فصلنامه پژوهش‌های حفاظتی ـ امنیتی
دانشگاه جامع امام حسین(علیه‌السلام)

سال دهم، شمارهٔ ۳۸ (تابستان ۱۴۰۰) صص ۱۹۲-۱۶۷

طراحی و ساخت ابزارِ ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری*

● صدیقه حیدری ●

دانشجوی دکتری تخصصی سنجش و اندازه‌گیری، دانشکده علوم انسانی، دانشگاه آزاد اسلامی واحد ساوه

● مجید برزگر ●

استادیار گروه روانشناسی و علوم تربیتی، دانشکده روانشناسی و علوم تربیتی، دانشگاه آزاد اسلامی واحد مرودشت (نویسنده مسئول)

● امیرحسین محمد داودی ●

دانشیار گروه مدیریت آموزشی، دانشکده علوم انسانی، دانشگاه آزاد اسلامی واحد ساوه

تاریخ دریافت: ۱۴۰۰/۰۲/۳۰ تاریخ پذیرش: ۱۴۰۰/۰۷/۰۵

چکیده

پژوهش حاضر با هدف طراحی و ساخت ابزارِ ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری در سال ۱۴۰۱ به صورت آمیخته (کیفی ـ کمّی) انجام شد تا به این سؤال پاسخ دهد که ابزار ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری، از چه گویه‌هایی تشکیل شده است؟ در بخش کیفی از متون بالادستی سه سال اخیر و نظرخواهی از خبرگان این حوزه بهره گرفته شد تا ساختار اولیه ابزار بدست آید. در بخش کمّی، ساختار اولیه ابزار در اختیار نمونه کوچکی از جامعه هدف قرار گرفت تا براساس داده‌های حاصل، روایی و اعتبار ابزار بررسی شود. به منظور بررسی روایی، از روایی محتوا، توان افتراقی و جهت بررسی اعتبار داده‌ها از همسانی درونی و همبستگی درون‌خوشه‌ای استفاده شد. درصد خطای الگوریتم شناسایی نیز ۴درصد بوده است که با ضریب هولستی محاسبه شد. یافته‌های حاصل از بخش کیفی تعداد ۷۵ مؤلفه مؤثر در فرهنگ و آگاهی امنیت سایبری را نشان داد که براساس آن استخر اولیه با ۹۸ گویه تهیه شد. پس از قرار دادن استخر اولیه گویه‌ها در اختیار خبرگان، یافته‌های حاصل از بررسی روایی محتوا نشان داد تعداد ۵۶ گویه از کیفیت لازم برخوردار نبوده و حذف شدند. بررسی توان افتراقی بیانگر توان بالاتر از ۱ همه گویه‌ها به استثنای گویه شماره ۴۱ بود. نتایج اعتبار نشان داد گویه شماره ۸ فاقد همبستگی قابل قبول بوده، از این‌رو از فرم نهایی حذف گردید. کران بالای فاصله اطمینان ICC نیز بیانگر توافق بسیارخوب داوران با یکدیگر بود. به‌طورکلی می‌توان گفت فرم ۴۱ گویه‌ای تهیه شده، دارای روایی محتوا و اعتبار قابل قبول بوده، بنابراین شرایط لازم جهت بررسی در سطح نمونه اصلی گروه هدف را داشته و می‌توان آن را در نمونه وسیعی از گروه هدف، جهت دستیابی به ساختار نهایی و نمرات هنجار به کار گرفت..

کلید واژگان: روایی؛ اعتبار؛ فرهنگ؛ آگاهی؛ امنیت سایبری

* این مقاله برگرفته از رساله دکتری با عنوان «ساخت ابزارِ ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری و تحلیل آن براساس نظریه کلاسیک و مدل‌های چندارزشیِ نظریه سؤال ـ پاسخ» می‌باشد.

مقدمه

امروزه، بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی در همه سطوح، اعم از افراد، مؤسسه‌های غیر دولتی و نهادهای دولتی و حاکمیتی، در فضای سایبر انجام می‌گیرد (ثقفی و اسماعیلی، ۱۳۹۹: ۶۵) و این در حالی است که اخیراً بسیاری از شرکت‌های خصوصی و سازمان‌های دولتی در سراسر جهان با مشکل حملات سایبری و خطر فناوری‌های ارتباطات بی‌سیم روبه‌رو هستند. دنیای امروز به شدت به فناوری الکترونیکی وابسته است و محافظت از این داده‌ها در برابر حملات سایبری یک مسئله چالش برانگیز است (یوچانگ و کینگوئی[1]، ۲۰۲۱: ۱). این حملات علیه زیرساختها نه تنها می‌تواند منجر به نشت داده‌ها شود، بلکه می‌تواند پیامدهای مالی قابل توجهی داشته و حتی منجر به از دست دادن جان افراد شود. در نتیجه، برای دفاع در برابر چنین حملاتی و با توجه به اینکه انسان‌ها نقش کلیدی در این فناوریها دارند، افزایش آگاهی از امنیت سایبری[2] مهم است (الزبیدی[3]، ۲۰۲۱: ۱).

عدم آگاهی کاربران در مورد تهدیداتی که ممکن است در فضای مجازی با آنها روبه‌رو شود، می‌تواند باعث اجرای موفقیتآمیز تهدیدها شود (بینو[4]، ۲۰۲۱: ۵۸۱). در این راستا بررسی متون حاکی از وجود شکاف‌هایی در این زمینه بوده و نشان داده است که هم مدیران ارشد و هم متخصصان امنیت سایبری، باید امنیت سایبری یک مؤسسه دیجیتالی موفق در حوزه اقتصاد را تضمین کنند. این شکاف‌ها ۴ عامل تعهد مدیریت عالی و پشتیبانی، بودجه‌بندی؛ رعایت امنیت سایبری و فرهنگ امنیت سایبری[5] را نشان داده‌اند. تفاوت بین بالاترین و پایین‌ترین حد هر ۴ عامل بسیار اندک بوده که نشانه اهمیت هر ۴ شاخص در آگاهی امنیت سایبری است. بنابراین از جمله پیامدهای عملی برای سیاستگذاران و متخصصان امنیت سایبری در فرهنگ و آگاهی امنیت سایبری، می‌توان به این امر اشاره کرد که مطالعه در این حوزه عامل حیاتی را ارائه می‌دهد که ممکن است به بهبود سیاستها یا دستورالعمل‌های آگاهی از امنیت سایبری موفق در سازمان‌ها، کمک کند (العلوی و الباسام[6]، ۲۰۲۱: ۱۷).

1. Yuchong & Qinghui
2. Awareness of Cyber Security
3. Alzubaidi
4. Bino
5. Culture of Cyber Security
6. Al-Alawi & Al-Bassam

در واقع، در کنار فرصت‌ها و قابلیت‌های ایجاد شده در زیستبوم سایبری کشور، سرمایه‌های سایبری موجود در معرض تهدیدها، آسیبها و مخاطرات هستند. از این‌رو، اقدام پیشگیرانه و مقابله‌ای با تهدیدها و آسیبها و جرائم سایبری مستلزم برنامه‌ریزی ملی، فراسازمانی و فرابخشی است (تقی‌پور و همکاران، ۱۳۹۹: ۹۵) چرا که میزان آسیب‌پذیری ناشی از تهدیدات سایبری که از تأثیرات فضای مجازی است، چندبُعدی بوده و به دلیل ارتباط با شبکه‌ها و زیرساخت‌های حساس، میزان آسیب آنها بسیار زیاد است و نمی‌توان آنها را تنها با روش‌های سنتی مانند استفاده از نیروی نظامی و پلیس مهار کرد، دولت‌ها به تنهایی برای مقابله با آنها کافی نیستند و همکاری مؤثر و دو جانبه بین دولت‌ها و بخش خصوصی که منافع مشترکی در برخورد با آنها را دارند می‌طلبد. بنابراین، تهدیدات سایبری تنها به دولت‌ها محدود نمی‌شود، افراد و شرکت‌های مختلف نیز از آسیب‌های این تهدیدها مصون نخواهند بود (یوچانگ و کینگوئی، ۲۰۲۱: ۲). اما علی‌رغم این واقعیت که مطالعات بیشماری در مورد مسائل امنیت سایبری در جهان انجام شده است، در کشور ما شکاف مطالعاتی وجود دارد که بر فرهنگ و آگاهی امنیت سایبری در بین مدیران سطح بالا، کارکنان و نگرش آنها تمرکز کند و این امر مستلزم وجود ابزاری در این حیطه است تا از طریق آن سطح فرهنگ و آگاهی افراد ارزیابی شده و تصمیمات یا راهکارها متناسب با آن سطح به‌کار گرفته شوند. چرا که پس از تعیین سطح فرهنگ و آگاهی، از طریق آموزش متناسب با آن سطح در افراد، همه کارکنان می‌توانند مجهز باشند تا به عنوان یک دیوار آتشین برای دفاع در برابر هرگونه حمله سایبری عمل کنند.

حال، با توجه به اینکه امنیت اطلاعات چالش پیش‌روی سازمان‌ها است و نقض امنیت تهدیدی جدی برای اطلاعات حساس است، بنابراین سازمان‌ها در رابطه با دارایی‌های اطلاعاتی خود با خطرات امنیتی روبه‌رو بوده که ممکن است ناشی از کارکنان خودشان باشد. پس وجود ساختاری در زمینه فرهنگ امنیت سایبری با پوشش عوامل مؤثر بر فرهنگ امنیت و عوامل منعکس کننده آن در این حیطه می‌تواند راهگشا باشد و از طریق معرفی یک چارچوب جامع در عمل، که در ایجاد فرهنگ امنیت نقش دارد، به بهبود مدیریت امنیت سایبری کمک خواهد شد چرا که عوامل در توجیه پذیرش فرهنگ امنیت بسیار حیاتی هستند و چارچوب، ابزار مهمی را ارائه می‌دهد که می‌تواند برای ارزیابی و بهبود فرهنگ امنیت سازمانی مورد استفاده قرار گیرد (تولا و همکاران[۷]، ۲۰۲۱: ۱). بنابراین با توجه به اینکه کارمندان کشور، افرادی هستند که علاوه بر اینکه یک

7. Tolah et al.

شهروند عادی محسوب می‌شوند، به واسطه شغل خود با سرمایه عموم مردم در ارتباط بوده و نقض احتمالی امنیت سایبری توسط آنان ممکن است زیان‌هایی را به بار آورد؛ از این‌رو، هدف قرار دادن این افراد به منظور ارزیابی سطح آگاهی و فرهنگشان نسبت به امنیت سایبری اهمیت پیدا می‌کند. از این جهت، هدف از انجام این پژوهش طراحی و ساخت ابزارِ ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری با کمک اسناد بالادستی و نظرخواهی از خبرگان درون کشوری حوزه امنیت سایبری بوده تا به این سؤال پاسخ داده شود که ابزاری که توانایی ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری را دارد، از چه گویه‌هایی تشکیل شده است؟

مبانی نظری و پیشینهٔ پژوهش

مبانی نظری

در جهان امروز، فرهنگ، اندیشه‌ها و رفتارها را جهت داده و روابط میان افراد و گروه‌های مختلف جامعه را تنظیم می‌کند. فرهنگ در تمامی حوزه‌های زیست اجتماعی بشر از جمله حوزه امنیت، مبنای اثرگذاری است (عسگری، ۱۴۰۰: ۱۶۳). در این راستا، پیر لوی[8] نوعی از فرهنگ را با عنوان فرهنگ سایبری معرفی کرده و آن را به عنوان مجموعه‌ای از تکنیک‌ها و شیوه‌هایی تعریف کرده است که به واسطه جوامع موجود در فضای مجازی توسعه و تقویت می‌شود و موقعیت انفعالی آن با امکان مشارکت و صدور بازخورد جایگزین شده و کانال‌های ارتباطی برخط را به پلتفرم‌های دو سویه و تعاملی تبدیل می‌کند که در حال حاضر بخشی از روال روزانه میلیاردها نفر در سراسر جهان است (لیما[9]، ۲۰۰۹؛ به نقل از کاردوسو و کاستانهو[10]، ۲۰۲۱: ۱). در واقع فرهنگ از هر نوعی که باشد، به عنوان مجموعه‌ای از نگرش‌ها، ارزش‌ها، اهداف و عملکردهای مشترک بیان می‌شود که یک نهاد یا سازمان را تعریف می‌کند. بنابراین فرهنگ امنیت سایبری به مجموعه‌ای از ارزش‌ها، قراردادها، شیوه‌ها، دانش، باورها و رفتارهای مرتبط با امنیت اطلاعات اشاره دارد که اسکلت آن توسط محیط کار همراه با زیرساخت‌های تکنولوژیکی و اقدامات متقابل امنیتی که آن را تعریف می‌کند، مشخص می‌شود (جورجیادو و همکاران، ۲۰۲۱ الف: ۴۳) و آگاهی از آن عبارت از شناسایی، پیشگیری و مقابله با حملات سایبری (ترخان و فتوح‌آبادی، ۱۳۹۵: ۱) و تصمیم‌گیری درست و به موقع برای مقابله با حملات سایبری می‌باشد (رشیدی و شکیبازاد، ۱۳۹۵: ۱).

8. Pierre Levy
9. Lima
10. Cardoso & Castanho

فضاهای سایبری امروزی به‌طور فزایندهای خصومت‌آمیز شده‌اند و برنامه‌ها و راه‌کارهایی که از طریق برنامه‌ریزی و اجرای رزمایشهای سایبری به وجود می‌آیند و تست می‌شوند نقش قابل توجهی در آمادگی و واکنش سایبری دارند و باعث ایجاد امنیت بیشتر در فضای سایبری می‌گردند (موحدی‌راد و و مدیری، ۱۳۹۳: ۱). در این راستا مرور ادبیات سیستماتیک در ۱۰ سال گذشته (۲۰۱۰-۲۰۲۰) نشان داد که در حالی که تغییرات قابل توجهی در استفاده از اصطلاحات (به عنوان مثال فرهنگ امنیت اطلاعات و فرهنگ امنیت سایبری) ایجاد شده است، بسیاری از عوامل تأثیرگذار مشابه هستند. حمایت‌ها، سیاست‌ها و رویه‌های مدیریت ارشد و برای مثال آگاهی، در ایجاد فرهنگ امنیت سایبری بسیار مهم است. بسیاری از چارچوب‌های مورد بررسی، مبانی مشترکی را آشکار کردند و فرهنگ سازمانی نقش مهمی در ایجاد مدل‌های مناسب فرهنگ امنیت سایبری ایفا کرد. پرسشنامه‌ها و نظرسنجی‌ها بیشترین ابزار مورد استفاده برای ارزیابی فرهنگ امنیت سایبری هستند، اما نگرانی‌هایی نیز وجود دارد که آیا به اقدامات پویاتر نیاز است یا خیر (اوچندو و همکاران[11]، ۲۰۲۱: ۱).

در حقیقت، زیرساخت‌های اطلاعاتی حیاتی به‌طور مداوم در معرض تهدید انواع مختلف حملات سایبری قرار دارند. در چند سال گذشته، دشمنان راه‌هایی برای توسعه بدافزارهایی پیدا کرده‌اند که به‌طورخاص برای هدف قرار دادن جامعهٔ هدف طراحی شده‌اند و حتی کاملاً موفق هم بوده‌اند. دشمنان از نظر استراتژی بسیار جلوتر هستند و از نظر فنی مهارت دارند تا از کنترل‌های سنتی پیشی بگیرند. براساس تحلیل چند روند اخیر حملات سایبری بیشتر حملات با هدف قرار دادن کاربر نهایی آغاز می‌شوند. از این‌رو کاربر نهایی به عنوان یک حلقه ضعیف در نظر گرفته می‌شود. همچنین در اکثر سازمان‌ها آموزش‌های امنیت سایبری به اعضای تیم امنیتی بدون اهمیت دادن به کاربران عادی محدود می‌شود. بنابراین، اگر کارکنان به اندازه کافی برای تشخیص یک تهدید امنیتی آموزش ندیده باشند، نمی‌توان از آنها انتظار داشت که از آن اجتناب کنند، آن را گزارش کنند یا آن را حذف کنند. کارکنان به آگاهی و آموزش امنیت سایبری نیاز دارند تا از خود و شرکت در برابر حملات سایبری جدید در حال تکامل محافظت کنند. با آگاه کردن کارمندان از اشکال جدید تهدیدات امنیتی و اقداماتی که باید در هنگام شناسایی یک فعالیت مشکوک دنبال کنند، می‌توانیم آسیب‌پذیرترین حلقه‌های زنجیره را تقویت کنیم (خان و همکاران[12]، ۲۰۲۰: ۲۹۸).

11. Uchendu et al.

اما تحلیل‌ها نشان داده است که محققان امنیتی، شاغلان و مدیران ممکن است از تلاش در اندازه‌گیری میزان آگاهی امنیتی کارکنان ناامید شوند، زیرا هیچ توضیحی در مورد بسیاری از مسائل نگران کننده وجود ندارد. در این راستا، مطالعات مختلفی برای شناسایی «بهترین عملکرد» در اندازه‌گیری آگاهی امنیتی انجام شده است که در پیوند با فرهنگ امنیت سایبری هستند (ایوانز و همکاران[۱۳]، ۲۰۱۹؛ آختر و همکاران[۱۴]، ۲۰۲۰؛ بانکیو و همکاران[۱۵]، ۲۰۲۰؛ الرادی و همکاران[۱۶]، ۲۰۲۰؛ گراسگر و ندبال[۱۷]، ۲۰۲۱؛ الزبیدی، ۲۰۲۱).

فرهنگ امنیت تا حدودی به تازگی ظهور کرده است و مدل اندازه‌گیری یا ابزار اندازه‌گیری برای آن تنها در دو مطالعه جورجیادو و همکاران (۲۰۲۱ الف) و الشیخ[۱۸] (۲۰۲۰) مشاهده شده است و این در حالی است که فرهنگ امنیت اطلاعات به‌طور قابل توجهی طولانی‌تر مورد مطالعه قرار گرفته است و بر دوره بررسی، غالب است. فرهنگ امنیت سایبری در دهه گذشته به یک اصطلاح تثبیت شده در صنعت و رسانه همراه با اصطلاحاتی مانند حمله سایبری، تهدید سایبری و جاسوسی سایبری تبدیل شده است اما شیوع آن در تحقیقات دانشگاهی محدود است. علی‌رغم این، با افزایش مقالات فرهنگ امنیت سایبری، درک اینکه تفاوت بین اصطلاحات در کجاست، حیاتی است. اگرچه فرهنگ امنیت اطلاعات و فرهنگ امنیت سایبری به عنوان مفاهیم مختلفی تعریف شده‌اند که می‌توانند هم‌پوشانی داشته باشند، این اصطلاحات اغلب به جای یکدیگر در ادبیات استفاده می‌شوند (اوچندو و همکاران، ۲۰۲۱: ۲۰).

گکازا و همکاران[۱۹] (۲۰۱۵) توافق کردند که تعریف واضحی از حوزه فرهنگ امنیت سایبری وجود ندارد و این باید با حذف ابهامی که واژگان مورد استفاده در رابطه با فرهنگ امنیت سایبری را احاطه کرده است، مورد توجه قرار گیرد. علاوه بر این، تحقیقات نشان می‌دهد که تمایلات رفتاری کارکنان نیز مهم است درحالی‌که به‌طور بالقوه نادیده گرفته می‌شود. با بررسی جنبه‌های انسانی به‌طور خاص، وانت ووت[۲۰] (۲۰۱۹) پیشنهاد می‌کند که سازمان‌ها باید رویکرد

12. Khan et al.
13. Evans et al.
14. Akhter et al.
15. Banciu et al.
16. Elradi et al.
17. Grassegger and Nedbal
18. Alshaikh
19. Gcaza et al.

سفارشی‌تری به فرهنگ امنیت سایبری داشته باشند و پیشنهاد می‌کند که کارکنان در شرکت از دیدگاه روان‌شناختی بیشتری ارزیابی شوند و به مفاهیمی مانند شخصیت، علایق، نیازها و انگیزه‌ها توجه کنند (اوچندو و همکاران، ۲۰۲۱: ۲۱).

شخصیت در پژوهش‌های اخیر مورد بحث قرار گرفته است (تولا و همکاران، ۲۰۱۹؛ دا-ویجا و همکاران[۲۱]، ۲۰۲۰) و انتشار این پژوهش‌ها حاکی از این است که در نظر گرفتن شخصیت در متون مرتبط با فرهنگ امنیت سایبری در حال افزایش است و این امر با افزایش تحقیقات فرهنگ امنیت سایبری در پنج سال گذشته مطابقت دارد. نگرانی بالقوه در این جهت مربوط به حریم خصوصی خود کارکنان است. برای مثال، جمع‌آوری اطلاعات شخصیتی می‌تواند در ایجاد برنامه‌های فرهنگ امنیت سایبری سفارشی شده‌تر در سازمان‌ها مفید باشد، اما نگرانی‌های مربوط به حریم خصوصی کارمندان می‌تواند منجر به عدم تمایل افراد به اشتراک‌گذاری چنین اطلاعات شخصی با کارفرمای خود شود (تولا و همکاران، ۲۰۱۹: ۱۴۳).

علاوه بر این، یک عامل منحصر به فرد موجود در چند پژوهش، فرهنگ ملی است (دا-ویجا و مارتینز[۲۲]، ۲۰۱۷؛ دا-ویجا و همکاران، ۲۰۲۰؛ روهوانیا و اوفوف[۲۳]، ۲۰۱۹). ظهور این عامل، به‌ویژه در مقالات اخیر، می‌تواند نشان دهد که فرهنگ امنیت سایبری در سطح ملی نیز نقش کلیدی در ایجاد فرهنگ امنیت سایبری شرکتی ایفا می‌کند. این موضوع در پژوهش گکازا و همکاران نیز (۲۰۱۵) پیشنهاد شده است و در هستی‌شناسی فرهنگ امنیت سایبری ملی توسعه یافته است، که شامل مفاهیمی مانند آموزش نیروی کار و شرکت‌های کوچک، متوسط و خرد است.

به‌طورکلی به منظور اندازه‌گیری سطح فرهنگ امنیت سایبری لازم است که سازمان‌ها در نظر داشته باشند که مؤلفه مهم دانش و رفتار هر دو باید در جایی که منابع اجازه می‌دهند مورد آزمایش و مشاهده قرار گیرند، زیرا این کار دقیق‌ترین ارزیابی را از وضعیت فرهنگ امنیت سایبری ارائه می‌دهد (اوچندو و همکاران، ۲۰۲۱: ۲۱).

---

20. Van't Wout
21. Da-Veiga et al
22. Martins
23. Ruhwanya & Ophoff

پیشینهٔ پژوهش

کاویانی و همکاران (۱۳۹۹) در پژوهشی با عنوان «الگوی توسعه راهبردی منابع انسانی در حوزه امنیت سایبری نیروهای مسلح ج.ا.ایران[۲۴]» به این نتیجه دست یافتند که در کنار ابعاد فنی و تجهیزاتی، تحقق امنیت سایبری نیازمند توسعه و پرورش منابع انسانی شایسته و کارآمد است از این‌رو، پیشنهادهایی در خصوص چگونگی تحقق توسعه راهبردی منابع انسانی در حوزه امنیت سایبری نیروهای مسلح ارائه نمودند.

جورجیادو و همکاران (۲۰۲۱ پ) در پژوهشی با عنوان «طراحی ابزار ارزیابی فرهنگ امنیت سایبری با هدف قرار دادن زیرساختهای مهم در بحران کووید -۱۹» ابزاری را تهیه کردند که ریشه آن در چارچوب فرهنگ امنیتی است و در دو سطح سازمانی و فردی طبقه‌بندی شده است. این ابزار ۱۰ بعد مختلف امنیتی را در قالب ۵۲ حوزه پوشش داده است و بر اولین چارچوب و بینش‌های آشکار آن در طول یک بحران جهانی تأکید می‌کند.

تولا و همکاران (۲۰۲۱) در پژوهشی با عنوان «تحلیل تجربی چارچوب عوامل کلیدی فرهنگ امنیت اطلاعات» بیان نمودند چارچوب عوامل کلیدی فرهنگ امنیت اطلاعات شامل عوامل مؤثر بر فرهنگ امنیت و عوامل منعکس کننده آن است. طی این بررسی اکتشافی یافتهها نشان داد که چارچوب از اعتبار برخوردار است و تناسب قابل قبولی با دادهها دارد. این مطالعه یک شکاف مهم در رابطه معنی‌دار بین ویژگی‌های شخصیتی و فرهنگ امنیت را پر نمود. همچنین از طریق معرفی یک چارچوب جامع در عمل، که در ایجاد فرهنگ امنیت نقش دارد، به بهبود مدیریت امنیت اطلاعات کمک کرده است. عوامل در توجیه پذیرش فرهنگ امنیت بسیار حیاتی هستند و چارچوب، ابزار مهمی را ارائه داده که می‌تواند برای ارزیابی و بهبود فرهنگ امنیت سازمانی مورد استفاده قرار گیرد.

روش‌شناسی پژوهش

این پژوهش، یک بررسی روش‌شناختی است که با هدف طراحی و تعیین ساختار اولیه ابزاری به منظور ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری بومی ایران انجام گرفت. طبق بررسی انجام شده، متون منتشر شده در حوزه امنیت سایبری در مجلات معتبر داخلی و خارجی توسط پژوهشگران

۲۴- ج.ا. ایران: جمهوری اسلامی ایران

ایرانی تنها به ابعاد فنی و یا حقوقی آن اشاره کرده و از بررسی حلقه مهم آن یعنی حلقه انسانی با تأکید بر فرهنگ و آگاهی غافل شده‌اند که در نتیجه آن، ابزار معتبر بومی ایران ساخته و یا منتشر نشده است. از این‌رو، پژوهش حاضر به صورت زیر انجام گرفت.

به منظور ساخت ابزار جهت ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری، مقیاس لیکرت که یکی از رایج‌ترین مقیاس‌های اندازه‌گیری است، در نظر گرفته شد. برای ساخت مقیاس لیکرت بایستی ۶ مرحله انجام شود. مرحله اول انتخاب موارد تشکیل دهنده پدیده مورد اندازه‌گیری (فرهنگ و آگاهی امنیتِ سایبری) و تدوین گویه‌های مناسب (منظور گویه‌هایی که فعل آنها مثبت نوشته شده باشد) و نامناسب (منظور گویه‌هایی که فعل آنها منفی نوشته شده باشد) مربوط به موضوع؛ مرحله دوم اجرای مقدماتی گویه‌ها در یک نمونه تصادفی از پاسخ دهندگان؛ مرحله سوم ارزش‌گذاری و محاسبه نمره کل برای هر پاسخ دهنده؛ مرحله چهارم تعیین توان افتراقی[۲۵] گویه‌ها؛ مرحله پنجم انتخاب گویه‌های برگزیده و مرحله ششم تعیین ضریب قابلیت اعتماد مقیاس است (سرمد و همکاران، ۱۴۰۰: ۱۵۵).

جهت انتخاب موارد تشکیل دهنده پدیده مورد اندازه‌گیری (فرهنگ و آگاهی امنیتِ سایبری) و تدوین گویه‌های مناسب و نامناسب مربوط به موضوع تلاش شد تا با استفاده از روش تحلیل مضمون که یکی از روش‌های متداول مورد استفاده در پژوهش‌های کیفی است (رجبی و همکاران، ۱۳۹۷: ۹۲)، به گردآوری، تحلیل و تفسیر موضوع پژوهش اقدام شود.

پس از شناسایی مضمون‌ها، به منظور بررسی روایی، از روایی محتوا با نظرخواهی از خبرگان حوزه امنیت سایبری و برای سنجش اعتبار[۲۶] (پایایی) داده‌ها نیز از ضریب اعتبار هولستی[۲۷] استفاده شد. براساس این روش، ابتدا کدگذاری با بررسی و مطالعه خط به خط مقاله‌های ۳ سال اخیر داخل و خارج کشور (مقالات داخل کشور استخراج شده از پایگاه‌های معتبر مانند پایگاه مرکز اطلاعات علمی جهاد دانشگاهی[۲۸]، پژوهشگاه علوم انسانی و مطالعات فرهنگی[۲۹]، بانک اطلاعات نشریات کشور[۳۰] و مرجع دانش، ناشر تخصصی کنفرانس‌های ایران[۳۱] و مقالات خارج کشور استخراج شده از پایگاه‌های معتبر مانند گوگل محقق[۳۲] و ساینس دایرکت[۳۳]) به صورت دستی

25. Discriminant Power
26. Reliability
27. Holsti's Cofficient of Reliability

انجام شد و بعد از اتمام آن، کدگذاری رایانه‌ای با استفاده از نرم‌افزار MAXQDA نسخه آزاد ۲۰۲۰ انجام شد. پس از آن تعداد کدهای نگارش شده در هر یک از این دو مرحله در قالب فرمول روش هولستی جایگذاری شد و مقدار این شاخص بالاتر از ۰/۷ و به میزان ۰/۹۶ به‌دست آمد که نشان‌دهنده ۴ درصد خطا در الگوریتم شناسایی کدها می‌باشد. بنابراین اعتبار نیز تأیید گردید.

یافته‌های پژوهش

جهت شناسایی مؤلفه‌های دخیل در فرهنگ و آگاهی امنیت سایبری، مجموعه مقالات منتشر شده داخل و خارج کشور مربوط به ۳ سال اخیر (از زمان شیوع کووید-۱۹) (از زمستان ۱۳۹۸ شمسی معادل زمستان ۲۰۲۰ میلادی تا بهار ۱۴۰۱ شمسی معادل بهار ۲۰۲۲ میلادی) که در حوزه امنیت سایبری با تأکید بر فرهنگ و آگاهی بودند، مورد بررسی قرار گرفت. مجموع مقالات در این حوزه ۱۰۲ مقاله (تعداد ۱۷ مقاله در داخل کشور و تعداد ۸۵ مقاله در خارج کشور) بوده است. از جمله معیارهای ورود محتوای قابل اجرا برای سؤال پژوهش، مطالعات مربوط به فرهنگ و آگاهی امنیت سایبری، مقالاتی در مورد روش‌ها/عوامل مربوط به فرهنگ و آگاهی امنیت سایبری در بخش عمومی/خصوصی و از جمله معیارهای خروج، حذف مقالات خارج از محدوده این بررسی، به عنوان مثال، مطالعات مربوط به ارزیابی برنامه آگاهی امنیت اطلاعات حذف شد، انتشارات غیردانشگاهی مانند خلاصه مقالات، فصل‌های کتاب و گزارش‌های شرکت و همچنین دسترسی به متن کامل برای برخی از مقالات مرتبط فراتر از چکیده ممکن نبوده، بنابراین حذف شدند. بنابراین شناسایی، استخراج و کدگذاری پس از اعمال ملاک‌های خروج، از ۷۰ مقاله انجام شد و تعداد ۱۴۰۲ کد شناسایی گردید که پس از حذف کدهای تکراری و با تطبیق کدگذاری با کدگذاری دوم دستاورد آن (۷۵ کد مؤلفه) بود. در مرحله بعدی، پس از شناسایی مؤلفه‌ها، اقدام به طراحی گویه‌ها نموده و استخر اولیه گویه‌ها با ۹۸ گویه تهیه گردید. به منظور بررسی روایی، از روایی محتوا با نظرخواهی از خبرگان (حوزه امنیت سایبری و متخصصان سنجش و اندازه‌گیری)

28. https://www.sid.ir/fa/journal/
29. www.ensani.ir
30. www.magiran.com
31. www.civilica.ir
32. https://scholar.google.com/
33. https://www.sciencedirect.com

که اعضای پانل خبرگان را تشکیل می‌دادند، استفاده شد و در راستای آن شاخص نسبت روایی محتوا (CVR)[۳۴]، شاخص روایی محتوا (CVI)[۳۵]، درجه اهمیت[۳۶] و نمره تأثیر[۳۷] (IS) محاسبه گردید. جهت اطمینان از اینکه مهم‌ترین و صحیح‌ترین محتوای (ضرورت آیتم) انتخاب شده است از شاخص نسبت روایی محتوا و برای اطمینان از اینکه آیتم‌های ابزار به بهترین نحو جهت اندازه‌گیری محتوا طراحی شده‌اند از شاخص روایی محتوا استفاده گردید.

برای بررسی روایی صوری به شکل کمّی پس از اصلاح گویه‌ها براساس نظر متخصصان، جهت کاهش عبارت‌ها، حذف عبارت‌های نامناسب و تعیین اهمیت هر یک از عبارت‌ها از روش کمّی تأثیر آیتم طبق طیف لیکرت سه درجه‌ای استفاده شد (ابتدا میانگین مقادیر قضاوت‌های اعضای پانل بر طبق پیشنهاد لاوشه[۳۸] محاسبه شد و مطابق آن به منظور محاسبه مقدار میانگین قضاوت تعلق گرفته به هر جزء ابزار، گزینه ضروری بودن با عدد ۲؛ گزینه مفید است اما ضروری نیست با عدد ۱ و گزینه ضروری نیست با مقدار صفر جایگزین شد). بنابراین با استفاده از فرمول روش تأثیر آیتم (فرمول ۱)، روایی صوری برای هر کدام از آیتم‌ها محاسبه گردید.

فرمول (۱) روش تاثیر آیتم

$$\text{Impact Score} = \text{Frequency}(\%) \times \text{Importance}$$

در روش تأثیر آیتم در صورتی که نمره تأثیر مساوی و یا بیشتر از ۱/۵ باشد، عبارت مورد نظر برای تحلیل‌های بعدی مناسب بوده و در ابزار حفظ می‌گردد (حسینی و همکاران، ۱۳۹۴؛ به نقل از سودی و همکاران، ۱۳۹۸: ۶۶). تعداد متخصصان در این بخش ۱۱ نفر بوده‌اند که روایی محتوا توسط آنان مطابق جدول (۱) بررسی شد.

34. Content Validity Ratio
35. Content Validity Index
36. Importance Degree
37. Impact Score
38. Lawshe

جدول (۱) استخر نهایی گویه‌ها با استفاده از نظر خبرگان و شاخص‌های CVR، CVI و IS محاسبه شده

ردیف اولیه	ردیف جدید	ردیف فرم توزیع	گویه	CVR	نمره تاثیر	CVIave	وضعیت گویه
۲	۱	۱	مدیر ما برای درک مهارت‌ها و رفتارهایی که کارمندان به آنها پایبند نیستند، تحلیل شکاف مهارت‌ها را انجام می‌دهد و از این اطلاعات برای ساختن نقشه راه آموزش پایه استفاده می‌کند.	۰/٦٤	۱/٦٤	۰/۹۱	پذیرش
۳	۲	٤	مدیر ما جهت رفع شکاف مهارتی شناسایی شده برای تأثیر مثبت بر رفتار امنیتی کارمندان، آموزش ارائه می‌دهد.	۰/٦٤	۱/٦٤	۰/۹۱	پذیرش
٤	۳	۷	رفتار افراد با یکدیگر هنگام انتقال اطلاعات بانکی، مهم است.	۰/٦٤	۱/۷۳	۰/۹۱	پذیرش
٦	٤	۹	مهم است که یک کارمند درک درستی از امنیت و ایمنی کامپیوتر داشته باشد.	۰/۸۲	۱/۹۱	۰/۹۱	پذیرش
۱۱	۵	۱۰	بسیاری از حوادث امنیتی (امنیت سایبری) محل کار ما، ناشی از رفتار غیر ایمن است.	۰/٦٤	۱/٦٤	۰/۸۲	پذیرش
۱۳	٦	۱۲	ارزیابی مهارت‌های امنیتی (امنیت سایبری) با استفاده از آموزش و سپس امتیازدهی آنان، تعیین کننده شایستگی کارکنان است.	۰/۸۲	۱/۹۱	۰/۹۱	پذیرش
۱۸	۷	۱۳	کارمندان خطرات سایبری را که هر روز با آن روبه‌رو هستند، درک می‌کنند.	۰/٦٤	۱/۷۳	۰/۹۱	پذیرش
۱۹	۸	۸	برخی از همکاران از خطرات سایبری که احتمالاً در حال حاضر در معرض آن هستند، بی‌اطلاع هستند.	۰/٦٤	۱/۸۲	۱	پذیرش
۲۲	۹	۱٤	نوع موقعیت کارمند (میزان دسترسی، دانش، امتیازات و مهارت‌ها) در بروز حوادث امنیت سایبری اثرگذار نیست.	۰/٦٤	۱/۷۳	۰/۸۲	پذیرش
۲۳	۱۰	۱۷	خستگی یا خواب آلودگی اثری در امنیت سایبری محل کار ندارد.	۰/٦٤	۱/۷۳	۱	پذیرش
۲٤	۱۱	۱۱	حجم کار ذهنی بالا در امنیت سایبری محل کار اثرگذار نیست.	۰/٦٤	۱/۷۳	۱	پذیرش
۲۵	۱۲	۱۹	میزان آگاهی کارمند از موقعیت شغلی، اثری در امنیت سایبری محل کار ندارد.	۰/٦٤	۱/۷۳	۰/۹۱	پذیرش
۲۷	۱۳	۳	فرآیندها و محیط کار (برنامه‌ریزی و کنترل کار، جریان داده‌ها و تنظیم کار) در امنیت سایبری نقش دارند.	۰/٦٤	۱/۷۳	۰/۸۲	پذیرش

ردیف اولیه	ردیف جدید	ردیف فرم توزیع	گویه	CVR	نمره تاثیر	CVIave	وضعیت گویه
۳۰	۱٤	۲۰	مشکلات خانوادگی می‌تواند منجر به تنش در محل کار شود.	۰/٦٤	۱/۷۳	۰/۹۱	پذیرش
۳۱	۱۵	۲۱	اختلالات جدی سلامت روان تأثیری در امنیت سایبری محل کار ندارد.	۰/٦٤	۱/۸۲	۰/۹۱	پذیرش
۳۳	۱٦	۲۳	داشتن تجربه‌کاری در حوزه امنیت اطلاعات نقشی در امنیت سایبری محل کار ندارد.	۰/٦٤	۱/٦٤	۰/۹۱	پذیرش
۳٤	۱۷	۱۵	کارمندی که از سیستم‌های متصل به شبکه استفاده می‌کند باید در حوزه امنیت اطلاعات و حملات سایبری تخصص داشته باشد.	۰/٦٤	۱/۷۳	۰/۸۲	پذیرش
۳۷	۱۸	۱۸	نگران هستم که اگر یک حمله سایبری را به پلیس گزارش کنم ممکن است این گزارش به اعتبار محل کار من آسیب برساند.	۰/٦٤	۱/۷۳	۱	پذیرش
٤۰	۱۹	٦	رویکردهای خاص فنی، رفتاری، فرهنگی و شخصی به شناسایی خطرات امنیتی احتمالی مرتبط با انسان کمکی نمی‌کند.	۰/٦٤	۱/٦٤	۰/۹۱	پذیرش
٤۲	۲۰	۱٦	من خارج از زمان کاری، در حوزه امنیت اطلاعات منابع اطلاعاتی معتبر را مطالعه می‌کنم تا دانش خود در این حوزه را افزایش دهم.	۱	۲	۰/۹۱	پذیرش
٤٤	۲۱	۲	مدیریت بودجه‌بندی و تخصیص منابع برای آموزش کاربران جهت فراگیری راه‌های جلوگیری از نفوذ هکرها لازم است.	۰/٦٤	۱/٦٤	۰/۸۲	پذیرش
٤۵	۲۲	۵	راه‌کارهایی که از طریق برنامه‌ریزی زیرساخت‌های فنی به وجود می‌آیند و تست می‌شوند نقش قابل توجهی در آمادگی و واکنش سایبری دارند.	۰/٦٤	۱/۷۳	۰/۹۱	پذیرش
٤٦	۲۳	۲۵	اقدامات مبتنی بر وجود برنامه‌های تحقیق و توسعه در امنیت سایبری محل کار اثرگذار نیستند.	۰/٦٤	۱/٦٤	۰/۹۱	پذیرش

ردیف اولیه	ردیف جدید	ردیف فرم توزیع	گویه	CVR	نمره تاثیر	CVIave	وضعیت گویه
٤٧	٢٤	٢٦	برنامه آگاهی از امنیت سایبری که یک سرمایه‌گذاری بلندمدت سازمانی است، در صورت ارائه آموزش به صورت مستمر به ایجاد فرهنگ امنیت سایبری کمک می‌کند.	٠/٦٤	١/٧٣	٠/٩١	پذیرش
٤٨	٢٥	٢٧	آموزش، وسیله اول در مورد چگونگی جلوگیری از تهدیدهای امنیت سایبری است زیرا برنامه‌های آموزش تأثیر مثبت و قابل توجهی بر فرهنگ امنیت سایبری دارد.	٠/٦٤	١/٦٤	٠/٨٢	پذیرش
٥٣	٢٦	٢٨	اجرای سیاست‌های امنیتی و رویکردهای جدید در آموزش اثری در امنیت سایبری سازمان ندارد.	٠/٦٤	١/٦٤	٠/٩١	پذیرش
٥٤	٢٧	٢٢	افرادی که دارای مشکلات شخصیتی هستند، امنیت سازمان را به خطر می‌اندازند.	٠/٦٤	١/٧٣	٠/٩١	پذیرش
٦٠	٢٨	٢٩	ممکن است کارمندی به‌دلیل فقر فرهنگی با استفاده از سیستم محل کار خود اقدام به فعالیتی مجرمانه کند بدون آنکه مطلع باشد مرتکب جرم شده است.	١	٢	٠/٩١	پذیرش
٦١	٢٩	٣٠	حقوق ناکافی و افزایش روزافزون هزینه‌ها ممکن است بر انگیزه کاری کارکنان اثر منفی بگذارد اما در دقت آنان حین کار با سیستم اثری ندارد.	٠/٨٢	١/٨٢	٠/٩١	پذیرش
٦٧	٣٠	٢٤	حوادث غیر عمدی خودی ممکن است ناشی از ناآشنایی و ناآگاهی نسبت به فناوری اطلاعات و امنیت باشد.	٠/٦٤	١/٨٢	٠/٨٢	پذیرش
٧٠	٣١	٣١	اشکالات ساختار فنی فضای مجازی خود یک عامل ریسک برای امنیت سایبری است.	٠/٨٢	١/٨٢	٠/٨٢	پذیرش
٧٦	٣٢	٣٢	آشنا نبودن به مباحث روز فناوری‌های نوین یکی از دلایل عدم پیشرفت کارمندان در دوره‌های آموزشی مرتبط با امنیت سایبری است.	٠/٦٤	١/٧٣	٠/٨٢	پذیرش
٧٧	٣٣	٣٣	منابع انسانی ناکارآمد در به خطر افتادن امنیت سایبری سازمان اثری ندارد.	٠/٦٤	١/٧٣	٠/٨٢	پذیرش
٧٩	٣٤	٣٤	آمادگی برای پذیرش فناوری‌های نوین در محیط کاری و سواد رسانه‌ای در پیشرفت	٠/٨٢	١/٨٢	٠/٨٢	پذیرش

ردیف اولیه	ردیف جدید	ردیف فرم توزیع	گویه	CVR	نمره تاثیر	CVIave	وضعیت گویه
			کارمندان قدیمی در دوره‌های آموزشی راه-کارهای حفظ امنیت سایبری در سازمان اثر دارد.				
۸۷	۳۵	۳۵	رمزگذاری سیستم محل کار، از اعمال بدخواهانه برخی کارمندان که قصد دشمنی با همکار خود را دارند، جلوگیری می‌کند.	۰/۸۲	۱/۸۲	۰/۹۱	پذیرش
۸۸	۳۶	۳۶	پشتیبان‌گیری ضعیف اثری در از دست رفتن احتمالی داده‌های مهم سیستم در طول روز ندارد.	۰/٦٤	۱/۷۳	۰/۸۲	پذیرش
۸۹	۳۷	۳۷	به روزرسانی ضعیف باعث از دست رفتن احتمالی داده‌های مهم سیستم در طول روز می‌شود.	۰/٦٤	۱/۷۳	۰/۸۲	پذیرش
۹۰	۳۸	۳۸	امنیت فیزیکی ضعیف اثری در از دست رفتن احتمالی داده‌های مهم سیستم در طول روز ندارد.	۰/٦٤	۱/۷۳	۰/۹۱	پذیرش
۹۲	۳۹	۳۹	وجود نیروهای متخصص در حوزه امنیت سایبری در حفظ امنیت سایبری سازمان اثرگذار است.	۰/۸۲	۱/۸۲	۱	پذیرش
۹٤	٤۰	٤۰	اعتماد بی‌جا باعث بروز خطرات امنیتی می‌شود.	۰/۸۲	۱/۹۱	۰/۸۲	پذیرش
۹٦	٤۱	٤۲	ارزیابی شایستگی کارکنان در حوزه امنیت سایبری در شناخت نقاط ضعف و قوت کارکنان و انتخاب برنامه‌های آموزشی برای تقویت آنان در این حوزه اثرگذار است.	۰/۸۲	۱/۹۱	۰/۷۳	پذیرش
۹۸	٤۲	٤۱	تعهد و مسئولیت‌پذیری کارمند در حفاظت از اطلاعات موجود در سیستم‌ها به منظور حفظ امنیت سایبری سازمان ضرورتی ندارد.	۰/٦٤	۱/۸۲	۰/۸۲	پذیرش

پس از دستیابی به فرم نهایی گویه‌ها (فرم ۴۲ گویه‌ای) اقدام به تعیین طیف پاسخ براساس طیف چند درجه‌ای لیکرت گردید. به منظور جلوگیری از دست دادن داده، تصمیم بر آن شد تا در این مرحله از طیف ۱۱ درجه‌ای لیکرت از کاملاً مخالفم (نمره صفر) تا کاملاً موافقم (نمره ۱۰) استفاده شود و در صورت مطلوب نبودن نتایج، طیف ۱۱ درجه‌ای به طیف ۹ یا ۷ درجه‌ای تعدیل یابد. با توجه به محتوای گویه‌ها، شایسته است گویه‌های دارای فعل منفی یا محتوای منفی به صورت معکوس نمره‌گذاری شوند.

اجرای مقدماتی گویه‌ها در یک نمونه تصادفی از پاسخ دهندگان

در این مرحله، با توجه به اینکه فرم دارای ۴۲ گویه بود، به ازای هر گویه یک نفر نمونه در نظر گرفته شد و با اعمال افت احتمالی نمونه، در نهایت از ۵۰ نفر خواسته شد تا در پژوهش مشارکت نمایند. به منظور جلوگیری از پاسخ حدسی بدون توجه به متن گویه، گویه‌های دارای فعل یا محتوای منفی (نامناسب) در بین گویه‌های دارای فعل یا محتوای مثبت (مناسب) به صورت تصادفی قرار داده شدند (ستون سوم در جدول ۱) و فرم جدید ابزار در اختیار آنان قرار داده شد. در این بخش نرخ بازگشت فرم ۹۶ درصد بوده است. در مرحله بعدی، پس از ارزش‌گذاری و محاسبه نمره کل برای هر پاسخ دهنده؛ پاسخ‌های ۲۵ درصد گروه بالا و ۲۵ درصد گروه پایین به منظور محاسبه توان افتراقی تک تک گویه‌ها استخراج گردید که براساس آن به استثنا گویه شماره ۴۱ در فرم توزیع شده (توان افتراقی ۰/۹۴)، سایر گویه‌ها دارای توان افتراقی بیش از ۱ در گروه بالا و پایین بوده‌اند.

انتخاب گویه‌های برگزیده

اینک با توجه به نتایج به‌دست‌آمده از تحلیل هرگویه، به انتخاب گویه‌ها می‌پردازیم. در انجام دادن این امر، گویه‌هایی برگزیده می‌شوند که توان تشخیص آنها بیشتر از بقیه باشد و گویه‌هایی که توان تشخیص آن‌ها بسیار کم باشد نادیده گرفته می‌شوند (سرمد و همکاران، ۱۴۰۰: ۱۵۶). از بین ۴۲ گویه بررسی شده، به نظر می‌رسد گویه شماره ۴۱ در فرم توزیع شده، به خوبی نتوانسته است بین گروه بالا و پایین تفاوت قائل شود.

تعیین ضریب قابلیت اعتماد مقیاس به منظور بررسی میزان اعتبار درونی گویه‌های برگزیده (۴۲ گویه)

جهت بررسی اعتبار درونی ۴۲ گویه، از دو شیوه تعیین همسانی درونی[39] و ثبات[40]، استفاده گردید. برای اندازه‌گیری همسانی درونی از ضریب آلفای کرونباخ[41] استفاده شد. آلفای کرونباخ معرف میزان تناسب گروهی از گویه‌هاست که یک سازه را می‌سنجند. ارزیابی ثبات نیز از طریق روش

39. Internal Consistency
40. Stability

آزمون – بازآزمون انجام پذیرفت. نکته مهم در این روش فاصله زمانی بین دو آزمون است. فاکس[۴۲] (۱۹۸۲) معتقد است فاصله زمانی بین دو آزمون باید تا حدی باشد که از طرفی فراموشی عبارات ابزار اتفاق بیفتد و از طرف دیگر تغییر در پدیده مورد اندازه‌گیری رخ ندهد. برنز و گراو[۴۳] (۲۰۰۳) این فاصله زمانی را دو هفته تا یک ماه پیشنهاد کرده‌اند (سودی و همکاران، ۱۳۹۸: ۶۹). در پژوهش حاضر، مشارکت کنندگان ابزار را در ۲ مرحله، با فاصله زمانی دو هفته تکمیل کردند. سپس نمرات کسب شده در این ۲ مرحله با استفاده از آزمون شاخص همبستگی درون خوشه‌ای (ICC)[۴۴] با هم مقایسه شدند.

جدول (۲) بررسی همبستگی هر گویه با نمره کل ابزار

شماره گویه	همبستگی هر گویه با نمره کل	مقدار آلفای کرونباخ در صورت حذف‌گویه	شماره گویه	همبستگی هر گویه با نمره کل	مقدار آلفای کرونباخ در صورت حذف‌گویه
۱	۰/٤۳۰	۰/۹۱۱	۲۲	۰/۵۱۰	۰/۹۱۰
۲	۰/٤٤۲	۰/۹۱۱	۲۳	۰/٤۸۵	۰/۹۱۰
۳	۰/٦۲۷	۰/۹۰۸	۲٤	۰/۵۹۹	۰/۹۰۹
٤	۰/٤٦٦	۰/۹۱۰	۲۵	۰/٤۹٦	۰/۹۱۰
۵	۰/۵٦٤	۰/۹۰۹	۲٦	۰/٦۳۳	۰/۹۰۹
٦	۰/۵۸۱	۰/۹۰۹	۲۷	۰/٦۰۳	۰/۹۰۹
۷	۰/۷۱۲	۰/۹۰۸	۲۸	۰/۵۸٤	۰/۹۱۰
۸	۰/۰۰۷	۰/۹۱۹	۲۹	۰/٤۵٤	۰/۹۱۰
۹	۰/۵۵٦	۰/۹۰۹	۳۰	۰/۱٦۱	۰/۹۱٤
۱۰	۰/٤۰۸	۰/۹۱۱	۳۱	۰/۵۸٤	۰/۹۰۹
۱۱	۰/۲۵۵	۰/۹۱۳	۳۲	۰/۲۰٦	۰/۹۱۳
۱۲	۰/٤۳۲	۰/۹۱۱	۳۳	۰/۵۳۱	۰/۹۱۰

41. Cronbach's Alpha Coefficient
42. Fox
43. Burns & Grove
44. Intraclass Correlation Coefficient (ICC)

شماره گویه	همبستگی هر گویه با نمره کل	مقدار آلفای کرونباخ در صورت حذف‌گویه	شماره گویه	همبستگی هر گویه با نمره کل	مقدار آلفای کرونباخ در صورت حذف‌گویه
۱۳	۰/۳۰۰	۰/۹۱۲	۳٤	۰/۳۳٥	۰/۹۱۲
۱٤	۰/٤٤۸	۰/۹۱۰	۳٥	۰/٥٥۳	۰/۹۰۹
۱٥	۰/٤۳٥	۰/۹۱۱	۳٦	۰/٤۰۳	۰/۹۱۱
۱٦	۰/۳٥۹	۰/۹۱۱	۳۷	۰/۳۷٤	۰/۹۱۱
۱۷	۰/۲۸۸	۰/۹۱۲	۳۸	۰/٥٦٦	۰/۹۰۹
۱۸	-۰/۱٦٤	۰/۹۲۰	۳۹	۰/٦۰۹	۰/۹۰۹
۱۹	۰/۳۲۲	۰/۹۱۳	٤۰	۰/۳۷۲	۰/۹۱۱
۲۰	۰/۷۲۱	۰/۹۰۷	٤۱	۰/۷۰۹	۰/۹۰۸
۲۱	۰/٥٤۷	۰/۹۰۹	٤۲	۰/٥۹٥	۰/۹۰۹

همانطورکه بیان شد، به منظور بررسی میزان همسانی درونی گویه‌های برگزیده (اعتبار)، اقدام به بررسی ضریب آلفای کرونباخ شد و یافته‌های جدول (۲) نشان داد به استثنای گویه‌های شماره ۸، ۱۷، ۱۸، ۳۰ و ۳۲ فرم توزیع شده، سایر گویه‌ها دارای همبستگی ۰/۳۰ و بالاتر با نمره کل ابزار بودند. گویه شماره ۸ دارای ضعیف‌ترین همبستگی (کمتر از ۰/۰۱) و گویه شماره ۲۰ فرم توزیع شده دارای بیشترین همبستگی (۰/۷۲۱) با نمره کل ابزار بودند. بنابراین همه گویه‌ها به استثنای گویه شماره ۸ (همبستگی ۰/۰۰۷)، ۱۷ (همبستگی ۰/۲۸۸)، ۱۸ (همبستگی ۰/۱۶۴-)، ۳۰ (همبستگی ۰/۱۶۱) و گویه شماره ۳۲ (همبستگی ۰/۲۰۶) دارای همبستگی ۰/۳۰ و بالاتر با نمره کل ابزار بودند.

همبستگی درون‌خوشه‌ای یک روش از نوع آنالیز واریانس[45] است که در آن پاسخ‌ها[46] همان نمرات اختصاص داده شده توسط ارزیابان و داوران است. در جدول (۳) در سطر اول یافته‌های مربوط به اعتبار حاصل از همبستگی درون‌خوشه‌ای یک اندازه‌گیری[47] و در سطر دوم یافته‌های مربوط به اعتبار حاصل از همبستگی درون‌خوشه‌ای میانگین ارزیابان و داوران[48] گزارش شده است.

45. ANOVA
46. Responses
47. Single Measures
48. Average Measures

جدول (۳) همبستگی درون‌خوشه‌ای

	همبستگی درون خوشه‌ای	۹۵ درصد فاصله اطمینان برای ضرایب درونی		Fمقدار آماره			
		کران پایین	کران بالا	ارزش	درجه آزادی۱	درجه آزادی۲	سطح معناداری
یک اندازه‌گیری (یک ارزیاب)	۰/۲۵	۰/۱۸	۰/۳۵	۱۶/۲۰	٤۷	۲۰٦۸	۰/۰۰۱
میانگین ارزیابان و داوران	۰/۹٤	۰/۹۱	۰/۹٦	۱٦/۲۰	٤۷	۲۰٦۸	۰/۰۰۱

در جدول (۳)، ستون همبستگی درون‌خوشه‌ای و اعداد آن، همان چیزی است که به دنبال آن هستیم. عدد ۰/۲۵ بیانگر مقدار ضریب همبستگی درون رده‌ای یا همان ICC در سطر اول برای حالتی است که اندازه‌گیری‌ها فقط توسط یک داور انجام می‌شود. مقدار ICC در سطر دوم (میانگین ارزیابان و داوران) به خوبی بالا است. عدد ۰/۹۴ نشان می‌دهد اعتبار نمرات داده شده توسط ارزیابان، هنگامی که میانگین آنها مورد بررسی قرار می‌گیرد، کاملاً قابل قبول است. همان‌گونه که مشاهده می‌شود برای سطر میانگین ارزیابان کران بالای فاصله اطمینان ICC عدد ۰/۹۶ شده است. این عدد بالا، بیانگر توافق بسیار خوب داوران با یکدیگر به حساب می‌آید. در هر فرضیه و آزمون آماری نیز می‌دانیم که با مقدار احتمال و سطح معناداری روبه‌رو هستیم. عدد به دست آمده یعنی P<۰/۰۰۱ نشان می‌دهد که فرض صفر (یعنی برابر صفر بودن ICC) رد می‌شود. بنابراین می‌پذیریم که به صورت معنادار ICC از عدد صفر بزرگتر است، ابزار از ثبات لازم برخوردار است و ارزیابان با یکدیگر توافق دارند.

نتیجه‌گیری و پیشنهاد

با توجه به اینکه بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی در همه سطوح، اعم از افراد، مؤسسه‌های غیر دولتی و نهادهای دولتی و حاکمیتی، در فضای سایبری انجام می‌گیرد؛ اخیراً بسیاری از شرکت‌های خصوصی و سازمان‌های دولتی در سراسر جهان با مشکل حملات سایبری و خطر فناوری‌های ارتباطات بی‌سیم روبه‌رو هستند و برای دفاع در

برابر این حملات و با توجه به اینکه انسان‌ها نقش کلیدی در این فناوریها دارند، افزایش آگاهی از امنیت سایبری مهم است چرا که عدم آگاهی کاربران در مورد تهدیداتی که ممکن است در فضای مجازی با آن‌ها روبه‌رو شود، می‌تواند باعث اجرای موفقیت‌آمیز تهدیدها شود. بنابراین سطح آگاهی افراد می‌تواند در این مسئله دخیل باشد. از این‌رو اندازه‌گیری سطح آگاهی افراد می‌تواند راه‌گشای برنامه‌های آموزشی یا دوره ضمن خدمت برای کارکنان ادارات و یا سازمان‌ها باشد. از سویی دیگر، بررسی متون نشان داد آگاهی رابطه تنگاتنگی با فرهنگ دارد و در پدیده سایبری با فرهنگ امنیت سایبری مواجه هستیم. بنابراین پژوهش‌گران مقاله حاضر تصمیم بر ارائه ابزاری به منظور ارزیابی فرهنگ و آگاهی امنیت سایبری گرفتند. نظر به اینکه کارمندان افرادی هستند که به سرمایه مردم دسترسی دارند بنابراین ارزیابی سطح آگاهی و فرهنگ این افراد نسبت به امنیت سایبری ضرورت دارد. به همین دلیل در این پژوهش گروه هدف، کارمندان کشور در نظر گرفته شدند. در واقع این پژوهش، یک بررسی روش شناختی است که با هدف طراحی و تعیین ساختار اولیه ابزاری به منظور ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری برای کارمندان کشور انجام گرفته است. در مرحله اول با استفاده از تحلیل مضمون و بررسی اسناد بالادستی مؤلفه‌های دخیل در فرهنگ و آگاهی امنیت سایبری شناسایی شد و براساس آن تعداد ۹۸ گویه برای ارزیابی فرهنگ و آگاهی امنیت سایبری کارمندان در استخر اولیه گویه‌ها، تدوین شد. سپس استخر اولیه در اختیار خبرگان حوزه هدف (پلیس فتا و متخصصان سنجش و اندازه‌گیری) قرار داده شد و در راستای آن شاخص نسبت روایی محتوا، شاخص روایی محتوا، درجه اهمیت و نمره تأثیر محاسبه گردید که در نتیجه آن تعداد ۵۶ گویه حذف شد و فرم ۴۲ گویه‌ای حاصل شد. پس از دستیابی به فرم نهایی گویه‌ها اقدام به تعیین طیف پاسخ براساس طیف ۱۱ درجه‌ای لیکرت گردید سپس اقدام به توزیع ابزار در یک نمونه تصادفی از گروه هدف شد. در مرحله بعدی، توان افتراقی تک تک گویه‌ها محاسبه شد که براساس آن به استثنای گویه شماره ۴۱ فرم توزیع شده، سایر گویه‌ها دارای توان افتراقی بیش از ۱ در گروه بالا و پایین بوده‌اند. به نظر می‌رسد گویه شماره ۴۱ فرم توزیع شده از قدرت تشخیص مناسب برخوردار نبوده است و حذف آن از فرم ۴۲ گویه‌ای اگرچه شایسته به نظر می‌آید اما پس از برآورد اعتبار فرم ۴۲ گویه با استفاده از دو روش تعیین همسانی درونی و ثبات، نظر به اینکه این گویه دارای اعتبار مطلوب بوده است، از این رو در فرم حفظ گردید.

همانطورکه بیان شد، به منظور بررسی میزان همسانی درونی گویه‌های برگزیده (اعتبار)، اقدام به بررسی ضریب آلفای کرونباخ شد و یافته‌ها داد از بین ۴۲ گویه، گویه شماره ۸، ۱۸ و ۳۰ فرم توزیع شده دارای همبستگی زیر ۰/۲ با نمره کل ابزار بودند. با توجه به اینکه اعتبار با افزایش حجم نمونه بهبود می‌یابد احتمال می‌رود اعتبار گویه ۱۸و ۳۰ با افزایش حجم نمونه بهبود یابد اما در خصوص گویه شماره ۸ بعید است که این مقدار آلفای کرونباخی که ناچیزتر از ۰/۰۱ است (۰/۰۰۷) با افزایش حجم نمونه افزایش یابد. بنابراین گویه شماره ۸ حذف و دو گویه ۱۸ و ۳۰ در فرم حفظ شدند و ترجیح داده شد تا در پژوهش آتی، در حجم نمونه بالا (حداقل ۲۰۰ نفر) با استفاده از سایر روش‌های برآورد اعتبار و نیز با استفاده از روایی سازه این مسئله مورد بررسی قرار گیرد.

به‌طورکلی یافته‌های حاصل از بررسی روایی محتوا نشان داد تعداد ۵۶ گویه از دید خبرگان از کیفیت لازم برخوردار نبوده و حذف شدند. بررسی توان افتراقی بیانگر توان بالاتر از ۱ همه گویه‌ها به استثناء گویه شماره ۴۱ بود. نتایج اعتبار (با در نظر گرفتن خطای ۵ درصد) نشان داد گویه شماره ۸ فاقد همبستگی قابل قبول بوده، از این‌رو از فرم نهایی حذف گردید. در خصوص همبستگی درون‌خوشه‌ای نیز، کران بالای فاصله اطمینان ICC نیز بیانگر توافق بسیارخوب داوران با یکدیگر بود. در واقع می‌توان گفت فرم ۴۱ گویه‌ای تهیه شده، دارای روایی محتوا و اعتبار قابل قبول بوده، بنابراین شرایط لازم جهت بررسی در سطح نمونه اصلی گروه هدف را داشته و می‌توان آن را در نمونه وسیعی از گروه هدف، جهت دستیابی به ساختار نهایی و نمرات هنجار به کار گرفت.

از آنجایی‌که در کشور ابزاری به منظور ارزیابیِ فرهنگ و آگاهی امنیتِ سایبری یافت نشد و در راستای رفع این خلاء، پژوهش حاضر در قالب رساله دکتری به انجام رسید، از این رو پیشنهاد می‌شود مسئولان ذی‌ربط نسخه نهایی این ابزار را که روایی و اعتبار و سایر ویژگی‌های روان‌سنجی آن با استفاده از روش‌های تخصصی سنجش و اندازه‌گیری در پژوهش‌های بعدی نویسندگان این مقاله، مورد بررسی و تأیید واقع شده است در دوره‌های ضمن خدمتی که برای کارمندان خود برگزار می‌کنند، به کار گیرند و با توجه به سطح فرهنگ و آگاهی افراد نسبت به امنیت سایبری، دوره‌های آموزشی لازم را در دوره‌های ضمن خدمت کارمندان خود بگنجانند.

در پایان از کلیه خبرگان مشارکت کننده در این پژوهش قدردانی می‌شود.

منابع و ماخذ:

الف)منابع فارسی

۱. ترخان، محمدرضا و وحید فتوح‌آبادی (۱۳۹۵)، ارائه یک الگوی مفهومی مبتنی بر آگاهی موقعیتی با هدف بهبود امنیت سایبری، دومین کنفرانس بین‌المللی یافته‌های نوین پژوهشی در مهندسی برق و علوم کامپیوتر، رامسر: https://civilica.com/doc/545851.

۲. تقی‌پور، رضا و دیگران (۱۳۹۹)، الگوی راهبردی مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران. فصلنامه پژوهش‌های حفاظتی و امنیتی، ۹(۳۵)، ۹۵-۱۲۴. https://jpas.ihu.ac.ir/article_206634.html?lang=fa.

۳. ثقفی، کامیار و علی اسماعیلی (۱۳۹۹)، طراحی الگوی مفهومی پایش تهدیدات سایبری جمهوری اسلامی ایران. فصلنامه پژوهش‌های حفاظتی و امنیتی، ۹(۳۵)، ۶۵-۹۴. https://jpas.ihu.ac.ir/article_206633.html.

۴. رجبی، محمد و دیگران (۱۳۹۷)، تحلیل مضمون الزامات تحققِ امنیت انتظامی در اندیشه فرماندهی معظم کل قوا (مدظله‌العالی). فصلنامه انتظام اجتماعی، ۱۰(۲)، ۸۵-۱۰۸. http://sopra.jrl.police.ir/article_94576.html.

۵. رشیدی، علی جبار و محمد شکیبازاد (۱۳۹۵)، ارایه چهارچوبی به منظور دستیابی به آگاهی وضعیتی سایبری پویا در صحنه نبرد سایبری، چهارمین کنفرانس بین‌المللی مهندسی برق و کامپیوتر،تهران، https://civilica.com/doc/608950

۶. سرمد، زهره و دیگران (۱۴۰۰)، روش‌های تحقیق در علوم رفتاری، چاپ چهلم، تهران: انتشارات آگه.

۷. سودی، حورا و دیگران (۱۳۹۸)، طراحی و روان‌سنجی پرسشنامه مدرسه اثربخش با معیارهای فرهنگی جامعه ایرانی، فصلنامه رهیافتی نو در مدیریت آموزشی، ۱۰ (۴، ۴۰)، ۸۷-۸۴. http://jedu.miau.ac.ir/article_3860.html

۸. عسگری، محمود (۱۴۰۰)، فرهنگ امنیتی در جمهوری اسلامی ایران، فصلنامه پژوهش‌های حفاظتی و امنیتی، ۱۰(۳۷)، ۱۶۳-۱۹۶. https://jpas.ihu.ac.ir/article_206955.html.

۹. کاویانی، حسن و دیگران (۱۳۹۹)، الگوی توسعه راهبردی منابع انسانی در حوزه امنیت سایبری نیروهای مسلح ج.ا.ایران. فصلنامه علمی راهبرد دفاعی، ۱۸(۱)، ۳۷-۶۶.

https://ds.sndu.ac.ir/article_1008.html

۱۰. موحدی‌راد، محمدرضا و ناصر مدیری (۱۳۹۳)، ارائه رویکردی ساختارمند برای پیاده سازی رزمایش‌های سایبری، اولین همایش ملی پژوهش‌های مهندسی رایانه،تهران، https://civilica.com/doc/347171.

الف)منابع لاتین

1. Akhter, M. S., Islam, M. H., & Momen, M. N. (2020). Problematic internet use among university students of Bangladesh: The predictive role of age, gender, and loneliness. Journal of Human Behavior in the Social Environment, 30(8), 1082-1093. https://www.tandfonline.com/doi/abs/10.1080/10911359.2020.1784346
2. Al-Alawi, A. I., & Al-Bassam, S. A. (2021). Assessing The Factors of Cybersecurity Awareness in the Banking Sector. AGJSR 37 (4): 17-32. Retrieved from https://www.researchgate.net/profile/Adel-Al-Alawi/publication/352855616
3. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404820302765
4. Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1), e06016. https://www.sciencedirect.com/science/article/pii/S2405844021001213
5. Banciu, D., Radoi, M., & Belloiu, S. (2020). Information security awareness in Romanian public administration: an exploratory case study. Studies in Informatics and Control, 29(1),

121-129. https://sic.ici.ro/information-security-awareness-in-romanian-public-administration-an-exploratory-case-study/

6. Bino, J. V. (2021). CYBER SECURITY AWARENESS BY USING SOCIAL MEDIA PLATFORMS AMONG STUDENTS. International Journal of Research, 8(5), 581-589. Retrieved from http://ijrjournal.com/index.php/ijr/article/view/51
7. Cardoso, L., & Castanho, M. (2021). A CYBERCULTURE STUDY: K-POP AND THE NEW MEDIA-BTS AND TWITTER. European Journal of Social Sciences Studies, 6(6). Retrieved from https://www.oapub.org/soc/index.php/EJSSS/article/view/1127/1713
8. Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. Computers & Security, 70, 72-94. https://www.sciencedirect.com/science/article/pii/S0167404817300937
9. Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers & Security, 92, 101713. https://www.sciencedirect.com/science/article/pii/S0167404820300018
10. Elradi, M. D., Altigani, A., & Abaker, O. I. (2020). Cyber security awareness among students and faculty members in a Sudanese college. Journal of Electrical Science & Engineering, 2(2), 24–28. https://ojs.bilpublishing.com/index.php/ese/article/view/2477
11. Evans, M., He, Y., Luo, C., Yevseyeva, I., Janicke, H., &

Maglaras, L. A. (2019). Employee perspective on information security related human error in healthcare: Proactive use of IS-CHEC in questionnaire form. IEEE Access, 7, 102087-102101. https://ieeexplore.ieee.org/abstract/document/8755984

12. Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021a). Designing a cyber-security culture assessment survey targeting critical infrastructures during covid-19 crisis. International Journal of Network Security & Its Applications (IJNSA) Vol, 13, 33-50. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3787197
13. Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021c). Working from home during COVID-19 crisis: a cyber security culture assessment survey. Security Journal, 1-20. Retrieved from https://link.springer.com/article/10.1057/s41284-021-00286-2
14. Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. Procedia Computer Science, 181, 59-66. https://www.sciencedirect.com/science/article/pii/S1877050921001381
15. Khan, A. H., Sawhney, P. B., Das, S., & Pandey, D. (2020, February). SartCyber Security Awareness Measurement Model (APAT). In 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC) (pp. 298-302). IEEE. Retrieved from https://ieeexplore.ieee.org/abstract/document/9087242
16. Ruhwanya, Z., & Ophoff, J. (2019). Information security culture assessment of small and medium-sized enterprises in Tanzania.

In International Conference on Social Implications of Computers in Developing Countries (pp. 776-788). Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-030-18400-1_63

17. Tolah, A., Furnell, S. M., & Papadaki, M. (2019). A comprehensive framework for understanding security culture in organizations. In IFIP World Conference on Information Security Education (pp. 143-156). Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-030-23451-5_11
18. Tolah, A., Furnell, S. M., & Papadaki, M. (2021). An Empirical Analysis of the Information Security Culture Key Factors Framework. Computers & Security, 108, 1-34. https://www.sciencedirect.com/science/article/pii/S0167404821001784
19. Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387. Retrieved from https://www.sciencedirect.com/science/article/pii/S016740482100211X
20. Yuchong, L. & Qinghui, L. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 1-11, In Press. https://www.sciencedirect.com/science/article/pii/S2352484721007289