ابعاد و مؤلفه‌های ساختاردهی فرهنگ امنیت سایبری در سازمان‌ها

بهمن جهانی[۱]، سید نصیب‌اله دوستی‌مطلق[۲]

[۱]دانشجوی دکتری مدیریت راهبردی فضای سایبر گرایش امنیت سایبری، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران
bhjahani@gmail.com
[۲]استادیار، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران
doustimotlagh@chmail.ir

چکیده

نتایج بدست آمده از تحقیقات مراکز پژوهشی و خدمات امنیت سایبری نشان می‌دهد که توسعه فناوری‌های زیرساختی، تدوین و ابلاغ دستورالعمل‌های امنیت سایبری و تربیت متخصصین این حوزه، در دفع تهدیدات چندان موفق نبوده و همچنان خسارت و آسیب به سرمایه‌های سایبری سازمان‌ها رو به افزایش است. یافته‌های این تحقیقات نشان می‌دهد که کارکنان در ایجاد تهدیدات امنیت سایبری سازمان‌ها یا تأمین آن نقش بسیار مهمی دارند که عدم توجه به این موضوع از مهمترین دلایل شکست برنامه‌های امنیت سایبری است. براین‌اساس حوزه جدیدی تحت عنوان فرهنگ امنیت سایبری، به جهت کلیدی بودن فرهنگ در شکل‌دهی به رفتار کارکنان، مطرح گردیده است. این تحقیق در پی یافتن ابعاد و مؤلفه‌های کلیدی و اثرگذار در ایجاد و ساختاردهی فرهنگ امنیت سایبری در سازمان‌ها است. این پژوهش از نوع کاربردی بوده و با استفاده از روش توصیفی تحلیلی با استناد به منابع کتابخانه‌ای، و تحلیل و بررسی اسناد این حوزه و بهره‌گیری از نظرات خبرگان، به دنبال ابعاد و مؤلفه‌های کلیدی ایجاد فرهنگ امنیت سایبری است. نتایج حاصل از تحقیق در سطح راهبردی ۵ بعد و ۱۶ مؤلفه، سطح عملیاتی ۷ بعد و ۱۸ مؤلفه و سطح تکنیکی ۴ بعد و ۸ مؤلفه را بر فرهنگ امنیت سایبری سازمان‌ها مؤثر دانسته است.

کلمات کلیدی: فرهنگ امنیت سایبری، مدل فرهنگ امنیت سایبری، فرهنگ سازمانی.

۱ مقدمه

پس از بررسی حوادث سایبری در سال‌های اخیر، محققین دریافتند که امنیت سایبری صرفاً در مؤلفه‌های سخت‌افزاری، نرم‌افزاری و زیرساخت‌ها خلاصه نمی‌شود و انسان‌ها مؤلفه بسیار مهمی هستند که هم در مؤلفه‌های دیگر نقش مستقیم و غیرمستقیم دارند و هم خود، مؤلفه مستقل و مؤثر هستند. بنابراین مقوله

ایجاد تغییر در رفتار و نگرش کارکنان در سازمان‌ها در همسویی با امنیت سایبری مطرح گردید. البته در دستورالعمل‌ها و نظامات پیشین نیز توجه به عوامل انسانی وجود داشته، لیکن فرض آن‌ها در رابطه با عامل انسانی به عنوان یک مؤلفه فرعی بوده و برنامه‌های امنیتی کارکنان نیز به نسبت همین دیدگاه در آموزش‌های کوتاه‌مدت و ابتدایی خلاصه شده است.

از جمله عوامل تأثیرگذار و درعین حال کلیدی در شکل‌گیری بینش و رفتار کارکنان، فرهنگ سازمان است. لذا تبدیل امنیت سایبری در سازمان‌ها به فرهنگ، یکی از روش‌های ایجاد همسویی کارکنان با سیاست‌های امنیت سایبری است و بدین جهت مقوله فرهنگ امنیت سایبری[1] به عنوان یکی از راهکارهای مناسب در تقویت جایگاه مؤلفه انسانی در زنجیره تأمین امنیت سایبری پیشنهاد شده است.

فرهنگ امنیت سایبری سازمان‌ها به دانش، باورها، ادراکات، نگرش‌ها، مفروضات، هنجارها و ارزش‌های افراد در رابطه با امنیت سایبری و نحوه انعکاس آنها، در رفتار افراد نسبت به فضای سایبر اشاره دارد. موضوع فرهنگ سازمانی امنیت سایبری، ملاحظات امنیت سایبری را بخشی جدایی‌ناپذیر از شغل، عادات و رفتار کارکنان می‌داند و آنها را جزئی از اقدامات روزمره تلقی می‌کند. از طرفی با توجه به اینکه محیط‌های کسب‌وکار دائماً در حال تغییرند، لذا سازمان‌ها نیز باید به طور فعال فرهنگ امنیت سایبری خود را در پاسخ به فناوری‌ها و تهدیدات جدید و همچنین اهداف، فرآیندها و ساختارهای متغیر خود حفظ و تطبیق دهند. یک فرهنگ امنیت سایبری موفق، تفکر امنیتی همه کارکنان (از جمله تیم امنیتی) را شکل می‌دهد، انعطاف‌پذیری را در برابر همه تهدیدات سایبری بهبود می‌بخشد، و در عین حال از تحمیل مراحل و هزینه‌های امنیتی سنگین که مانع انجام مؤثر وظایف کلیدی کسب‌وکار است، پرهیز می‌کند [۸].

ایجاد فرهنگ امنیت سایبری مانند ایجاد و توسعه هر کلان طرحی در سازمان‌ها نیازمند برنامه‌ریزی است. برنامه‌ریزی نیز بدون شناخت دقیق مفهوم و درک ابعاد و مؤلفه‌های کلیدی و اثرگذار امکان‌پذیر نمی‌باشد. بدین منظور، این تحقیق بدنبال یافتن پاسخ به این پرسش است که جهت ایجاد فرهنگ امنیت سایبری کدامیک از ابعاد و مؤلفه‌های سازمان باید مدنظر قرار گرفته و نسبت به تغییر و همسو نمودن آنها برنامه‌ریزی لازم صورت پذیرد.

در راستای تحقق هدف تحقیق ابتدا در ادبیات نظری، تعاریف و مفاهیم فرهنگ سازمانی و فرهنگ امنیت سایبری مرور شده و سپس ضرورت توجه به این موضوع مدنظر قرار گرفته است. از آنجایی که تدوین مدل‌ها، مبتنی بر ابعاد و مؤلفه‌هاست، لذا در ادامه، مدل‌های مهمی که در حوزه ایجاد فرهنگ امنیت سایبری مطرح هستند، بررسی شده است. براساس مدل‌ها، ابعاد و مؤلفه‌ها استخراج شده و پس از طی فرایند تجزیه و تحلیل و تأیید خبرگان، در فصل یافته‌ها، ساختار کامل آنها ارائه شده است. نهایتاً در فصل نتیجه‌گیری توضیحاتی در رابطه با تحقیق و یافته‌های آن و تأثیر این تحقیق در حوزه‌های کاربردی و علمی امنیت سایبری ارائه شده است. همچنین پیشنهادهایی برای ادامه مسیر تحقیق و افزایش غنای علمی این حوزه ارائه گردیده است.

[1] Cyber Security Culture

۲ مبانی نظری و پیشینه تحقیق

۱.۲ پیشینه تحقیق

در رابطه با موضوع فرهنگ امنیت سایبری، تحقیقات مختلف و متنوعی در سال‌های اخیر خصوصاً از سال ۲۰۱۷ به بعد انجام شده که برخی از این تحقیقات که ارتباط بیشتری با این پژوهش دارند عبارتند از:

میکائیل وایل در مقاله خود که در راستای یافتن فرهنگ امنیت سایبری و رابطه آن با ابعاد مختلف سازمان انجام شده، ضمن تأیید رابطه فرهنگ سازمان با امنیت سایبری، مؤلفه‌های تعهد رهبر و چشم‌انداز سازمان را بر همسوسازی هنجارها، اقدامات رهبری و رفتار کارکنان در رابطه با امنیت سایبری مؤثر دانسته است [۱۱].

اخیار نصیر و همکاران در مقاله خود، عوامل ایجاد فرهنگ امنیت سایبری را در سازمان به چهار سطح تقسیم کرده‌اند؛ در سطح اول سیاست‌ها، دسترسی‌ها و مقررات، در سطح دوم و پائین‌تر، اهداف، راهبردها و اقدامات، و در سطح سوم هنجارها و رفتارهای امنیتی و در سطح آخر مجموعه اقدامات آگاهی و افزایش دانش در کارکنان را ذکر نموده‌اند [۱۲].

لین و وورن چارچوبی را در قالب سه فاز برای ایجاد امنیت سایبری در سازمان‌های نظامی پیشنهاد داده‌اند که در این تحقیق در فاز اول مؤلفه‌های سیاست‌ها، آموزش، برنامه‌ریزی و در فاز دوم، تمرینات سایبری، ارزیابی امنیت سایبری و در فاز سوم نیز که اجرای برنامه‌های تدوین شده است، مؤلفه‌ی آگاه‌سازی و ارزیابی را ارائه نموده‌اند [۱۰].

راملوکان و همکاران در تحقیق خود، چارچوب تغییرات مدیریتی در سازمان را جهت استقرار فرهنگ امنیت سایبری در قالب ۳ بعد در نظر گرفته‌اند: ۱) منابع: با مؤلفه‌های فناوری‌ها – فرایندها – افراد، ۲) قابلیت‌ها: با مؤلفه‌های کنترل‌های تکنیکی – حکمرانی – فرهنگ، ۳) مزیت رقابتی: با مؤلفه افزایش تاب‌آوری [۱۳].

۲.۲ مفاهیم و تعاریف

فرهنگ سازمانی

قبل از پرداختن به مفهوم فرهنگ امنیت سایبری باید منظور از فرهنگ سازمانی که مفهومی کلان‌تر است، مشخص گردد. برای فرهنگ سازمانی تعاریف متعدد و مختلفی در منابع ذکر شده که برخی از آنها عبارتند از [۱]:

- یک نظام اعتقادی، که بین اعضای یک سازمان مشترک است (Spender).
- ارزش‌های قوی که به‌طور گسترده مشترک است (Relly).
- مجموعه‌ای از باورهای مشترک و دائم که از طریق ابزارهای متنوع مادی منتقل می‌شوند و در زندگی افراد ایجاد معنا و مفهوم می‌کند (Kouzes, calwall and Posner).

- یک سلسله از نهادها، تشریفات، و اسطوره‌هایی که منتقل‌کننده ارزش‌ها و باورهای اساسی آن سازمان به کارکنانش می‌باشد (Petera and Waterman).

به‌طور کلی فرهنگ در سازمان، نقش‌های گوناگونی ایفا کرده و تعیین‌کننده مرز فکری و ارزشی سازمان است، نوعی احساس هویت در اعضای سازمان به‌وجود می‌آورد، باعث می‌شود نوعی تعهد جمعی در افراد به وجود آید، موجب ثبات و پایداری سازمان به‌عنوان یک سیستم اجتماعی می‌شود و بالاخره فرهنگ یک عامل قوی کنترل، کنترل مالی و بودجه‌ای در سازمان است [۲].

همچنین فرهنگ سازمانی به‌عنوان «ارزش‌ها و رفتارهایی تعریف می‌شود که به منحصر به‌فرد شدن محیط اجتماعی و روانی یک سازمان کمک می کند» [۲].

فرهنگ در سازمان تابع برخی نشانه‌ها و علائم است که برخی از آنها از نظر ادگار شاین عبارتند از [۲]:

۱. مقررات رفتاری مشاهده شده در تعاملات افراد با یکدیگر
۲. نُرم‌ها و هنجارهای گروهی
۳. ارزش‌های حمایت‌شده
۴. روش‌ها، عادت‌ها، تفکر، الگوهای ذهنی یا پارادایم‌ها
۵. مثل‌ها و استعاره‌ها

فرهنگ امنیت سایبری

اصطلاح «فرهنگ امنیت سایبری» در سال‌های اخیر مطرح شده و تعاریف مختلفی نیز برای آن ذکر شده است. اما تعریفی که مورد اجماع بیشتری است عبارت است از:

«فرهنگی که هر مشارکت‌کننده‌ای در جامعه اطلاعاتی، متناسب با نقش خود، از خطرات امنیتی مربوطه و اقدامات پیشگیرانه آگاه باشد، مسئولیت را بر عهده گیرد و برای بهبود امنیت سیستم‌ها و شبکه‌های اطلاعاتی خود گام بردارد» [۷].

تعاریف جامع دیگر در این رابطه توسط ICAO[۲] ارائه شده است. در این تعریف فرهنگ امنیت «مجموعه‌ای از هنجارها، باورها، ارزش‌ها، نگرش‌ها و مفروضاتی است که در عملکرد روزانه یک سازمان نهفته است و توسط اعمال و رفتار همه نهادها و پرسنل درون سازمان منعکس می‌شود و شامل امنیت همه سازمان است».

[۲] سازمان بین‌المللی هوانوردی کشوری

۳.۲ کارکنان و آسیب‌پذیری‌های سایبری

با مطالعه نقش کارکنان در آسیب‌پذیری‌های سایبری می‌توان به لزوم ایجاد فرهنگ سازمانی امنیت سایبری دست یافت، چرا که کارکنان و فرهنگ سازمانی دو موجودیت غیرقابل تفکیک و در تعامل با یکدیگرند. لذا بررسی آسیب‌پذیری‌های سایبری با منشأ کارکنان و ارتباط آن با فرهنگ سازمانی اجتناب ناپذیر است.

براساس تحقیقاتی که حاصل تحلیل داده‌های حوادث سایبری در شرکت‌ها و سازمان‌های مختلف دنیاست و توسط شرکت کسپرسکی[۳] انجام شده است، به‌طور کلی آسیب‌پذیری‌هایی که توسط کارکنان به‌صورت مستقیم یا غیرمستقیم ایجاد می‌گردند عبارتند از [۹]:

۱. خطا، بی‌احتیاطی و ناآگاهی کارکنان
۲. بی‌مسئولیتی کارکنان
۳. نداشتن دید جامع و کل‌نگر به امنیت اطلاعات در سازمان
۴. نادیده‌گرفتن امنیت اطلاعات در فرایندهای سازمان
۵. خطای تغییرات حفاظتی در زیرساخت‌های فنی توسط متخصصین امنیت
۶. خطای تدوین‌کنندگان سیاست‌های امنیت اطلاعات
۷. نادیده‌گرفتن تهدیدات و نشناختن صحیح سرمایه‌های سایبری و وابسته به سایبر
۸. خطای مدیران در نادیده گرفتن اهمیت جایگاه افسر امنیت سایبری در سازمان
۹. هزینه‌انگاری امنیت سایبری

۴.۲ ضرورت ایجاد فرهنگ امنیت سایبری

در ایجاد یک فرهنگ باید نسبت به چهار واقعیت آگاهی کامل داشت [۵]:

۱. در افزایش سطح آگاهی و تغییر رفتار، فرهنگ نقشی مهم ایفا می‌نماید.
۲. هر کسی جهان را از دریچه فرهنگ خود تفسیر می‌کند.
۳. فرهنگ درست و غلط وجود ندارد و فقط تفسیرهای متفاوت از یک وضعیت وجود دارد.
۴. کدام فرهنگ‌ها نقش آفرینند و مفروضات اساسی و مورد حمایت در آنها کدامند؟

[3] Kaspersky

مطابق نتایج تحقیقات ارائه شده، عوامل انسانی عامل اکثر نقض‌های داده در سازمان‌ها هستند، در حالی‌که سازمان‌ها دارای سیاست‌های امنیت سایبری هستند ولی کارمندان، آنها را به‌عنوان دستورالعمل‌های راهنما می‌بینند و نه قوانین لازم‌الاجرا [۳]. در مقابل، توسعه فرهنگ امنیت سایبری به جای تلاش برای وادار کردن افراد به رفتار ایمن، در بینش آنها تغییر ایجاد کرده، آگاهی امنیتی و درک مخاطرات را تقویت می‌کند و صمیمیت را در فرهنگ سازمانی به جای استفاده از قوانین سخت‌گیرانه و خشک حفظ می‌کند [۳].

تفاوت اصلی بین آگاهی امنیتی و فرهنگ امنیتی این است که فرهنگ چیزی بیش از آگاهی است. فرهنگ امنیتی ترکیبی از افراد، سیاست و فناوری است. نکته کلیدی این است که آگاهی یکی از مؤلفه‌های فرهنگ‌سازی است و نباید، تنها راه در رسیدن به سطح مطلوب پیشگیری از مخاطرات سایبری عوامل انسانی، در نظر گرفته شود [۳].

بنابراین هدف اصلی فرهنگ امنیت سایبری، توسعه و پیاده‌سازی زیست‌بوم فرهنگی برای حمایت از امنیت سایبری است. نیاز به پرداختن به فناوری و فرآیندهای امنیت سایبری مستلزم توسعه فرهنگ امنیت سایبری است. داشتن فرهنگ امنیت سایبری فرآیندی پویا است که توجه مستمر را می‌طلبد [۳].

۵.۲ مدل‌های فرهنگ امنیت سایبری

علی‌رغم نو بودن موضوع فرهنگ امنیت سایبری، به جهت اهمیت بالای این موضوع، مدل‌هایی جهت سنجش و ارائه تصویری از سطح سازمان در این حوزه، توسعه داده شده‌اند. عمدتا مدل‌های ارائه شده را می‌توان به دو گروه تقسیم نمود. گروه اول مدل‌هایی هستند که فرایند استقرار فرهنگ امنیت سایبری را مدنظر قرار داده‌اند و در آن‌ها کمتر به ابعاد و مؤلفه‌ها پرداخته شده است. گروهی دیگر به ابعاد و مؤلفه‌ها و ساختار مورد نیاز در کنار برنامه‌ها و فرایندها، برای ایجاد فرهنگ امنیت سایبری پرداخته‌اند. با توجه به موضوع، در این تحقیق به برخی از مهمترین مدل‌ها در گروه دوم اشاره می‌گردد.

مدل هفت‌بلوک فرهنگ امنیت سایبری

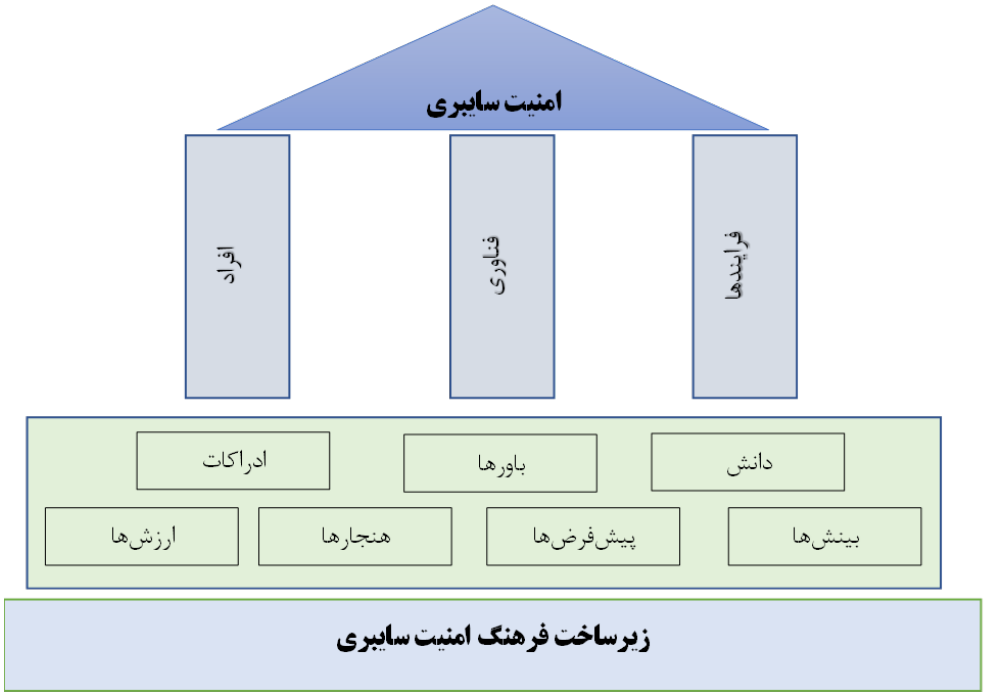
این مدل که در شکل ۱ زیرساخت فرهنگ امنیت سایبری را نشان می‌دهد از افراد، فناوری و فرآیندهای امنیت سایبری پشتیبانی می‌کند. اما ایجاد این مؤلفه‌ها که ستون‌های امنیت سایبری می‌باشند نیازمند زیرساخت‌هایی است. هفت بلوک دانش، باورها، ادراکات، نگرش‌ها، مفروضات، هنجارها و ارزش‌ها، محیط اجتماعی و روانی مناسبی را برای حمایت از امنیت سایبری فراهم می‌کند [۴].

مدل هفت‌بعدی اندازه‌گیری فرهنگ امنیت سایبری مؤسسه ENISA

در این مدل (ENISA)[۴] فرهنگ امنیت سایبری مبتنی بر امنیت اطلاعات به هفت بعد تقسیم شده است که عبارتند از [۶]:

۱. رفتارها: اقدامات ارادی یا آگاهانه کارکنان که مستقیم یا غیرمستقیم بر روی فرهنگ امنیت اثرگذار است.

[4] The European Union Agency for Cybersecurity



شکل ۱: مدل هفت‌بلوک زیرساخت فرهنگ امنیت سایبری [۴]

۲. نگرش‌ها: احساسات و گرایش‌ها در رابطه با اقداماتی که مرتبط با امنیت سازمان است.

۳. شناخت‌ها: دانش، آگاهی و باورهایی از کارکنان که بر اقدامات و کارآمدی آنها در امنیت سازمان مؤثر است.

۴. انطباق: مربوط به داشتن سیاست‌های امنیت سازمانی، آگاهی از آنها و دسترسی به دستورالعمل‌های حاصل از سیاست‌ها است.

۵. ارتباطات: راه‌هایی که کارکنان با دیگران در رابطه با مقوله‌های امنیت، گزارش‌دهی حوادث و احساس تعلق سازمانی ارتباط برقرار می‌کنند.

۶. هنجارها: اینکه کارکنان چه بخشی از اقدامات و عملیات سازمان را به‌طور طبیعی مرتبط با امنیت درک می‌کنند و چه بخشی را خارج از آن می‌دانند.

۷. مسئولیت‌ها: آگاهی از اینکه هریک از کارکنان عنصری حیاتی در پایداری یا از بین رفتن امنیت در سازمان هستند.

مؤسسه ENISA در رابطه با فرهنگ امنیت سایبری فرایندهای اقدام و مدل‌های مختلفی ارائه نموده است. این مؤسسه ابعاد اثرگذار بر فرهنگ امنیت سایبری را در سازمان‌ها به دو بعد اصلی انسانی و بیرونی تقسیم‌بندی نموده است.

۱. مؤلفه‌های انسان‌پایه:

۱-۱) روانشناختی: شامل عوامل و شرایطی است که منجر به تغییر رفتار انسان به‌لحاظ روان‌شناختی و درونی می‌گردد.

۱-۲) شخصیت و انطباق: شامل روش‌ها و فرایندهایی است که کارکنان در آن نسبت به تشخیص و مواجهه با تهدیدات سایبری، ریسک‌ها و حوادث، آگاهی و حساسیت یافته و مسئولیت‌پذیر می‌شوند و به‌عبارتی امنیت سایبری در کارکنان درونی‌سازی می‌گردد.

۱-۳) محیط اجتماعی: با توجه به اینکه انسان موجودی اجتماعی است، بسیاری از رفتارها در محیط اجتماع شکل می‌گیرد. براین اساس این مؤلفه شامل انتظارات و واکنش‌های مدیران و تأییدات و نگرش‌های همکاران پیرامونی در تغییر رفتار کارکنان است.

۲. مؤلفه‌های بیرونی:

فرهنگ ملی: عمده موارد مربوط به این مؤلفه مربوط به تأثیراتی است که فرهنگ یک کشور بر رفتار افراد آن می‌گذارد. اینکه رفتاری توسط فرهنگ ملی مورد تأیید یا رد قرار گیرد می‌تواند موجب رشد یا از بین رفتن آن رفتار در افراد گردد. لذا این مؤلفه شامل مواردی از فرهنگ درونی کشورها یا فرهنگ غالب خارج از سازمان است که بر تغییر رفتار کارکنان تأثیر می‌گذارد.

۳ روش‌شناسی تحقیق

از منظر هدف، این تحقیق کاربردی می‌باشد و روش تحقیق بکارگرفته شده در آن نیز، توصیفی تحلیلی است که با استناد به منابع کتابخانه‌ای و با تحلیل و بررسی اسناد در این حوزه، ابعاد و مؤلفه‌های مربوط به ایجاد و ساختاردهی فرهنگ امنیت سایبری سازمان‌ها را جستجو نموده است.

در فرایند انجام این پژوهش بدواً تعاریف و مفاهیم، مدل‌های فرهنگ سازمانی، فرهنگ امنیت سایبری در سازمان‌ها، از میان اطلاعات کتابخانه‌ای و اسناد معتبر اینترنتی مرتبط با موضوع، مورد مطالعه قرار گرفت. در انتخاب اسناد مورد مطالعه به‌روز و معتبر بودن، دو شاخص کلیدی بود که استخراج داده‌ها براساس این دو شاخص انجام شد. در این راستا ابعاد و مؤلفه‌ها، از میان مدل‌هایی که در منابع کتابخانه‌ای به آنها پرداخته شده بود، استخراج گردید و تطبیق و جمع‌بندی آنها براساس دو شاخص بیان شده؛ به‌روز بودن مطالب و اعتبار منابع انجام شد. نظر خبرگان فرهنگ سازمانی و امنیت سایبری در رابطه با ابعاد و مؤلفه‌های استخراج شده و در ادامه، سطوح سازمانی هریک از آنها، براساس ابزار پرسشنامه و طی فرایندهای مجزا، گردآوری و

مورد تجزیه و تحلیل قرار گرفت و نهایتاً ابعاد و مؤلفه‌های مرتبط با هدف تحقیق براساس سه سطح مدنظر مشخص شد.

۴ یافته‌ها

در ابتدای استخراج و جمع‌بندی ابعاد و مؤلفه‌های تحقیق، مشخص شد که ابعاد فرهنگ امنیت سایبری دارای اثرگذاری برابر نبوده و به‌طور کلی در سه سطح راهبردی، عملیاتی و تکنیکی منشأ اثر هستند. لذا هریک از ابعاد و مؤلفه‌ها بر اساس شدت اثرگذاری در یکی از سه سطح جای گرفت.

براین اساس نظر خبرگان بر روی سه مقوله سطح، بعد و مؤلفه دریافت شد. برای گردآوری داده‌ها ۲ پرسشنامه تدوین شد. در پرسشنامه اول ابعاد و مؤلفه‌ها مورد پرسش قرار گرفت. پس از تجزیه و تحلیل پاسخ‌ها، مواردی که امتیاز بالاتر از نصف یعنی ۲/۵ را کسب نموده بودند، از نظر خبرگان به عنوان ابعاد و مؤلفه‌های فرهنگ امنیت سایبری در نظر گرفته شدند. در ادامه جهت تعیین جایگاه هریک از ابعاد در سطوح سازمانی، پرسشنامه دوم به خبرگان ارائه شد و نظر ایشان در رابطه با جایگاه هریک از ابعاد اخذ شد. پس از تجزیه و تحلیل داده‌های این مرحله بالاترین امتیاز کسب شده برای هر بعد در سطوح مدنظر، به عنوان سطح مناسب خبرگان در نظر گرفته شد. براساس این دو فرایند گردآوری و تجزیه و تحلیل، نهایتا پاسخ به سئوال تحقیق که ابعاد و مؤلفه‌های ساختاردهی فرهنگ امنیت سایبری در سازمان‌ها بود در سه سطح، براساس جدول ۱ مشخص شد.

۵ نتیجه‌گیری

در کنار برنامه‌ها و دستورالعمل‌های صرفاً حقوقی و فنی که تاکنون جهت ارتقاء امنیت سایبری در کشور اجرا شده، نتایج حاصل از این تحقیق روش دیگری را پیشنهاد می‌نماید که در آن امنیت سایبری در جو حاکم برسازمان یا فرهنگ غالب آن جاری می‌شود و رفتار امن در کلیه سطوح سازمانی در کارکنان و مدیران درونی می‌گردد.

جهت پاسخ به مسئله تحقیق که ابعاد و مؤلفه‌های مؤثر بر ایجاد و ساختاردهی فرهنگ امنیت سایبری در سازمان می‌باشد، ادبیات، مدل‌ها و فرایندهای ایجاد فرهنگ امنیت سایبری مدنظر قرار گرفت. در فرایند مطالعه مشخص شد که فرهنگ امنیت سایبری با سه سطح راهبردی، عملیاتی و تکنیکی سازمان‌ها در تعامل است و تصمیمات و اقدامات سازمان در این سه سطح بر ایجاد این نوع فرهنگ در سازمان به نسبت اهمیت و جایگاه آن سطح، تأثیر دارد. بنابراین نمی‌توان سطح تأثیر ابعاد و مؤلفه‌ها را برابر درنظر گرفت.

ابعاد و مؤلفه‌های سطح راهبردی در پی ایجاد و همسوسازی ارزش‌ها، راهبردها، سیاست‌ها و دستورالعمل‌ها و ساختار سازمان با فرهنگ امنیت سایبری است. همچنین در سطح عملیاتی به اقدامات مختلفی در سازمان در حوزه‌های کارکنان و مشاغل آنها و اقدامات سایبری همچون تمرینات، هنجارسازی، اتحادها و اطلاع‌رسانی در میان همه کارکنان تأکید دارد تا امنیت سایبری را به امری روزمره و جدایی‌ناپذیر از فعالیت‌ها و وظایف مدیران و کارکنان سازمان مبدل کند. اما در سطح تکنیکی به فراهم نمودن بسترهای

جدول ۱: سطوح، ابعاد و مؤلفه‌های ساختاردهی فرهنگ امنیت سایبری

سطح سازمانی	ابعاد	مؤلفه‌ها
راهبردی	ارزش‌ها	حفظ و صیانت از سرمایه‌های سایبری- صیانت از کارکنان در مقابل حوادث سایبری
	سبک رهبری	حمایت از امنیت- واکنش به حوادث سایبری- واکنش به رفتار کارکنان در حوادث سایبری- مدیریت سرمایه‌های سایبری
	راهبردها	انطباق راهبردهای موجود با امنیت سایبری- راهبرد امنیت سایبری- ایجاد راهبرد فرهنگ امنیت سایبری- ایجاد راهبردهای کاهش اثرات منفی محیط پیرامونی در فرهنگ امنیت سایبری
	سیاست‌ها	انطباق سیاست‌های موجود با امنیت سایبری- ایجاد سیاست‌های جدید امنیت سایبری
	ساختار	تقویت جایگاه سازمانی امنیت سایبری- تطبیق مشاغل و جایگاه آنها با آسیب‌پذیری‌های سایبری مرتبط- تطبیق سلسله‌مراتب گزارش‌دهی با پاسخ‌گویی حوادث سایبری
عملیاتی	آموزش و آگاه‌سازی	انطباق برنامه‌های آموزشی موجود با امنیت سایبری- تدوین و اجرای برنامه‌های آموزشی امنیت سایبری کارکنان- تدوین و اجرای برنامه‌های آموزشی ویژه متخصصین سایبری
	امور شناختی	بررسی و شخصیت شناسی کارکنان نسبت به امنیت سایبری- تدوین برنامه روانشناختی مدیران و کارکنان در تطبیق و تثبیت رفتار امنیت سایبری - تدوین برنامه‌های شناختی در تقویت مسئولیت‌پذیری و پاسخگویی در قبال امنیت سایبری
	امور خدمات شغلی	تطبیق مشاغل با آسیب‌پذیری‌های سایبری آنها- تدوین برنامه ترغیب و تنبیه کارکنان در قبال رفتارها و واکنش‌های منطبق با امنیت سایبری- ایجاد برنامه چرخش شغلی کارکنان در انطباق شخصیت، شغل و آسیب‌پذیری سایبری
	تمرینات سایبری	تدوین و اجرای برنامه برگزاری تمرینات سایبری دوره‌ای درون سازمانی- تدوین و اجرای برگزاری تمرینات سایبری با سازمان‌های متولی- تدوین و اجرای برگزاری تمرینات سایبری با سازمان‌های همکار
	اتحادهای سایبری	همکاری با سازمان‌های همسو در حوزه امنیت سایبری- ایجاد روش‌ها و دستورالعمل‌های برقراری ارتباط سایبری میان سازمانی
	هنجارسازی امنیت سایبری	استفاده از نمادهای امنیت سایبری- ایجاد گروه‌های رسمی و غیررسمی رصد، مقابله و پاسخ‌گویی امنیت سایبری
	اطلاع‌رسانی امنیت سایبری	استفاده از شبکه‌های اطلاع‌رسانی درون سازمانی- ایجاد کمپین‌های امنیت سایبری- ایجاد شبکه اطلاع‌رسانی واکنش به حوادث سایبری
تکنیکی	تقویت زیرساخت	ایجاد زیرساخت شبیه‌سازی تمرینات سایبری- ایجاد زیرساخت رصد و تشخیص رفتار کارکنان در قبال امنیت سایبری
	اطلاع‌رسانی فنی	تدوین برنامه گزارش‌دهی دوره‌ای آسیب‌پذیری‌ها- شبکه اطلاع‌رسانی و آگاه‌سازی از آسیب‌پذیری‌های جدید
	شبکه ارتباط درون سازمانی	ایجاد شبکه‌های ارتباطی کارکنان در حوزه امنیت سایبری- ایجاد بسترهای امن ارتباط میان کارکنان در حوادث سایبری
	شبکه ارتباط برون سازمانی	ایجاد بستر امن ارتباط کارکنان سایبری سازمان با کارکنان سایبری سازمان‌های همسو- ایجاد بستر تمرینات سایبری میان سازمانی

فنی فرهنگ امنیت سایبری که در سطوح بالاتر مدنظر قرار گرفته شده بود می‌پردازد و علاوه برآن شبکه‌هایی جهت ارتباط برون‌سازمانی فراهم می‌نماید.

برای ایجاد فرهنگ امنیت سایبری در سازمان، بررسی تحقیقات قبلی توسط محقق نمایانگر این موضوع است که موارد انجام شده بر اساس هدفی خاص بوده و باهدف این تحقیق که نگاهی جامع به کلیه ابعاد و سطوح سازمان در ایجاد فرهنگ سایبری است، تفاوت داشته‌اند. نتایج این تحقیق با توجه به عمومیت و جامعیت نسبی آن و توجه به تمام سطوح سازمان، می‌تواند دستورالعمل و راهنمایی برای برنامه‌ریزان سازمانی باشد تا در تدوین برنامه ارتقاء فرهنگ امنیت سایبری به سطوح، ابعاد و مؤلفه‌های مختلف توجه نموده و امنیت سایبری را امری جامع و چندبعدی در نظر گیرند. همچنین نتایج این تحقیق راهنمایی است برای محققینی که در این موضوع اقدام به تحقیق می‌نمایند، تا براساس آن بتوانند به مدل‌های مختلف فرهنگ امنیت سایبری پرداخته و دامنه موضوع را توسعه و تعمیق بخشند.

محققین علاقمند به این موضوع می‌توانند در رابطه با ابعاد و مؤلفه‌های فرهنگ امنیت سایبری در حوزه‌های تخصصی همانند صنایع، امور نظامی و زیرساخت‌های حیاتی به تحقیق بپردازند. همچنین روش‌های ارزیابی و سنجش ارتقاء فرهنگ امنیت سایبری در سازمان‌ها با هدف ایجاد مسیر برای برنامه‌ریزی را به عنوان موضوع تحقیق مدنظر قرار دهند. علاوه بر آن به نظر می‌رسد با توجه به اهمیت بسیار بالای امور شناختی کارکنان و ارتباط آن با فرهنگ امنیت سایبری، می‌توان به این مقوله به صورت ویژه توجه نموده و تحقیقاتی در رابطه با این موضوع صورت پذیرد.

مراجع

[۱] سعیدی، پرویز (۱۳۸۹). شناسایی فرهنگ سازمانی براساس مدل کویین و گارت. فصلنامه روانشناسی تربیتی.

[۲] طوسی، محمدعلی (۱۳۷۲). فرهنگ سازمانی. تهران: مرکز آموزش مدیریت دولتی.

[3] A. Fagerström (2013). Creating, Maintaining and Managing an Information Security Culture.

[4] Alvarez-Dionisi, L., & Urrego-Baquero, N. (2019, March 15). Implementing a Cybersecurity Culture. Retrieved from ISACA: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/implementing-a-cybersecurity-culture

[5] Barker, J., Davis, A., Hallas, B., & Mc Mahon, C. (2021). Cybersecurity ABCs: Delivering awareness, behaviours and culture change. BCS Publishing.

[6] Cyber Security Culture in organisations. (2017). ENISA.

[7] Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A Cyber-Security Culture Framework for Assessing Organization Readiness. Journal of Computer Information Systems, DOI: 10.1080/08874417.2020.1845583, pp. 452-462.

[8] Henry, Shawn (2017, 11, 17). IABM. Retrieved from The Top 5 Cybersecurity Mistakes Companies Make and How to Avoid Them: https://theiabm.org/top-5-cybersecurity-mistakes-companies-make-avoid/

[9] Kaspersky. Retrieved from https://www.kaspersky.com/blog/the-human-factor-in-it-security/

[10] Leenen, L. v. (2019). Framework for the cultivation of a military cybersecurity culture. 14th International Conference on Cyber Warfare and Security (ICCWS 2019) pp. 212-220.

[11] Mncedisi Willie, M. (2023). The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture. SSRN.

[12] Nasir, A. F. (2023). How to Cultivate Cyber Security Culture? The Evidences from Literature. International Journal of Synergy in Engineering and Technology, pp. 13-19.

[13] Ramluckan, T. (2020). A Change Management Perspective to Implementing a Cyber Security Culture. 19th European Conference on Cyber Warfare and Security. 10.34190/EWS.20.059.