	۸۰۴, ۷۰۰	۸۷۹, ۱۵۷	۱, ۱۴۲, ۴۶۲	۱, ۲۰۵, ۸۱۲
اروپا	۵۴۳, ۰۰۰	۸۳۰, ۱۸۷	۱, ۰۸۶, ۱۴۶	۱, ۲۲۲, ۱۵۴
استرالیا	۱۰۷, ۰۰۰	۱۰۸, ۹۵۰	۱۳۴, ۶۹۰	۱۴۳, ۶۸۰

جدول ۶. شکاف نیروی امنیت سایبری [۲]

	۲۰۱۹	۲۰۲۰	۲۰۲۱	۲۰۲۲
ایالات متحده آمریکا	—	۳۵۹, ۲۳۶	۳۷۷, ۰۰۰	۴۱۰, ۶۹۵
اروپا	۲۹۱, ۰۰۰	۱۶۸, ۰۰۰	۱۶۸, ۰۰۰	۳۱۷, ۰۵۰
استرالیا	—	۲۷, ۱۹۲	۲۵, ۰۰۰	۳۹, ۴۹۶

یک مرجع قابل اعتماد است که تعهد کشورها به امنیت سایبری را بر اساس پنج رکن اساسی زیر ارزیابی می‌کند: الف) اقدامات قانونی، ب) اقدامات فنی، پ) اقدامات سازمانی، ج) ظرفیت‌سازی، و د) همکاری. این ارکان ماهیت به‌هم‌پیوسته‌ای دارند و نمی‌توان آن‌ها را به‌صورت مجزا در نظر گرفت، اما رکن چهارم (ظرفیت‌سازی) بیشتر به آموزش و به‌کارگیری متخصصان امنیت سایبری مربوط می‌شود.

برآورد و شکاف نیروی کار امنیت سایبری و شکاف‌های مهارتی در میان متخصصان امنیت سایبری در گزارش‌های سالانه ISC^2 [۲] و ISACA [۳] معیارهای دیگری است که می‌توان برای بررسی اثربخشی در نظر گرفت. این گزارش‌ها بر اساس داده‌های نظرسنجی‌های برخط در سراسر آمریکای شمالی، اروپا، آمریکای لاتین، آسیا و اقیانوسیه تهیه‌شده و به مطالعه نیروی کار امنیت سایبری پرداخته‌اند. جدول ۵ برآورد نیروی کار و جدول ۶ شکاف نیروی کار امنیت سایبری در ایالات متحده آمریکا، اروپا و استرالیا را برحسب تعداد نفر نشان می‌دهد.

همانطور که مشاهده می‌شود، از سال ۲۰۲۱ به سال ۲۰۲۲ اروپا با ۱۲٪، بیشترین افزایش نیروی کار امنیت سایبری تجربه کرده و بعد از آن استرالیا ۷٪ و آمریکا ۵٪ افزایش نیروی کار را تجربه کرده‌اند.

با این که نیروی کار امنیت سایبری به سرعت در حال رشد است، سرعت رشد تقاضا بیشتر است. آمریکا و اروپا به ترتیب با کمبود حدود ۴۰۰ هزار نفر و ۳۰۰ هزارنفر نیروی متخصص در سال ۲۰۲۲ در بالای جداول آماری موجود قرار دارند. هم‌اکنون درحدود ۴ میلیون نفر کمبود نیروی متخصص امنیت سایبری در کشورهای توسعه‌یافته و در حال توسعه وجود دارد که به دلیل پرداخت دستمزدهای بالا و امکانات اقتصادی مناسب شاهد سیل مهاجرت از کشورهای ضعیف‌تر به قوی‌تر هستیم [۲]. این امر شکاف بزرگ امنیتی برای تعداد زیادی از کشورها ایجاد کرده است و آن‌ها را به سمت ارائه طرح و برنامه ظرفیت‌سازی نیروی انسانی متخصص امنیت سایبری رهنمون شده است. تحلیل شکاف نیروی کار امنیت سایبری (ISC^2) تشریح می‌کند که کشورها در چه وضعیتی قرار دارند، در چه وضعیتی باید باشند (شرایط ایده‌آل آینده) و چگونه می‌توان شکاف بین این دو را از بین برد.

[2] International Information Systems Security Certification Consortium

[3] Information Systems Audit and Control Association

در خصوص شکاف‌های مهارتی نیز پاسخ‌های نظرسنجی ISACA در سال‌های ۲۰۲۱ و ۲۰۲۲ نشان می‌دهد که مهارت‌های نرم و محاسبات ابری به ترتیب اولین و دومین شکاف بزرگ مهارت در میان متخصصان امنیت سایبری است. شکاف‌های قابل توجه دیگر شامل اجرای کنترل‌های امنیتی، کدگذاری، توسعه نرم‌افزار، موضوعات مرتبط با داده‌ها و موضوعات مرتبط با شبکه است [۱۲].

۶ نتیجه‌گیری

کمبود نیروی کار و شکاف مهارتی امنیت سایبری یک نگرانی عمده برای توسعه اقتصادی و امنیت ملی است. در این مقاله، ابتدا مهم‌ترین چارچوب‌های بین‌المللی آموزش و به‌کارگیری متخصصان امنیت سایبری به طور خلاصه معرفی و ویژگی‌های کلیدی آن‌ها بررسی و تحلیل شدند. همچنین مزایا و معایب هر چارچوب ارزیابی شد و نشان داده شد که این چارچوب‌ها نقش بسیار تأثیرگذاری در رسیدگی به چالش‌های سازمان‌های جهانی در ایجاد و توسعه منابع انسانی متخصص امنیت سایبری داشته‌اند.

پیشرفت فناوری‌های اطلاعات و ارتباطات موجب شده است حوزه امنیت از این قافله پرشتاب جا بماند. از طرفی گستردگی فناوری‌ها، موجب گستردگی و نیاز به تخصص‌های متنوع امنیت سایبری شده است و لازم است کشور همانند رویکردهای جهانی در زمینه ظرفیت‌سازی نیروی انسانی متخصص امنیت سایبری اقداماتی انجام دهد. دیگر نمی‌توان انتظار داشت با دو یا چند نوع تخصص امنیت اطلاعات و امنیت شبکه همه نیازهای کشور را پوشش داد و بتوان در مقابل تهدیدها و آسیب‌پذیری‌های متنوع و گسترده مقاومت نمود.

در دهه‌های اخیر موضوع امنیت سایبری در سیاست‌گذاری‌های کلان در قالب سیاست‌های کلی پدافند غیرعامل (۱۳۸۹)، سیاست‌های کلی امنیت فضای تولید و تبادل اطلاعات و ارتباطات (۱۳۸۹)، وظایف شورای عالی فضای مجازی (۱۳۹۴) و سیاست‌های کلی برنامه ششم توسعه (۱۳۹۴) مورد توجه قرارگرفته‌اند و وزارت علوم و بخش خصوصی در زمینه آموزش امنیت سایبری تلاش‌هایی داشته‌اند. با این وجود، همچنان متولی کلیدی و چارچوب و نظام جامعی برای آموزش و به‌کارگیری متخصصان امنیت سایبری در ایران وجود ندارد چه برسد به آنکه بتوان چالش‌های موجود، آمار مناسب از تعداد متخصصان امنیت سایبری کنونی و تعداد مورد نیاز در بخش‌های مختلف را استخراج کرد.

متولیان ظرفیت‌سازی و تربیت نیروی انسانی در کشور باید به این نقطه از درک برسند که آموزش امنیت سایبری هزینه نیست بلکه پیشگیری از هزینه‌های غیرقابل جبران برای کشور و زیرساخت‌های حیاتی است. از این رو برای کشور و بر اساس مطالعات جهانی و کشور یک برنامه ملی ظرفیت‌سازی و تربیت نیروی انسانی در حوزه امنیت سایبری تحت اجرای یک متولی واحد پیشنهاد می‌گردد. برای شروع، الگوبرداری از چارچوب مهارت‌های سایبری اروپا با توجه به سادگی و انعطاف‌پذیری آن می‌تواند مناسب باشد. برای این منظور باید از راهنمای پنج مرحله‌ای مدولار برای اعمال چارچوب کمک گرفت و مؤلفه‌های مناسب را به گونه‌ای انتخاب کرد و با فضای آموزشی و بازار کار کشور تطبیق داد که موارد زیر را مدنظر قرار دهد:

- جامعیت و درنظرگرفتن نیازمندی همه ذینفعان.
- الزام نهادهای آموزشی کشور (وزارت علوم، وزارت آموزش و پرورش، فنی و حرفه‌ای و بخش خصوصی) به ارائه برنامه مدون آموزشی مدرن در زمینه امنیت سایبری.
  - تربیت مدرسان آموزش امنیت سایبری.
  - آموزش متنوع امنیت سایبری در دانشگاه‌ها.
  - آموزش امنیت سایبری به عنوان یک درس اجباری برای همه رشته‌های دانشگاهی.
  - شروع آموزش از مهدکودک تا پایان متوسطه با پوشش دانش‌آموزان، والدین و معلمان.
- انطباق برنامه‌های آموزشی با رویکردها و چارچوب‌های بین‌المللی برای پیشگیری از حمله‌ها و تهدیدها.
- آموزش حرفه‌ای مبتنی بر گواهی‌نامه‌های معتبر.
- داشبورد حاکمیتی از وضعیت آماری تربیت، به‌کارگیری و جذب نیروی امنیت سایبری.
- پشتیبانی بخش خصوصی و شرکت‌ها از تأمین نیروی انسانی خبره در امنیت سایبری به وسیله معرفی زمینه‌های کاری، آموزشی و جذب.
- تهیه محتوای رایگان و آگاهی‌رسانی به‌روز برای مخاطبان عمومی.
- تولید محتوای رایگان حرفه‌ای برای بازآموزی و آموزش نیروهای متخصص فناوری اطلاعات و ارتباطات.
- آموزش‌های ضمن خدمت دوره‌ای و به‌روز برای کارکنان بخش‌های دولتی و عمومی.
- آموزش اجباری امنیت سایبری و آموزش دوره‌ای برای کسب‌وکارها.
- برگزاری همایش‌ها و کنفرانس‌های دوره‌ای.
- تعیین متولی حاکمیتی برای نظارت و ارائه طرح عمل به همه دستگاه‌ها و ذینفعان.

سپاسگزاری

از پژوهشکده امنیت ارتباطات و فناوری اطلاعات و پژوهشگاه ارتباطات و فناوری اطلاعات برای در اختیارگذاشتن نتایج پروژه پژوهشی در حوزه ظرفیت‌سازی و تربیت نیروی انسانی امنیت سایبری تشکر می‌شود.

مراجع

[1] Ciuchi, C. Building a resilient ecosystem for cybersecurity in education. in *Cybersecurity - Challenges and Perspectives in Education*, pp. 141–152. Academica Greifswald, 2020.

[2] ISC^2 (2022) cybersecurity workforce study

2022. https://www.isc2.org/Research/Workforce-Study. Accessed: 29 December 2022.

[3] Newhouse, William, Keith, Stephanie, Scribner, Benjamin, and Witte, Greg. National initiative for cybersecurity education (nice) cybersecurity workforce framework. *NIST special publication*, 800(2017):181, 2017.

[4] for Cybersecurity, European Union Agency. *European Cybersecurity Skills Framework (ECSF): User Manual*. ENISA_2, 2022.

[5] Australian government, australian signals directorate, asd cyber skills framework. https://www.cyber.gov.au/sites/default/files/2020-09/ASD-Cyber-Skills-Framework-v2.pdf. Accessed: 2022-08-23.

[6] Seong, Jee Young, Kristof-Brown, Amy L, Park, Won-Woo, Hong, Doo-Seung, and Shin, Yuhyung. Person-group fit: Diversity antecedents, proximal outcomes, and performance at the group level. *Journal of Management*, 41(4):1184–1213, 2015.

[7] Dawson, Jessica and Thomson, Robert. The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in psychology*, 9:744, 2018.

[8] Fontenele, Marcelo and Sun, Lily. Knowledge management of cyber security expertise: an ontological approach to talent discovery. in *2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)*, pp. 1–13. IEEE, 2016.

[9] Furnell, Steven. The cybersecurity workforce and skills. *Computers & Security*, 100:102080, 2021.

[10] Bell, Richard Scott, Vasserman, Eugene Y, and Sayre, Eleanor C. A longitudinal study of students in an introductory cybersecurity course. in *2014 ASEE Annual Conference & Exposition*, pp. 24–61, 2014.

[11] Global cybersecurity index 2020. International Telecommunication Union (ITU). 2020.

[12] Isaca state of cybersecurity. 2022.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2023, Volume 21, Number 2 (pp. 24–32)
https://monadi.isc.org.ir

Presented at the ISCISC 2023 in Iranian Research Organization for Science & Technology, Tehran, Iran

Analysis of global trends in providing educational frameworks for training cyber security professionals★

Ahmad Rahdari [1,2] and Mohammad Hesam Tadayon [*,2]

[1] *University of Shiraz, Shiraz, Iran*
[2] *Iran Telecommunication Research Center, Tehran, Iran*

ARTICLE INFO.

Keywords:
Cybersecurity
Education
Training
Skill
Knowledge
Ability
Work role
Human Recourse Development
The US Cybersecurity Workforce Framework (NICE)
European Cybersecurity Skills Framework (ECSF)
Australian Cyber Skills Framework (ASD)

dor: 20.1001.1.24763047.1402.12.2.3.9

Type: Research paper

ABSTRACT

Cyber security education in Iran is not aligned with global standards and approaches, and three factors, the educational sector, training applicants and stakeholders, and companies do not have proper knowledge of the required specializations and work roles. Different specializations in cyber security work fields in Iran do not match the international standard puzzles and this has created security holes in the country's cyber ecosystem. People working in cyberspace need a combination of domain-specific knowledge, skills, abilities, and other expertise to be as reliable and resilient as the technologies they work with. At the international level, several frameworks have been designed and implemented for the training and employment of cybersecurity professionals. The most important of which are the US National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, the European Cybersecurity Skills Framework (ECSF), and the Australian Signals Directorate (ASD) Cyber Skills Framework. In this paper, each of these frameworks is briefly introduced and their key features, including purpose, structure, and components, are reviewed and analyzed. In addition, their effectiveness in handling global organizations' challenges in creating and developing cybersecurity expert human resources is evaluated and analyzed critically. This review highlights the strengths and weaknesses of each framework, shows the propinquity of one of the frameworks to Iran's educational and labor markets, and provides recommendations for designing a national framework for training and employing cybersecurity professionals, which can be a great lesson for the country to ensure that the necessary measures are taken as soon as possible by those in charge.

★ The ISCISC 2023 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: a.rahdari@hafez.shirazu.ac.ir (Ahmad Rahdari), tadayon@itrc.ac.ir (Mohammad Hesam Tadayon)