Scientific Journal of Electronical & Cyber Defence
Vol. 11, No. 1, Spring 2023, Serial No. 41

Identify the Factors Affecting the Culture and Awareness of Cyber Security Using Theme Analysis

S. Heydari, M. Barzgar*, A. H. Mohammad Davoodi

*Assistant Professor, Department of Psychology, Marvdasht Branch, Islamic Azad University, Marvdasht, Iran

(Received: 08/06/2021, Accepted: 03/10/2021)

ABSTRACT

Cybercriminals are targeting more humans than machines these days because they try to exploit users' vulnerabilities to achieve their destructive goals. The main purpose of this study is to identify the factors affecting the culture and awareness of cyber security using theme analysis. The research is applied in terms of purpose, exploratory in terms of method and qualitative in terms of data type. The research data includes all valid articles in the field of culture and cyber security awareness published in 2020 to 2022 inside and outside the country, with 3 keywords (culture, awareness, cyber security) in the valid have been collected and reviewed in the framework of MAXQDA software. The criteria for entering articles in the research was the applicable content for the research question and the criteria for excluding abstracts, book chapters, short reports and lack of access to the full text of the article. Validity was assessed using content validity and data reliability was estimated using Holstie method. Findings showed a review of 392 theme identified the basic themes related to cybersecurity culture and awareness, of which 12 themes were asset organizing, continuity, access and trust, operations, protection, security governance, attitude, behavior, competence, commitment and support, cyber security and they covered the budget. The identified factors can be used as analytical tools in the field of assessing the culture and awareness of cyber security, which is an important factor in the occurrence of cybercrime, in a logical and principled way to reduce cybercrime and solve related problems in the economic field. Educational, security, social and cultural payments.

Keywords: Theme analysis, Effective Factors, Culture, Awareness, Cyber Security.

* Corresponding Author Email: Mbarzegar55@gmail.com

نشریه علمی "پدافند الکترونیکی و سایبری"
سال یازدهم، شماره ۱، بهار ۱۴۰۲، ص ۶۷-۸۰

علمی – پژوهشی

شناسایی عوامل مؤثر بر فرهنگ و آگاهی امنیت سایبری با استفاده از تحلیل مضمون

صدیقه حیدری[۱]، مجید برزگر[۲*]، امیرحسین محمّدداودی[۳]

۱- دانشجوی دکترا، واحد ساوه، دانشگاه آزاد اسلامی، ساوه، ۲- استادیار، واحد مرودشت، دانشگاه آزاد اسلامی، مرودشت، ۳- دانشیار، گروه مدیریت آموزشی، واحد ساوه، دانشگاه آزاد اسلامی، ساوه، ایران

(دریافت: ۱۴۰۰/۱۲/۲۵، پذیرش: ۱۴۰۱/۰۳/۱۸)

چکیده

این روزها، مجرمان سایبری بیشتر انسان‌ها را هدف قرار می‌دهند تا ماشین‌ها، زیرا سعی می‌کنند با سوءاستفاده از نقاط ضعف کاربران، اهداف مخرب خود را به انجام برسانند. هدف اصلی پژوهش حاضر شناسایی عوامل مؤثر بر فرهنگ و آگاهی امنیت سایبری با استفاده از تحلیل مضمون است. پژوهش از نظر هدف کاربردی، از نظر روش، اکتشافی و از نظر نوع داده، کیفی است. داده‌های پژوهش شامل کلیه مقالات معتبر در حوزه فرهنگ و آگاهی امنیت سایبری منتشر شده در سال‌های ۲۰۲۰ الی ۲۰۲۲ در داخل و خارج کشور می‌باشد که با ۳ کلیدواژه (فرهنگ، آگاهی، امنیت سایبری) در پایگاه‌های معتبر جمع‌آوری و با بهره‌گیری از روش تحلیل مضمون، در چارچوب نرم‌افزار MAXQDA مورد بررسی قرار گرفته است. معیار ورود مقالات به پژوهش، محتوی قابل اجرا برای سؤال پژوهش و معیارهای خروج خلاصه مقالات، فصل‌های کتاب، گزارش‌های کوتاه و عدم دسترسی به متن کامل مقاله بوده است. سنجش روایی با استفاده از روایی محتوی و برآورد پایایی داده‌ها با استفاده از روش هولستی انجام شد. یافته‌ها نشان داد از بررسی متون ۳۹۲ مضمون پایه مرتبط بافرهنگ و آگاهی امنیت سایبری شناسایی شد که ۱۲ مضمون سازمان‌دهنده دارایی‌ها، تداوم، دسترسی و اعتماد، عملیات، محافظت، حکمرانی امنیتی، نگرش، رفتار، شایستگی، تعهد و حمایت، رعایت امنیت سایبری و بودجه‌بندی را پوشش دادند. عوامل شناسایی شده می‌توانند در قالب ابزار تحلیلی در زمینهٔ ارزیابی فرهنگ و آگاهی امنیت سایبری که عامل مهمی در وقوع جرائم سایبری است، مبنای عمل قرار گیرد تا به‌گونه‌ای منطقی و اصولی به کاهش جرائم سایبری و حل مشکلات مرتبط با آن در حوزه‌های اقتصادی، آموزشی، امنیتی، اجتماعی و فرهنگی پرداخت.

کلیدواژه‌ها: تحلیل مضمون، عوامل مؤثر، فرهنگ، آگاهی، امنیت سایبری.

۱- مقدمه

امروزه در شروع هزاره سوم میلادی فناوری‌های نوین اطلاعات و ارتباطات به نحوه شگفت‌آوری وارد ساختار زندگی انسان‌ها شده است که تجلی آن فضای تبادل اطلاعات (فضای سایبر) است [۱]. این فضا امکاناتی را در اختیار افراد قرار داده که تمیز مجرمان از هم را مشکل، انجام جرم به‌سهولت و قربانی شدن به‌راحتی صورت می‌گیرد [۲]. در سال‌های اخیر نقض حریم شبکه‌های اطلاعاتی و ارتباطی که بیشتر با نام حملات سایبری شناخته می‌شوند [۳] و گرایش به این حملات مبتنی بر باج‌افزارها به‌صورت نمایی و به‌شدت در حال افزایش است [۴]، ازاین‌رو تلاش‌هایی در مقیاس بزرگ و کوچک برای کاهش تهدیدات امنیت سایبری در سراسر جهان انجام شده است. بااین‌حال، محققان استدلال کرده‌اند که، علی‌رغم آمادگی‌های فناورانه که کشورها می‌توانند برای محافظت از خود در برابر حملات انجام دهند، عوامل انسانی ممکن است دلیل اصلی افزایش نقض امنیت سایبری در سال‌های اخیر باشد. پژوهش محمّد و همکاران [۵] که در زمینه علوم اجتماعی توسعه‌یافته است، استدلال کرده است که عوامل انسانی درون و بین‌فردی، مانند عوامل زیستی، روانی و فرهنگی، باید به‌طورکلی در نظر گرفته شوند تا به طور مؤثر آگاهی از اهمیت امنیت مجازی افزایش یابد.

در حقیقت انقلاب در زمینه فناوری اطلاعات منجر به افزایش چشمگیر تعداد افراد متصل به اینترنت و استفاده از آن‌ها شده است [۶] و افزایش وابستگی به فناوری‌های اطلاعاتی خطرات احتمالی حملات سایبری[۲] را چندین برابر کرده است [۷]. علی‌رغم کنترل‌های فناورانه پیشرفته‌ای که توسط سازمان‌ها اجرا می‌شود، عامل انسانی همچنان از طریق کانال‌های مهندسی اجتماعی به‌عنوان یک تهدید قابل‌توجه در این فضا دیده می‌شود. شرکت‌ها می‌توانند راه‌حل‌های فنی مناسب را پیاده‌سازی کنند، اما هنوز قادر به کنترل عامل انسانی نیستند. در این راستا ابراهیمی[۸] مدلی ارائه کرده است که بر عناصر امنیت انسانی از جمله تعهد مدیریت، مهارت‌ها، تجربیات، خودکارآمدی منابع انسانی و فرهنگ امنیتی و آموزش به‌عنوان عوامل آسیب‌پذیر در مسائل امنیت سایبری تمرکز دارد، چرا که مردم دائماً از طریق رایانه‌های خود به سوابق بانکی، مالی و پزشکی خود دسترسی دارند که خود در برابر تهدیدات امنیت سایبری آسیب‌پذیر

* رایانامه نویسنده مسئول: Mbarzegar55@gmail.com

[2] - cyber-attacks

هستند. براین‌اساس، سازمان‌ها اخیراً در معرض خطر امنیت سایبری قرار گرفته‌اند که به‌موجب آن، اقدامات پیشگیرانه‌ای را برای حفظ امنیت اطلاعات سازمانی و کنترل ریسک انجام می‌دهند. امروزه کارکنان از مکان‌های مختلف برای دسترسی به اطلاعات سازمانی از طریق تلفن همراه خود استفاده می‌کنند. تغییرات در شرایط کار، به‌ویژه در بحران‌هایی مانند کرونا، به کارکنان اجازه می‌دهد تا با کار از راه دور از خانه خود به اطلاعات سازمانی دسترسی داشته باشند. ازاین‌رو دانش امنیت سایبری برای همه کارمندان یا کاربران باتوجه‌به نیاز آن‌ها ضروری است و برنامه آگاهی از امنیت سایبری که یک سرمایه‌گذاری بلندمدت سازمانی است، در صورت ارائه آموزش به‌صورت مستمر به ایجاد فرهنگ امنیت سایبری کمک می‌کند [۹].

به‌طورکلی شهروندان با چالش‌های عظیمی همچون حفظ امنیت سایبری، امنیت سایبری و حریم خصوصی سایبری روبرو هستند. دولت‌ها نیز منابع قابل‌توجهی را برای افزایش آگاهی شهروندان خود در مورد این سه حوزه اختصاص می‌دهند تا آن‌ها را برای مدیریت خطرات برخط خود مجهز کنند. برای اطمینان از حداکثر کارایی، این تلاش‌ها باید بتوانند سطوح موجود آگاهی را بسنجند تا اطمینان حاصل شود که ایجاد آگاهی شکاف‌های آگاهی در سطح جمعیت را هدف قرار می‌دهد. تعدادی پرسش‌نامه مناسب و دقیق برای این منظور وجود دارد. بااین‌حال، ممکن است این موارد در آشکارکردن شکاف‌ها و مسائل آگاهی در کشورهای درحال‌توسعه دقیق نباشد. شهروندان کشورهای درحال‌توسعه با طیف وسیعی از چالش‌های زمینه‌ای خاص، متفاوت از چالش‌هایی که شهروندان کشورهای توسعه‌یافته با آن مواجه‌اند، روبرو هستند و این امر احتمالاً بر توسعه و نگهداری آگاهی سایبری آن‌ها تأثیر می‌گذارد. بنابراین مدلی جهت سنجش آگاهی سایبری، شانس بیشتری برای آشکارکردن جنبه‌های آگاهی خاصی دارد که نیاز به توجه دارند [۱۰].

در تکمیل مطالب ذکر شده باید گفت تسریع حملات سایبری در سال‌های اخیر بر عملکرد کلی سازمان‌ها در سراسر جهان تأثیر منفی گذاشته و سازمان‌ها برای پیشگیری و مقابله با حملات سایبری با چالش افزایش امنیت سایبری خود روبرو هستند، اما مطالعاتی در مورد عوامل مؤثر بر آگاهی امنیت سایبری سازمان‌ها از دیدگاه جامع وجود ندارد [۱۱] و متأسفانه این مسئله در کشور ما (ایران) نیز به چشم می‌خورد؛ فقدان هم‌افزایی نهادهای پژوهشی امنیت سایبری در کشور باعث شده است تا بهره‌مندی از مدلی برای حاکمیت این فضا به‌منظور استفاده متناسب از همه ظرفیت‌ها، راه‌حلی مناسب برای حاکمیت محسوب شود [۱۲].

در واقع با افزایش موارد نقض سایبری، باید به‌موقع بررسی شود که چگونه می‌توان ضعیف‌ترین حلقه در این زنجیره امنیتی، یعنی انسان را تقویت کرد. همچنین باید بررسی شود که چگونه هنجارهای فرهنگی، به‌عنوان انتظارات مشترک و قوانینی که رفتار افراد را در گروه‌های اجتماعی هدایت می‌کنند، بر تصمیم افراد جهت اتخاذ اقدامات حفاظتی، تأثیر می‌گذارد. از سویی دیگر، رفتارهای امنیتی فردی به انگیزه و محیط فرهنگی افرادی بستگی دارد که از تهدیدات سایبری آگاه باشند، خطرات سایبری را درک کنند و اقدامات حفاظتی در برابر تخلفات سایبری انجام دهند [۱۳].

ازاین‌رو مسئله‌ای که ذهن نگارندگان این سطور را درگیر نموده است، این امر است که عوامل مؤثر بر فرهنگ و آگاهی امنیت سایبری، چه عواملی هستند؟ بر پایه همین پرسش و باتوجه‌به مقالات معتبر در حوزه فرهنگ و آگاهی امنیت سایبری منتشر شده در ۲ سال اخیر در داخل و خارج کشور، تلاش شد تا با استفاده از روش تحلیل مضمون[1]، این عوامل شناسایی و تفسیر شوند.

۱-۲- مبانی نظری

بیش از دو دهه است که اینترنت نقش مهمی در ارتباطات جهانی ایفا کرده و به طور فزاینده‌ای در زندگی مردم سراسر جهان ادغام شده است. نوآوری‌ها و هزینه کم در این زمینه دسترسی، استفاده و عملکرد اینترنت را به میزان قابل‌توجهی افزایش داده است، بنابراین امروزه اینترنت حدود ۳ میلیارد کاربر در سراسر جهان دارد [۱۴]. اینترنت یک شبکه جهانی گسترده ایجاد کرده است که سالانه میلیاردها دلار برای اقتصاد جهانی تولید می‌کند [۱۵] و این روزها، بیشتر فعالیت‌های رسانه‌ای به این فضا منتقل می‌شود، بیشتر مبادلات مالی از طریق این فضا انجام می‌شود و بخش قابل‌توجهی از زمان و فعالیت شهروندان صرف تعامل در این فضا می‌گردد [۱۶].

ازاین‌رو، سهم درآمد کسب‌وکارهای فضای مجازی در تولید ناخالص داخلی کشورها به میزان قابل‌توجهی افزایش یافته است و در بین شاخص‌های تعیین شده برای اندازه‌گیری میزان توسعه، شاخص‌های فضای مجازی سهم عمده‌ای دارند. بخش قابل‌توجهی از سرمایه مادی و معنوی کشورها صرف این فضا می‌شود و بخش قابل‌توجهی از درآمد مادی و دستاوردهای معنوی شهروندان به دست می‌آید یا تأثیر عمده‌ای بر این فضا دارد [۱۷]. به عبارت دیگر، جنبه‌های مختلف زندگی شهروندان به معنای واقعی کلمه با این فضا آمیخته شده است و هرگونه بی‌ثباتی، ناامنی و چالش در این فضا بر جنبه‌های مختلف زندگی شهروندان تأثیر مستقیم می‌گذارد [۱۸] و اینجاست که ما با مقوله‌ای با عنوان «فرهنگ و آگاهی امنیتِ سایبری» مواجه هستیم. فرهنگ به‌عنوان مجموعه‌ای از نگرش‌ها، ارزش‌ها، اهداف و عملکردهای مشترک بیان می‌شود که یک نهاد یا سازمان را تعریف می‌کند. بنابراین

[1] Thematic Analysis

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 فناورانه و اقدامات متقابل امنیتی که آن را تعریف می‌کند، مشخص می‌شود [۱۹و۲۰] و آگاهی از آن عبارت از شناسایی، پیشگیری و مقابله با حملات سایبری [۲۱] و تصمیم‌گیری درست و به‌موقع برای مقابله با حملات سایبری [۲۲] است.

رسولی [۲۳] با مطالعه متون حوزه امنیت سایبری مهم‌ترین حملات سایبری را شامل جنگ سایبری، حمله‌های سایبری، جرائم سایبری، جاسوسی سایبری و آشفتگی‌های سایبری دانسته و ذکر کرده است که برای مقابله با این تهدیدات سه سطح امنیت که باید به آن‌ها توجه کرد شامل حوزه‌های امنیتی زیرساخت‌ها، سطح امنیتی در حوزه‌های فردی و اجتماعی و سطح امنیتی در حوزه‌های ملی و حاکمیتی می‌باشد [۲۳]. این پدیده امنیت ملی را از ابعاد مفهوم امنیت، دولت‌محوری در امنیت، بعد جغرافیایی تهدید، گستردگی آسیب‌پذیری‌ها، شیوه مقابله با تهدیدها و تعدد بازیگران در این عرصه، تحت‌تأثیر قرار داده است [۲۴].

در واقع فضاهای سایبری امروزی به طور فزاینده‌ای خصومت‌آمیز شده‌اند و برنامه‌ها و راهکارهایی که از طریق برنامه‌ریزی و اجرای رزمایش‌های سایبری به وجود می‌آیند و تست می‌شوند نقش قابل‌توجهی در آمادگی و واکنش سایبری دارند و باعث ایجاد امنیت بیشتر در فضای سایبری می‌گردند [۲۵]. در این راستا مرور ادبیات سیستماتیک در ۱۰ سال گذشته (۲۰۱۰-۲۰۲۰) نشان داد که درحالی‌که تغییرات قابل‌توجهی در استفاده از اصطلاحات (به‌عنوان مثال فرهنگ امنیت اطلاعات و فرهنگ امنیت سایبری) ایجاد شده است، بسیاری از عوامل تأثیرگذار مشابه هستند. حمایت، 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 [۲۶].

این روزها، مجرمان سایبری بیشتر انسان‌ها را هدف قرار می‌دهند تا ماشین‌ها، زیرا آن‌ها سعی می‌کنند با سوءاستفاده از نقاط ضعف کاربران، اهداف مخرب خود را به انجام برسانند. بنابراین، آسیب‌پذیری‌های انسانی تهدیدی جدی برای امنیت و یکپارچگی سیستم‌ها و داده‌های رایانه‌ای است. گرایش بشر به اعتماد و کمک به دیگران، و همچنین خصوصیات شخصی، اجتماعی و فرهنگی، نشان‌دهنده میزان حساسیت است که ممکن است شخص نسبت به انواع خاصی از حملات و راهبردهای فریبکاری از خود نشان دهد. نتایج حاصل از بررسی متون نشان داده است که ارزیابی آسیب‌پذیری انسان در چارچوب‌های مختلفی باهدف ارزیابی ظرفیت امنیت سایبری سازمان‌ها گنجانده شده است، اما این امر به ارزیابی یک‌بار و نه به‌صورت مداوم مربوط می‌شود. علاوه بر این، بدخواهی انسان هنوز در چارچوب‌های فعلی ارزیابی آسیب‌پذیری انسان نادیده گرفته می‌شود [۲۷].

به‌هرحال در این پژوهش فرهنگ و آگاهی امنیت سایبری مدنظر قرار گرفته شد تا بر مبنای آن عوامل مؤثر شناسایی گردد؛ این عوامل در زمینه‌های سیاسی، اقتصادی، اجتماعی، فرهنگی، نظامی و غیره مطرح می‌شود. البته باید توجه داشت که فرهنگ و آگاهی امنیت سایبری را می‌توان از لحاظ سطح‌بندی نیز به سطوح مختلف فردی، داخلی، ملی، منطقه‌ای و جهانی تقسیم‌بندی نمود که به فراخور بحث، نگارندگان به دنبال عوامل مؤثر بر فرهنگ و آگاهی امنیت سایبری با تأکید بر بُعد انسانی که پوشش‌دهنده بخش عظیمی از سطوح مطرح شده است، خواهند بود.

۳-۱- پیشینه پژوهش

جعفری [۱۲] در پژوهش خود به این نتایج رسید که امنیت فضای سایبر، پیرو فضای سایبر، تحت‌تأثیر تغییرات مستمر است و به دلیل این که حفظ امنیت در این فضا از مسائل مهم در امنیت ملی کشور محسوب می‌شود و همچنین به علت نبود هم‌افزایی نهادهای پژوهشی امنیت سایبری در ایران، بهره‌مندی از مدلی برای حاکمیت این فضا به‌منظور استفاده متناسب از همه ظرفیت‌ها، راه‌حلی مناسب برای حاکمیت محسوب می‌شود. وی بیان کرد که از مهم‌ترین گزاره‌های موجود در حوزه امنیت سایبری ارائه سیاست‌های یکپارچه از طریق ایجاد نقشه راه فناوری و محصولات بومی امنیت سایبر، نهادینه شده دغدغه امنیت در کشور و مدیریت متعهد به بخش خصوصی می‌باشد.

صفائی و قدیری [۲۸] در پژوهش خود تمام روندهای فعلی حملات امنیت سایبری در طی همه‌گیری و چگونگی تغییر حملات بین همه‌گیرهای مختلف را ارائه داده، تأثیر کووید-۱۹ بر جامعه، از دیدگاه تهدید امنیت سایبری را نیز بیان کرده و در مورد اینکه چرا آموزش امنیت سایبری هنوز از اهمیت بالایی برخوردار است، بحث کردند. نتایج حاصل از مصاحبه با خبرگان حوزه امنیت سایبری حاکی از آن بود که آموزش، وسیله اول در مورد چگونگی جلوگیری از تهدیدهای امنیت سایبری است.

کاویانی و همکاران [۲۹] در پژوهشی به این نتیجه رسیدند که در کنار ابعاد فنی و تجهیزاتی، تحقق امنیت سایبری نیازمند توسعه و پرورش منابع انسانی شایسته و کارآمد است و بر اساس

نتایج تحقیق، پیشنهادهایی در خصوص چگونگی تحقق توسعه راهبردی منابع انسانی در حوزه امنیت سایبری نیروهای مسلح ارائه دادند.

عظمی و همکاران [۳۰] در پژوهشی به این نتیجه رسیدند که آموزش امنیت، برنامه‌های آموزش و آگاهی از امنیت اطلاعات تأثیر مثبت و قابل‌توجهی بر فرهنگ امنیت اطلاعات داشت. علاوه بر این، رفتار امنیتی گزارش شده کارکنان به‌عنوان یک واسطه جزئی در رابطه بین آگاهی از امنیت اطلاعات و فرهنگ امنیت اطلاعات عمل نمود.

جورجیادو و همکاران [۳۱] در پژوهشی به این نتیجه رسیدند که تهدید خودی هم توسط جامعه علمی و هم متخصصان امنیتی به‌عنوان یکی از بزرگ‌ترین خطرات امنیتی برای شرکت‌ها، مؤسسات و سازمان‌های دولتی شناخته شده است. این پژوهش باهدف ارائه چارچوب فرهنگ امنیت سایبری با تمرکز واضح بر عامل انسانی، رویکرد خاص شاخص‌های فنی، رفتاری، فرهنگی و شخصی را در نظر گرفته و در شناسایی خطرات احتمالی امنیتی ناشی از افراد ممتاز کمک می‌کند.

کولینز و هیندز [۳۲] در پژوهشی به این نتیجه رسیدند که ایجاد عادات اجتناب‌ناپذیر یا ناخودآگاه، پرورش آگاهانه عادات و تأثیرات اجتماعی و سازمانی در حوزه امنیت سایبری مهم هستند. بر اساس یافته‌ها، دستورالعمل‌هایی برای حمایت از ایجاد عادت امنیت سایبری در محل کار ارائه شد که این تجربیات ذهنی را منعکس می‌کند، یعنی معرفی راه‌حل‌های خودکار، تسهیل نشانه‌های خارجی، افزایش علاقه به مسائل امنیت سایبری در بین کارکنان، ایجاد فرهنگ شغلی امنیت سایبری مثبت و برجسته‌سازی رفتار مثبت و ارائه دسترسی به اطلاعات امنیت سایبری قابل دسترس برای کارکنان. این نتایج اولین گام در شناسایی چگونگی سوءاستفاده از عادات برای تغییر رفتارهای امنیت سایبری مثبت است، به‌گونه‌ای که وابستگی به رفتارهای عادی در محیط‌های شلوغ و تحت فشار زمان می‌باشد.

در یک جمع‌بندی از مطالب ارائه شده باید گفت این پژوهش‌ها در درجه اول به‌صورت کل‌نگری بوده و در درجه دوم به طور دقیق عوامل مؤثر بر فرهنگ و آگاهی امنیت سایبری را پوشش نداده‌اند و تنها اشاراتی به ضعیف‌بودن حلقه انسانی نموده‌اند و به توصیف آن به‌صورت مختصر اکتفا کرده‌اند. براین‌اساس، مهم‌ترین وجوه نوآورانه و تمایزبخش پژوهش حاضر از سایر پژوهش‌ها را می‌توان در روش‌مندی، دقیق بودن و گزارش یافته‌های جدید مختص پاندمی کووید-۱۹ و پاندمی‌های مشابه احتمالی در آینده، در آن دانست. ازاین‌رو، در بخش بعدی پس از ارائه روش، نتایج و بحث در قالب دو بخش آشنایی با داده‌ها و کدگذاری اولیه و نیز جستجو برای یافتن مضامین به گزارش یافته‌ها اقدام شده؛ ابتدا مجموعه مقالات فاقد طبقه‌بندی حوزه امنیت سایبری با تأکید بر فرهنگ و آگاهی در داخل کشور و خارج کشور و سپس در بخش دوم مضامین پایه، سازمان‌دهنده و فراگیر امنیت سایبری با تأکید بر فرهنگ و آگاهی در قالب جدول تدوین گردیده و در نهایت شبکه مضامین عوامل مؤثر در فرهنگ و آگاهی امنیت سایبری ترسیم گردید.

۲- روش تحقیق

پژوهش حاضر از نوع کیفی بوده و درصدد است تا با استفاده از روش تحلیل مضمون به گردآوری، تحلیل و تفسیر موضوع پژوهش اقدام نماید. این روش دارای شش گام است که به ترتیب عبارت از آشناشدن با داده‌ها، کدگذاری اولیه، جستجو برای یافتن مضامین، بازبینی مضامین، تعریف و نام‌گذاری مضامین و تولید گزارش نهایی هستند. تحلیل مضمون شیوه‌ای در روش پژوهش کیفی است که بر شناسایی، تحلیل و تفسیر الگوی معانی داده‌های کیفی تمرکز دارد. مضمون عنصر کلیدی در این روش است. مضمون‌ها پرارزش‌ترین واحدهایی هستند که در تجزیه‌وتحلیل محتوا باید مدنظر قرار گیرند و منظور از مضامین معنای خاصی است که از یک کلمه یا جمله یا پاراگراف مستفاد می‌شود. قابل ذکر است که روش تحلیل مضمون، طیف گسترده‌ای از فنون را دربر می‌گیرد اما در این پژوهش باتوجه‌به هدف و سؤالات پژوهش از تکنیک شبکه مضامین استفاده شده است که در آن پژوهشگر داده‌ها را برای شناسایی مضامین بررسی نموده، مضامین پایه، سازمان‌دهنده و فراگیر را تشخیص داده و پس از آن، یک نقشه گرافیکی از ارتباط میان آن‌ها را نمایش می‌دهد. این شبکه‌ها صرفاً ابزاری تحلیلی هستند و نه خود تحلیل؛ وقتی یک شبکه مضمونی ساخته شد می‌توان از آن به‌مثابه ابزاری تصویری برای تفسیر متن استفاده کرد تا نتایج حاصل از متن و خود متن برای پژوهشگر و خوانندگان روشن شود [۳۳].

در واقع مضامینِ شناخته، منبع اصلی تشکیل شبکه‌های مضامین است و در آن مشخص خواهد شد که برخی مضامین پیشنهادشده، واقعاً مضمون نیستند (مثلاً اگر داده‌های کافی وجود نداشته باشد و یا داده‌های آن، خیلی متنوع باشد)، برخی مضامین با همدیگر هم‌پوشانی دارد (مثلاً اگر دو مضمونِ جدا، یک معنی و مفهوم داشته باشد و با هم مضمون واحدی، تشکیل دهند) و ممکن است لازم باشد سایر مضامین به مضامین جداگانه‌ای تفکیک شود.

در پژوهش حاضر به‌منظور بررسی روایی، از روایی محتوی به مدد خبرگان حوزه امنیت سایبری کشور و محاسبه دو شاخص نسبت روایی محتوی (CVR)[1] و شاخص روایی محتوی (CVI)[2]

[1] - Content Validity Ratio
[2] - Content Validity Index

استفاده شد. تعداد متخصصان در این بخش ۵ نفر بوده‌اند که روایی محتوی توسط آنان تأیید شد (CVR=1 و CVI=0.99).

برای سنجش اعتبار[1] (پایایی) داده‌ها نیز از ضریب اعتبار هولستی[2] استفاده شد. هولستی از جمله صاحب‌نظران تحلیل محتوی است که فرمولی را برای تعیین اعتبار داده‌های اسمی بر حسب درصد توافق مشاهده شده (*PAO*)[3]، ارائه کرده است. بر اساس این روش، ابتدا کدگذاری با بررسی و مطالعه خط‌به‌خط مقاله‌های ۲ سال اخیر داخل و خارج کشور (۱۳ مقاله داخل کشور استخراج شده از پایگاه‌های معتبر مانند پایگاه مرکز اطلاعات علمی جهاد دانشگاهی[4]، پژوهشگاه علوم انسانی و مطالعات فرهنگی[5]، بانک اطلاعات نشریات کشور[6] و مرجع دانش، ناشر تخصصی کنفرانس‌های ایران[7] و ۵۷ مقاله خارج کشور استخراج شده از پایگاه‌های معتبر مانند گوگل محقق[8] و ساینس دایرکت[9]) به‌صورت دستی 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:

$$PAO = \frac{2M}{(N_1+N_2)} \qquad (۱)$$

در این فرمول M تعداد موارد کدگذاری مشترک بین دو کدگذاری (۳۹۲) و N_1 (۴۲۸) و N_2 (۳۹۲) به ترتیب تعداد کلیه موارد کدگذاری شده توسط کدگذاری اول و دوم است. مقدار PAO بین صفر (عدم توافق) تا یک (توافق کامل) قرار می‌گیرد و اگر از ۰/۷ بزرگ‌تر باشد مطلوب است. در پژوهش حاضر مقدار این شاخص بالاتر از ۰/۷ و به میزان ۰/۹۶ به دست آمد. بنابراین اعتبار نیز تأیید گردید.

۳- نتایج و بحث

۳-۱- آشنایی با داده‌ها و کدگذاری اولیه

برای انجام پژوهش حاضر، مجموعه مقالات منتشر شده داخل و خارج کشور مربوط به ۲ سال اخیر (از زمان شیوع کووید-۱۹) (از زمستان ۱۳۹۸ شمسی معادل زمستان ۲۰۲۰ میلادی تا زمستان ۱۴۰۰ شمسی معادل زمستان ۲۰۲۲ میلادی) که در حوزه امنیت سایبری با تأکید بر فرهنگ و آگاهی بودند، مورد بررسی قرار گرفت. کلیدواژه‌های مورد استفاده جهت جستجو نیز سه کلیدواژه "فرهنگ، آگاهی و امنیت سایبری" بودند. 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 محتوی 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، به‌عنوان 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. ازاین‌رو، شناسایی، استخراج و کدگذاری پس از اعمال ملاک‌های خروج، از ۶۸ مقاله (۱۳ مقاله فارسی و ۵۵ مقاله انگلیسی) انجام شد و تعداد ۱۴۰۲ کد (۲۴۸ کد در مقالات فارسی و ۱۱۵۴ در مقالات انگلیسی) کد شناسایی گردید که پس از حذف کدهای تکراری (۱۱۴ کد در مقالات فارسی و ۳۱۴ کد در مقالات انگلیسی) حاصل و با تطبیق کدگذاری با کدگذاری دوم دستاورد آن در جدول (۱) (۹۴ کد) و جدول (۲) (۲۹۸ کد) ارائه شده است.

جدول (۱): مجموعه مقالات فاقد طبقه‌بندی حوزه امنیت سایبری با تأکید بر فرهنگ و آگاهی در داخل کشور

ردیف	منبع	نکات کلیدی	تعداد اولیه	تعداد نهایی
۱	[۳۴]	امنیت فرهنگی، سرمایه اجتماعی، سواد رسانه‌ای، امنیت اخلاقی، پایبندی به مذهب، پایبندی به آداب‌ورسوم، احساس تعلق به هویت ملی، عدالت اجتماعی، اعتماد اجتماعی، جامعه‌پذیری.	۱۱	۱۰
۲	[۲]	عوامل فردی (تخصص داشتن)، عوامل خانوادگی (سرمایه اجتماعی - خانوادگی)، عوامل اجتماعی، سرمایه اجتماعی، بسته‌بودن حوزه عمومی، تغییرات سبک زندگی، ناکامی‌های اجتماعی، مدیریت نامناسب اوقات فراغت، اعتراض اجتماعی، عوامل فرهنگی (اعتقادات و باورهای دینی، جنون ثروت)، عوامل اقتصادی (احساس محرومیت نسبی، رواج فساد در جامعه)، عوامل سیاسی و قضایی (غلبه تفکر سختگیرانه در دستگاه قضایی، سیاست‌گذاری در زمینه فضای مجازی، فقدان شفافیت در ساختار و عملکرد حاکمیت و دولت)، دو ساحتی	۴۵	۲۸

[1] - Reliability
[2] - Holsti's Cofficient of Reliability
[3] - Percentage of Agreement Observation
[4] - https://www.sid.ir/fa/journal/
[5] - www.ensani.ir
[6] - www.magiran.com
[7] - www.civilica.ir
[8] - https://scholar.google.com/
[9] - https://www.sciencedirect.com

ردیف	منبع	نکات کلیدی	تعداد اولیه	تعداد نهایی
		شدن جامعه، ورود ارزش‌های مدرن به جامعه، گسترش جهانی‌شدن، زیرساخت‌های فنی، دانش، مشارکت اجتماعی، همبستگی.		
۳	[۳۵]	هوشمندسازی، فرهنگ‌سازی، عوامل روان‌شناختی، توانمندسازی، هویت فرهنگی، خودآگاهی، فضاسازی رسانه‌ای.	۲۳	۷
۴	[۳۶]	محافظت (ایمن‌سازی و پایداری امنیت)، دسترسی، شایستگی کارکنان، تهدید بنیان‌های خانواده، نارضایتی کارکنان از فشار کاری، استفاده از گوشی هوشمند و رعایت‌نکردن ملاحظات امنیتی، یکپارچگی، حریم خصوصی، منابع و دارایی‌های سایبری، آسیب‌های امنیتی، توان و قدرت پاسخگویی به تهدید، روش‌های مدیریت و نظارت.	۳۹	۱۶
۵	[۳۷]	فقر فرهنگی، مشکلات روحی روانی.	۸	۲
۶	[۳۸]	مدیریت اشتراک اطلاعات، فیلترینگ، ناآرامی اجتماعی، کثرت اجتماعی، انعطاف زمانی، انتشار اخبار جعلی، گسترش طلاق، خیانت، افول بنیان خانواده (آسیب اجتماعی).	۳۷	۱۱
۷	[۳۹]	نظارت مستمر امنیت، مدیریت امنیت شبکه.	۲۶	۲
۸	[۴۰]	باورها و افکار، خودکنترلی.	۱۲	۲
۹	[۱]	عوامل درون‌سازمانی (نیروهای متخصص و آموزش‌دیده، رصد و پایش)، عوامل برون‌سازمانی (بهره‌برداری از اقدامات فنی و مخابراتی، همکاری با دیگر بانک‌ها و همکاری‌های بین‌المللی، سیستم عدالت کیفری، راه‌اندازی اینترنت ملی).	۲۴	۹
۱۰	[۲۹]	توسعه و پرورش نیروی انسانی.	۵	۱
۱۱	[۲۳]	جنگ سایبری، حمله‌های سایبری، آشفتگی‌های سایبری، حوزه‌های ملی.	۱۰	۴
۱۲	[۴۱]	نیروی انسانی	۳	۱
۱۳	[۴۲]	حکمرانی امنیتی.	۵	۱

جدول (۲): مجموعه مقالات فاقد طبقه‌بندی حوزه امنیت سایبری با تأکید بر فرهنگ و آگاهی در خارج کشور

ردیف	منبع	نکات کلیدی	تعداد اولیه	تعداد نهایی
۱	[۴۳]	کنترل‌های امنیتی در سازمان، زیان مالی.	۶	۲
۲	[۴۴]	ثبات سیاسی (عدم وجود خشونت/شاخص تروریسم)، فرهنگ متکی بر کنترل دولتی، مدیریت فضای سایبری، اقدامات حقوقی، اقدامات سازمانی (اقدامات مبتنی بر وجود هماهنگی نهادها)، اقدامات ظرفیت‌سازی (اقدامات مبتنی بر وجود برنامه‌های تحقیق و توسعه)، باتنت‌ها، بدافزار، کیفیت نظارتی.	۳۹	۱۲
۳	[۴۵]	قلدری سایبری	۹	۱
۴	[۴۶]	جعل هویت، محرک‌ها (ترس، کنجکاوی، ارتباط جنسی، طمع).	۱۸	۵
۵	[۸]	آگاهی امنیت سایبری، خطای انسانی، قربانی شدن، استاندارد زندگی، سرقت اطلاعات بانکی در فضای سایبری، فیشینگ، ایمیل‌های ناشناس.	۲۸	۷
۶	[۴۷]	نقض داده‌ها (افشای غیرمجاز اطلاعات شخصی)، جرایم مالی فردی، خطرات مرتبط با محتوا (قرارگرفتن در معرض محتوای غیرقانونی یا نامناسب)، ردگیری سایبری.	۲۲	۶
۷	[۴۸]	امنیت سایبری، عامل انسانی، تأثیرات روان‌شناسی کاربر، رمز عبور.	۱۰	۴
۸	[۴۹]	پشتیبانی مدیریت (مشارکت امنیت مدیریت، تخصیص منابع و بودجه‌بندی)، پیشینه فرهنگی، ارتباطات و تجربه، رفتارهای همکار (استقلال، اشتراک‌پذیری)، ویژگی‌های جمعیتی (سن، جنس، صنعت‌کار و سطح تحصیلات)، مفروضات و باورهای فرهنگی، دید امنیتی (در معرض قرارگرفتن)، مهارت‌ها.	۳۹	۱۹
۹	[۲۷]	تمایل انسان به کمک، سوءاستفاده	۷۳	۳۳

ردیف	منبع	نکات کلیدی	تعداد اولیه	تعداد نهایی
		کاربر، ویژگی‌های شخصیتی (گشودگی، وظیفه‌شناسی (صداقت، خودمداری قوی و مسئولیت‌پذیری)، برون‌گرایی (مهارت‌های اجتماعی: احساس راحتی، مشتاق، پرانرژی، پرحرف)، توافق‌پذیری، روان‌رنجوری (سطح اضطراب، ثبات هیجانی))، فرایندهای شناختی(تصمیم‌گیری، ریسک‌پذیری و انگیزه حفاظت)، تکنیک‌های متقاعدسازی (متقابل، کمیابی، اثبات اجتماعی (تطابق)، اختیار و دوست‌داشتن.)، قضاوت اجتماعی، امنیت دستگاه، موقعیت‌های اجتماعی فعلی (مانند شیوع کووید-۱۹)، حجم کار.		
۱۰	[۶]	خطرات امنیتی، حساب‌های مالی، داده‌های محرمانه.	۱۳	۳
۱۱	[۱۶]	مدیریت نیروی کار، مقیاس‌پذیری، انعطاف‌پذیری، داده‌های بسیار، ناامنی سایبری، رایانش ابری، مهندسی اجتماعی مبتنی بر شبکه "ارتباطات مبتنی بر "DoS/DDoS"، نقص نرم‌افزار"، پردازنده‌های جاسازی شده (حملات کلیدی شناخته شده"، سیستم‌های کنترلی "حملات هدفمند"، شنود.	۳۱	۱۴
۱۲ ۱۳	[۳۱]، [۵۰]	خرابکاری فناوری اطلاعات: جعل (نقش سازمانی: امتیازات، مهارت‌ها)، سابقه تصدی و سطح سابقه، فقدان حسابرسی)، رویدادهای استرس‌زا، عدم تشخیص تخلف از قوانین)، تهدید ناخواسته خودی (خستگی یا خواب‌آلودگی، چارچوب‌بندی، محدودیت‌های شناختی، سوگیری‌ها یا استدلال نادرست، خلق‌وخوی، تأثیر حالات فیزیکی، مواد مخدر یا هورمون عدم تعادل)، مدیریت پیکربندی سخت‌افزار، ایمنی و امنیت فیزیکی)؛ استمرار (مکانیسم‌های پشتیبان‌گیری، تداوم کسب‌وکار)؛ تفکیک نقش، روابط شخص ثالث)؛ عملیات (بررسی انطباق، تکمیل مستندات، تمایز کارآمد توسعه، رویه‌های عملیاتی)؛ حاکمیت امنیتی (مدیریت چک‌لیست‌های حسابرسی)؛ نگرش (جو کارکنان، پروفایل و رضایت کارکنان).	۱۰۴	۳۷
۱۴	[۲۰]	روابط بین کارکنان.	۱۲	۱
۱۵	[۵۱]	ارتباط ریسک، پیام‌های امنیتی	۱۸	۳

ردیف	منبع	نکات کلیدی	تعداد اولیه	تعداد نهایی
		متقاعدکننده، بهره‌برداری از سوگیری‌های شناختی.		
۱۶	[۵۲]	هویت سایبری، شهرت دیجیتال.	۲۶	۲
۱۷	[۵۳]	سطح تحصیلات، حملات اینترنت اشیا.	۹	۲
۱۸	[۵۴]	رسانه‌های اجتماعی	۸	۱
۱۹	[۵۵]	دارایی‌های معنوی	۱۲	۱
۲۰	[۵۶]	مجرمان سایبری	۱۳	۱
۲۱	[۱۹]	سازگاری کلی فناوری، دورکاری، بلوغ امنیتی مدیریت، کار تیمی؛ سطح فردی فرهنگ (ترس از ویروس کرونا، عوامل امنیتی مرتبط با انسان، درک خطر امنیتی، سابقه شغلی، تجربه کاری و تخصص تهدیدات سایبری مرتبط با انسان).	۴۱	۱۱
۲۲	[۳۲]	انگیزش درونی و بیرونی، مدل‌سازی اجتماعی.	۸	۲
۲۳	[۵۷]	تاکتیک‌ها، تکنیک‌ها، رویکرد نوآورانه، فروشندگان و مشتریان سازمانی، شبیه‌سازی دشمن.	۲۶	۵
۲۴	[۵۸]	منافع شخصی، سهل‌انگاری، حملات به وب‌میل و سرورهای VPN شرکتی، سیستم‌های کنترل قدیمی در تأسیسات	۳۴	۴
۲۵	[۵۹]	موانع درک شده، خودکارآمدی امنیتی.	۷	۲
۲۶	[۶۰]	امنیت ملی، شناسایی، هوش مصنوعی.	۲۳	۳
۲۷	[۶۱]	اسرار تجاری، مسائل امنیتی، بار فرهنگی ناپایدار.	۱۲	۳
۲۸	[۲۶]	فرهنگ ملی، رفتار اخلاقی، انگیزش کارکنان.	۱۹	۳
۲۹	[۶۲]	فناوری ارتباطات، جرم مجازی، شناسایی یک وب‌سایت/لینک تقلبی، دانلود فایل‌ها.	۱۶	۴
۳۰	[۶۳]	فرهنگ دیجیتال، ویژگی‌های فرهنگی، حفاظت از خود.	۱۴	۳
۳۱	[۱۱]	آمادگی امنیت سایبری (کارکرد، شناسایی (کنترل پورت‌های فعالیت‌هایی برای حفاظت از خدمات سایبری، رمزگذاری داده‌ها) بازیابی (فعالیت‌هایی برای بازیابی خرابی‌ها)	۲۱	۷
۳۲	[۶۴]	باج‌افزار، نقض امنیت داده.	۹	۲
۳۳	[۶۵]	حفاظت و ایمنی.	۵	۲
۳۴	[۷]	جوامع، خطاهای کاربر، فرهنگ محل کار، شناسایی و برنامه‌ریزی.	۱۹	۴
۳۵	[۶۶]	فرهنگ سایبری (تعهد مدیریت عالی، مدیریت و عملیات امنیتی)؛ مالکیت امنیت اطلاعات؛ فرهنگ امنیت مجموعه (آگاهی از حوادث، ارزش‌ها و	۸۸	۲۴

ردیف	منبع	نکات کلیدی	تعداد اولیه	تعداد نهایی
		موانع)؛ راهبردی و نظارت امنیتی؛ ارزیابی فرهنگ حفاظت از اطلاعات (تعهد، ضرورت، اهمیت و مسئولیت پذیری امنیت اطلاعات)؛ رعایت نظارت بر امنیت اطلاعات، پیامدها، سرمایه‌گذاری، سازگاری و قابلیت فناوری اطلاعات)؛ فرهنگ گزارش‌دهی و واکنش به گزارش رویداد، مسائل عمومی امنیت اطلاعات.		
۳۶	[۶۷]	احراز هویت دومرحله‌ای، مدیریت بودجه‌بندی برای آموزش کاربران.	۹	۲
۳۷	[۶۸]	یادگیری	۸	۱
۳۸	[۶۹]	کنترل‌های فنی، توانایی‌های شناختی مانند IQ غیرکلامی، تکانشگری شناختی.	۱۵	۳
۳۹	[۷۰]	تروریسم سایبری، افزایش قانون سایبری.	۸	۲
۴۰	[۷۱]	حملات ویروس، فقدان قوانین بین‌المللی یکسان و قوی.	۱۲	۲
۴۱	[۷۲]	توسعه و تقویت فرهنگ امنیتی سازمان.	۶	۱
۴۲	[۷۳]	ارزیابی مشارکت (سازمانی و خصوصی).	۱۰	۳
۴۳	[۷۴]	حوادث امنیتی، خطرات سایبری.	۱۴	۲
۴۴	[۷۵]	فرهنگ امنیت اطلاعات.	۷	۱
۴۵	[۷۶]	آگاهی از ریسک.	۷	۱
۴۶	[۷۷]	شناسایی رفتارهای کلیدی، فرهنگ امنیت سایبری	۵	۲
۴۷	[۷۸]	خطرات امنیت سایبری.	۱۳	۱
۴۸	[۷۹]	عوامل انسانی، سیستم‌های اطلاعاتی، خط‌مشی (نظارت، دستگاه‌های شخصی، امنیت فیزیکی)، عوامل محیطی.	۳۲	۷
۴۹	[۸۰]	تبادل اطلاعات، بی‌دقتی، نقض امنیت اطلاعات.	۷	۳
۵۰	[۸۱]	اعتبار، ویژگی‌های انسانی.	۲۹	۲
۵۱	[۸۲]	فرهنگ سازمانی (انتظارات، استانداردها و اصول، آرمان‌های مشترک سازمان)، بینش، ایدئولوژی‌ها، رویه‌های شرکت، روحیه، قوانین سازمان‌ها، ذهن‌آگاهی، تشخیص و توانایی توجیه.	۳۰	۱۱
۵۲	[۸۳]	رفتار امنیت اطلاعات فردی، سفارشی‌سازی برای نیازهای کارکنان و سازمان، ادغام منابع یادگیری الکترونیکی و فیزیکی.	۱۳	۳
۵۳	[۸۴]	تعامل انسان و کامپیوتر.	۲۴	۱
۵۴	[۸۵]	آپلود ناخودآگاه اپلیکیشن‌های تلفن همراه.	۱۸	۱
۵۵	[۸۶]	ساختار فعالیت‌ها و ارزیابی ریسک (توان‌بخشی، قوانین/سیاست‌های امنیت سایبری (پردازش و ذخیره‌سازی، گردش کار، مکان فیزیکی سرورها))، تحول دیجیتال، هنجارها و ارزش‌های افراد، افزایش مهارت‌های دیجیتال	۳۰	۹

۲-۳- جستجو برای یافتن مضامین

در این مرحله، تلاش می‌شود تا کدهای به‌دست‌آمده از مرحله پیشین ذیل مضامین پایه، سازمان‌دهنده و فراگیر طبقه‌بندی گردند. جدول شماره (۳)، نمایی از این تلاش را ترسیم نموده است.

جدول (۳): مضامین پایه، سازمان‌دهنده و فراگیر امنیت سایبری با تأکید بر فرهنگ و آگاهی در مقالات ۲ سال اخیر ایران و جهان

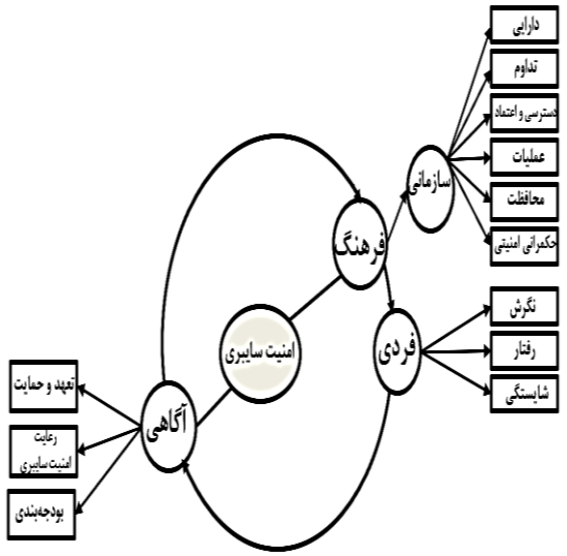
مضمون فراگیر	مضامین سازمان‌دهنده		مضامین پایه
فرهنگ و آگاهی امنیت سایبری	فرهنگ سازمانی	دارایی‌ها	امنیت فرهنگی، پایبندی به مذهب، اعتقادات و باورهای دینی، هویت فرهنگی، منابع و دارایی‌های سایبری، سرمایه اجتماعی، سرمایه اجتماعی - خانوادگی، نیروی انسانی، حوزه‌های ملی، ویژگی‌های جمعیتی، اسرار تجاری.

مضمون فراگیر	مضامین سازمان‌دهنده		مضامین پایه
		تداوم	نظارت مستمر امنیت، مکانیسم‌های پشتیبان‌گیری، تداوم کسب‌وکار، کیفیت نظارتی، خط‌مشی (نظارت، دستگاه‌های شخصی، امنیت فیزیکی).
		دسترسی و اعتماد	تفکیک نقش، روابط شخص ثالث، اعتماد اجتماعی، دورکاری، کار تیمی، فروشندگان و مشتریان سازمانی، تعامل انسان و کامپیوتر، فیلترینگ.
		عملیات	بررسی انطباق، تکمیل مستندات، تمایز کارآمد توسعه، رویه‌های عملیاتی، قوانین سازمانی.
		محافظت (جهت تمرکز بر آینده‌نگری)	زیرساخت‌ها (هوشمندسازی، فرهنگ‌سازی، توانمندسازی، رسیدگی به زیرساخت‌های فرهنگی - آموزشی، فضاسازی رسانه‌ای، ایمن‌سازی و پایداری امنیت، ارتقا کمی و کیفی منابع انسانی)، توان و قدرت پاسخگویی به تهدید، هوش مصنوعی،
		حکمرانی امنیتی	روش‌های مدیریت و نظارت، مدیریت اشتراک اطلاعات، مدیریت امنیت شبکه، مدیریت امنیت فضای سایبری، مدیریت نیروی کار، مدیریت پیکربندی سخت‌افزار، سیاست‌گذاری در زمینه فضای مجازی، اقدامات ظرفیت‌سازی (اقدامات مبتنی بر وجود برنامه‌های تحقیق و توسعه)، شناسایی و برنامه‌ریزی، بهره‌برداری از اقدامات فنی و مخابراتی، اقدامات حقوقی، اقدامات سازمانی (اقدامات مبتنی بر وجود هماهنگی نهادها)، شناسایی رفتارهای کلیدی، ارزیابی فرهنگ حفاظت از اطلاعات (تعهد، ضرورت، اهمیت و مسئولیت‌پذیری امنیت اطلاعات)؛ ارزیابی مشارکت (سازمانی و خصوصی)، ساختار فعالیت‌ها و ارزیابی ریسک (توان‌بخشی، قوانین/سیاست‌های امنیت سایبری (پردازش و ذخیره‌سازی، گردش کار،

مضمون فراگیر	مضامین سازمان‌دهنده		مضامین پایه
			مکان فیزیکی سرورها))، عوامل درون‌سازمانی (نیروهای متخصص و آموزش‌دیده، رصد و پایش)، عوامل برون‌سازمانی (همکاری با دیگر بانک‌ها و همکاری‌های بین‌المللی، سیستم عدالت کیفری، راه‌اندازی اینترنت ملی)، ثبات سیاسی، آمادگی امنیت سایبری، عدالت اجتماعی.
	فرهنگ فردی	نگرش	جَو کارکنان، پروفایل و رضایت کارکنان، باورها و افکار، دید امنیتی (در معرض قرارگرفتن)، غلبه تفکر سختگیرانه در دستگاه قضایی، فقدان شفافیت در ساختار و عملکرد حاکمیت و دولت، مسائل امنیتی، عوامل محیطی، بینش، ایدئولوژی‌ها.
		رفتار	رواج فساد در جامعه، دو ساحتی شدن جامعه، ورود ارزش‌های مدرن به جامعه، گسترش جهانی‌شدن، تهدید بنیان‌های خانواده، ارتباطات و تجربه، رفتارهای همکار (استقلال، اشتراک‌پذیری)، رفتار اخلاقی، انگیزش کارکنان، رفتار امنیت اطلاعات فردی، تغییرات سبک زندگی، جامعه‌پذیری، ناکامی‌های اجتماعی، اعتراض اجتماعی، مشارکت اجتماعی، همبستگی، یکپارچگی، نارضایتی کارکنان از فشار کاری، ناآرامی اجتماعی، گسترش طلاق، خیانت، افول بنیان خانواده (آسیب اجتماعی)
		شایستگی	تخصص داشتن، احساس تعلق به هویت ملی، امنیت اخلاقی، پایبندی به آداب‌ورسوم، دانش، شایستگی کارکنان، تأثیرات روان‌شناسی کاربر، یادگیری، توانایی‌های شناختی، تکانشگری شناختی، تشخیص و توانایی توجیه، روحیه.
	آگاهی	تعهد و حمایت	سواد رسانه‌ای، درک، موانع درک شده، خودکارآمدی امنیتی، خودآگاهی، پشتیبانی مدیریت، خودکنترلی، تعهد مدیریت عالی، ذهن‌آگاهی.

مضمون فراگیر	مضامین سازمان‌دهنده		مضامین پایه
		رعایت امنیت سایبری	استفاده از گوشی هوشمند و رعایت‌نکردن ملاحظات امنیتی، حریم خصوصی، مدیریت نامناسب اوقات فراغت، انعطاف زمانی، انتشار اخبار جعلی، کثرت اجتماعی، جنگ سایبری، حمله‌های سایبری، آشفتگی‌های سایبری، بدافزار، فیشینگ، ایمیل‌های ناشناس، نقض داده‌ها، رمز عبور، تهدید ناخواسته خودی، رسانه اجتماعی، سیستم‌های کنترل قدیمی در تأسیسات، حفاظت از خود، تروریسم سایبری، بی‌دقتی، خطای انسانی، مهندسی اجتماعی، جرم مجازی، خرابکاری فناوری اطلاعات.
		بودجه‌بندی	بودجه‌بندی برای آموزش کاربران، تخصیص منابع، سفارشی‌سازی نیازهای کارکنان و سازمان، ادغام منابع یادگیری الکترونیکی و فیزیکی

جمع‌بندی از جدول فوق‌الذکر را می‌توان در قالب شبکه مضامین در شکل (۱) ترسیم نمود.



شکل (۱): شبکه مضامین عوامل مؤثر در فرهنگ و آگاهی امنیت سایبری

مطابق یافته‌ها، عوامل مؤثر در فرهنگ امنیت سایبری در دودسته فرهنگ سازمانی و فردی تقسیم‌بندی می‌شوند. در فرهنگ سازمانی یکی از این عوامل به دارایی‌های سازمان (شامل افراد، ساختمان‌ها، ماشین‌ها، سیستم‌ها و دارایی‌های اطلاعاتی) اشاره دارد و شامل سیاست‌هایی است که چندین سطح رازداری، دردسترس‌بودن و کنترل صداقت را اعمال می‌کند. عامل دیگر، تداوم است. استمرار یا تداوم به‌منظور تضمین عملیات، خدمات و تداوم تولید برای یک سازمان در سطوح از پیش تعیین شده است، درحالی‌که از شهرت و منافع ذی‌نفعان اصلی در موارد حوادث مخرب محافظت می‌کند. دسترسی و اعتماد سومین عامل مؤثر در فرهنگ امنیت سایبری است که تمرکز بر دسترسی مناسب به منابع در سراسر سازمان را (درحالی‌که نقش‌ها و مجوزهای مختلف را روشن می‌کند) فراهم می‌آورد. علاوه بر این، هرگونه تعامل سازمان با عوامل شخص ثالث مانند تأمین‌کنندگان، مشتریان، مقامات و... را نیز محدود می‌نماید. عملیات چهارمین عامل مؤثر بوده که به مدیریت شیوه‌های تجاری برای ایجاد بالاترین سطح کارایی ممکن در داخل سازمان و درنظرگرفتن جنبه‌های امنیتی که از نتایج نهایی آن محافظت می‌کند، اشاره دارد و حفاظت که پنجمین عامل شناسایی شده می‌باشد، بر آینده‌نگری تمرکز داشته تا تمام دارایی‌های فنی لازم برای بهبود و عملکرد کارآمد امنیت سایبری را برنامه‌ریزی نموده و به‌درستی پیکربندی کند. آخرین عامل شناسایی شده، حکمرانی امنیتی است و منظور از آن اقدامات صورت‌گرفته برای برنامه‌ریزی، مدیریت و بهبود امنیت سایبری می‌باشد.

در فرهنگ فردی چهار عامل نگرش، رفتار، شایستگی و آگاهی شناسایی شد. منظور از نگرش، احساسات و اعتقادات کارکنان نسبت به پروتکل‌ها و مسائل امنیتی است. عامل رفتار، به رفتارهای آگاهانه نسبت امنیت سایبری که به‌صورت روزمره در محل کار افراد رخ می‌دهد، اشاره می‌کند. عامل شایستگی نیز مولفه‌های دخیل در ارزیابی توانایی‌ها، مهارت‌ها، دانش و تخصص کارکنان که آن‌ها را قادر می‌سازد تا با سیاست‌ها و رویه‌های امنیتی سازمان مطابقت داشته باشند، مورد بررسی قرار می‌دهد. عامل آگاهی که نقش پررنگی در امنیت سایبری دارد، مولفه‌های مربوط به درک کارکنان، دانش و آگاهی آن‌ها از مسائل و فعالیت‌های امنیتی را در قالب تعهد و حمایت، رعایت امنیت سایبری و بودجه‌بندی پوشش می‌دهد.

۴- نتیجه‌گیری

به‌دست‌آوردن درک عمیق از خطراتی که سازمان‌ها با آن روبرو هستند می‌تواند منجر به تصمیم‌گیری‌های آگاهانه در مورد پذیرش کنترل ریسک شود که می‌تواند احتمال وقوع یک تهدید سایبری را کاهش دهد یا توانایی کاهش انواع آسیب را بهبود بخشد. چنین اطلاعاتی برای نظارت بر ریسک و عملکردهای رهبری سازمان بسیار مهم است، زیرا آن‌ها برای انعطاف‌پذیری و

ریسک‌پذیری، برنامه‌ریزی می‌کنند و همچنین برای متصدیان امنیت سایبری که نیاز به درک ریسک باقی‌مانده‌ای که می‌تواند ناشی از استفاده از کنترل‌های ریسک و تغییر چشم‌انداز تهدید باشد، ضروری است [۴۱]. همچنین وجود یک برنامه رضایت‌بخش آگاهی از امنیت سایبری در این حیطه احساس می‌شود. این برنامه باید شامل آموزش کافی باشد که با اهداف سازمان همسو بوده و تمرکز بر افزایش آگاهی امنیت سایبری در حین انجام وظایف کارکنان و ارتباط تعاملی بین همه ذی‌نفعان برای هر موضوع امنیت سایبری داشته باشد. درصورتی‌که برنامه‌های آگاهی برای تغییر نگرش مردم نسبت به حوادث سایبری طراحی نشده باشند و نتوانند تأثیر مثبتی بر هر سازمانی اعمال کنند، ممکن است ناموفق باشند [۷]. در این راستا، پژوهش حاضر باهدف شناسایی عوامل مؤثر برای مضمون فراگیر "فرهنگ و آگاهی امنیت سایبری" با استفاده از تحلیل مضمون انجام شد و در نتیجه آن ۳۹۲ مضمون پایه شناسایی شد که ۱۲ مضمون سازمان‌دهنده دارایی‌ها، تداوم، دسترسی و اعتماد، عملیات، محافظت، حکمرانی امنیتی، نگرش، رفتار، شایستگی، تعهد و حمایت، رعایت امنیت سایبری و بودجه‌بندی را پوشش دادند. از ۱۲ مضمون سازمان‌دهنده، ۹ مضمون مربوط به فرهنگ امنیت سایبری و ۳ مضمون مربوط به آگاهی امنیت سایبری بوده‌اند.

قابل ذکر است که برای سنجش روایی پژوهش از شاخص نسبت روایی محتوی و شاخص روایی محتوی استفاده شد. براین‌اساس، از نظر افراد خبره در زمینه تخصصی مورد نظر (خبرگان سایبری استان اصفهان) استفاده و الگوی حاصل از این پژوهش در اختیار تعدادی از آنان قرار گرفت و نظرات آن‌ها جهت اصلاح الگو و سایر مضامین مستخرج درباره سؤال پژوهش مورد استفاده قرار گرفت. برای سنجش پایایی داده‌ها نیز از روش هولستی بهره گرفته شد. براین‌اساس، ابتدا کدگذاری با مطالعه سطر به سطر مقالات فارسی و ترجمه مقالات انگلیسی به‌صورت دستی صورت گرفت و پس از اتمام آن، کدگذاری رایانه‌ای با بهره‌گیری از نرم‌افزار MAXQDA انجام شد. سپس تعداد کدهای نگاشته شده در هر یک از این دو مرحله در قالب فرمول جای‌گذاری شد که باتوجه‌به عدد حاصل که برابر با ۰/۹۶ بود، اعتبار نتایج مقاله پیشرو، مورد تأیید قرار گرفت.

باتوجه‌به یافته‌های پژوهش، پیشنهاد می‌شود عوامل شناسایی شده در قالب یک ابزار جهت ارزیابی فرهنگ و آگاهی امنیت سایبری که عامل مهمی در وقوع جرائم سایبری است، تنظیم شود. با قراردادن این ابزار در اختیار پلیس فتای کشور و تکمیل آن توسط شاکیان پرونده‌های جرایم سایبری حوزه امور اقتصادی، آموزشی، امنیتی، اجتماعی و فرهنگی؛ می‌توان سطح فرهنگ و آگاهی افراد نسبت به امنیت سایبری را تخمین زده و بر اساس آن اقدام به ارائه راهکارهای آموزشی جهت آگاهی‌بخشی کرد تا افراد با کسب آگاهی در این زمینه کمتر در دام مجرمان سایبری قرار گیرند و در نتیجه آن امید است کاهش جرایم در این حوزه را شاهد باشیم.

۵- مراجع

[1] F. Tavakoli, M. Mortazavi, M. Keshavarz Tork M, "Determining Strategic Factors Affecting the Prevention of Cybercrime with Fuzzy Delphi Approach," Journal of Social Order (JoSS), vol. 12, no. 4, pp. 113-140, 2021. [in Persian]

[2] B. Karimzadeh, B. Pourghahramani, J. Beigi, "Designing a Native Model of Social Capital to Prevent Cybercrime," Journal of Social Order (JoSS), vol. 13, no. 2, pp. 115-148, 2021. [in Persian]

[3] K. Dadashtabar Ahmadi, M. Mahmoudbabouei, "An active cyber defense model for use in cyber deception technology," Electronic and Cyber Defense, vol. 9, no. 4, pp. 125-140, 2022. [in Persian]

[4] H. Javaheri, H. Akbari, E. Shaghaghi, "Improvement in the Ransomwares Detection Method With New API Calls Features," Electronic and Cyber Defense, vol. 8, no. 4, 107-118, 2021. [in Persian

[5] T. Mohammad, NA. Hussin, MH. Husin, "Online safety awareness and human factors: An application of the theory of human ecology," Technology in Society (techsoc). Vol. 1, no. 68, pp.1-14, 2022.

[6] A. Alzubaidi, "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia," Heliyon (heliyon). vol. 1 no. 7(1), pp. 1-13, 2021.

[7] MI. Al-Ghamdi, "Effects of knowledge of cyber security on prevention of attacks," Materials Today: Proceedings (matpr).vol. 10, 1-17, 2021.

[8] M. Ebrahimi, "A Model of Human Factors in Cyber Security," Information Manipulation and Its Impact Across All Industries, pp. 102-121. 2022.

[9] R. Sabillon, "The Cybersecurity Awareness Training Model (CATRAM)," InResearch Anthology on Advancements in Cybersecurity Education, pp. 501-520, 2022.

[10] A. Da Veiga, M. Loock, K. Renaud. "Cyber4Dev-Q: Calibrating cyber awareness in the developing country context," The Electronic Journal of Information Systems in Developing Countries (EJISDC), vol. 88, no. 1, pp. 1-21, 2022.

[11] S. Hasan, M. Ali, S. Kurnia, R. Thurasamy, "Evaluating the cyber security readiness of organizations and its influence on performance," Journal of Information Security and Applications (jisa), vol. 1, no. 58, pp. 1-27, 2021.

[12] Z. Jafari, "Cyber Security," 7th National Conference on New Ideas in Engineering, Rasht. pp. 1-12, 2022. [in Persian]

[13] KW. HOE KW, "Culture and cyber security: How cultural tightness-looseness moderates the effects of threat and coping appraisals on mobile cyber hygiene (smu)," pp. 1-245, 2021.

[14] S. Tan, P. Xie, JM. Guerrero, JC. Vasquez, Y. Li, X. Guo, "Attack detection design for dc microgrid using eigenvalue assignment approach," Energy Reports (ICPE). Vol. 1, no. 7, pp. 469-476, 2021.

[15] MA. Judge, A. Manzoor, C. Maple, JJ. Rodrigues, S. ul Islam. "Price-based demand response for household load management with interval uncertainty," Energy Reports (ICPE). vol. 1, no. 7, pp. 8493-504, 2021.

[16] I. Priyadarshini, R. Kumar, R. Sharma, PK. Singh, SC. Satapathy, "Identifying cyber insecurities in trustworthy space and energy sector for smart grids," Computers & Electrical Engineering (compeleceng). vol. 1, no. 93, pp. 1-20, 2021.

[17] M. Amir, T. Givargis, "Pareto optimal design space exploration of cyber-physical systems," Internet of things (IOT). vol. 1, no. 12, pp. 1-32, 2020.

[18] N. Li, C. Tsigkanos, Z. Jin, Z. Hu, C. Ghezzi. "Early validation of cyber–physical space systems via multi-concerns integration," Journal of Systems and Software (jss). vol. 1, no. 170, pp. 1-18, 2020.

[19] A. Georgiadou, S. Mouzakitis, D. Askounis, "Designing a cyber-security culture assessment survey targeting critical infrastructures during covid-19 crisis," International Journal of Network Security & Its Applications (IJNSA), vol. 1, pp. 1-13, 2021.

[20] L. Cardoso, M. Castanho. "A Cyberculture Study: K-Pop And The New Media-Bts And Twitter," European Journal of Social Sciences Studies (SSS). vol. 9, no. 6(6), pp. 1-23, 2021.

[21] MR. Tarkhan, V. Fatouhabadi, "Presenting a Conceptual Model Based on Situational Awareness Aimed at Improving Cyber Security," Second International Conference on New Research Findings in Electrical Engineering and Computer Science, Ramsar, 2017. [in Persian]

[22] AJ. Rashidi, M. Shakibazad, "Presenting a Framework for Achieving Dynamic Cyber Situation Awareness on the Cyber Battle Scene," Fourth International Conference on Electrical and Computer Engineering, Tehran, 2017. [in Persian]

[23] A. Rasooli. "The concept of cyber attacks and strategies to deal with it," the Second National Conference on Cyber Defense, Maragheh, 2020. [in Persian]

[24] A. Khalilipor Roknabadi, Y. Nooralivand, "Cyber threats and national security," Strategic Studies Quarterly, vol. 15, no. 56, pp. 167-196, 2012. [in Persian]

[25] MR. Movahedirad, N. Modiri, "Presenting a Structured Approach to Implementing Cyber Exercises," The First National Conference on Computer Engineering Research, Tehran, 2015. [in Persian]

[26] B. Uchendu, JR. Nurse, M. Bada, S. Furnell. "Developing a cyber security culture: Current practices and future needs," Computers & Security (cose). vol. 1, no. 109, pp. 1-29, 2021.

[27] D. Papatsaroucha, Y. Nikoloudakis, I. Kefaloukos, E. Pallis, EK. Markakis, "A Survey on Human and Personality Vulnerability Assessment in Cyber-security: Challenges, Approaches, and Open Issues," arXiv preprint arXiv:2106.09986 (cs.CR). 2021.

[28] A. Safaei, M. Ghadiri, "Impacts of Covid-19 epidemic in the field of cyber security," 7th IRGC National Conference on Defense Science and Engineering, Tehran, 2021. [in Persian]

[29] H. Kaviani, N. Mirsepasi, G. Me'marzadeh Tehran, "A Pattern for Strategic Development of Human Resources in the Field of Cyber Security of the Armed Forces of Islamic Republic of Iran," Defence Studies, vol. 18, no. 1, pp. 37-66, 2020. [in Persian]

[30] NA. Azmi, AP. Teoh, A. Vafaei-Zadeh, H. Hanifah, "Predicting information security culture among employees of telecommunication companies in an emerging market," Information & Computer Security. pp. 1-11, 2021

[31] A. Georgiadou, S. Mouzakitis, D. Askounis, "Detecting Insider Threat via a Cyber-Security Culture Framework," Journal of Computer Information Systems (CIS). vol. 26, pp. 1-10, 2021.

[32] EI. Collins, J. Hinds, "Exploring Workers' Subjective Experiences of Habit Formation in Cybersecurity: A Qualitative Survey," Cyberpsychology, Behavior, and Social Networking (CBSN). vol. 1, no. 24(9), pp. 599-604, 2021.

[33] M. Rajabi, H. Rajabi, M. Ahmadabadi, "The Theme Analysis of the Requirements for the Realization of the Disciplinary Security in the Thought of the Supreme Commander of All Armed Forces," Journal of Social Order (JoSS), vol. 10, no. 2, pp. 85-108, 2018. [in Persian]

[34] S. Sharifi Rahnmo, A. Fathi, E. Emrani, M. Sharifi Rahnmo, B. Zare kohan, M. Ebrahimi, "Forecasting Components of Youth Cultural Security based on the Degree of Attachment to Cyberspace," Societal Security Studies (SSS), vol. 12, no. 65, 69-88, 2021. [in Persian]

[35] S. Razavi, J. Sadehmiri, "Influential components in raising the level of awareness and intelligence of NAJA personnel against the threats and injuries of soft war based on the intellectual system of Imam Khamenei, the Supreme Leader," Police Protectoral and Security Studies quarterly (SPAPS), vol. 15, no. 55, pp. 43-77, 2020. [in Persian]

[36] Farashi A., Estarky A., Abiri D. "The role of preventive actions in protecting the organization's cyber missions," Police Protectoral and Security Studies quarterly (SPAPS), vol. 15, no. 55, pp. 129-160, 2020. [in Persian]

[37] H. Sayyadi Tooranloo, S. Mirghafoori, M. Mahdavi, S. Saghafi, "Analysis of factors related to the establishment of Cybercrime using a Fuzzy approach," Quarterly of Order & Security Guards (OSRA), vol. 13, no. 3, pp. 27-54, 2020. [in Persian]

[38] R. Zakeri Hamane, M. Azam Azade M. , GHaziNejad, S. Bastani, "Qualitative Study of Users' Sense of Online Security in Social Networks," New Media Studies (NMS), vol. 6, no. 21, pp. 141-178, 2020. [in Persian]

[39] M. Sahraei, M. Valavi, B. Bayat, A. Taraghi, "Provide a native model of cyber monitoring, monitoring and alerting based on the ooda cycle," National Security (NS), vol. 10, no. 37, pp. 473-512, 2020. [in Persian]

[40] A. Ferasati, S. Rah peyk, "Investigating the Impact of Preventive Components on Controlling and Reducing the Crimes of Armed Forces Payers," National Security (NS), vol. 10, no. 35, pp. 291-326, 2020. [in Persian]

[41] SA. Samouti, M. Azizipour, Field study of cyber threats in the human resources layer and the importance of cyber security awareness, Second National Conference on Cyber Defense, Maragheh, 2020. [in Persian]

[42] MR. Eivazi, MM. Dadashi Chakan, "Types of threats in cyberspace and strategies to deal with it," Second National Conference on Cyber Defense, Maragheh, 2020. [in Persian]

[43] A. Erola, I. Agrafiotis, JR. Nurse, L. Axon, M. Goldsmith, S. Creese. "A system to calculate cyber-value-at-risk," Computers & Security (COSE). vol. 1, no. 113, pp. 102-124, 2022.

[44] TA. Nguyen., K. Koblandin, S. Suleymanova, V. Volokh, "Effects of 'Digital'Country's Information Security on Political Stability," Journal of Cyber Security and Mobility (CSM). Vol. 1, pp. 29-52, 2022.

[45] AG. Adamu, MM. Siraj, SH. Othman, "An assessment of cybersecurity awareness level among Northeastern University students in Nigeria," International Journal of Electrical and Computer Engineering (ECE). vol. 1, no. 12(1), pp. 572-589, 2022.

[46] B. Iser, R. Brandtweiner, "Role of Awareness to Prevent Personal Disasters: Reducing the Risks of Falling for Phishing by Strengthening User Awareness," Wit Transactions on The Built Environment (WIT).vol. 207, pp. 79-88, 2022.

[47] MD. Richardson, PA. Lemoine, WE. Stephens, RE. Waller, "Planning for Cyber Security in Schools: The Human Factor," Educational Planning (ERIC). vol. 27, no. 2, pp. 23-39, 2020.

[48] [48] M. Grobler, R. Gaire, S. Nepal. "User, usage and usability: Redefining human centric cyber security," Frontiers in big Data (fData). Vol. 5, pp. 1-12, 2021.

[49] K. Khando, S. Gao, SM. Islam, A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," Computers & Security (COSE). vol. 106, pp. 1-17, 2021.

[50] A. Georgiadou, S. Mouzakitis, D. Askounis, "Working from home during COVID-19 crisis: a cyber security culture assessment survey," Security Journal (SJ). vol. 26, pp. 1-20, 2021.

[51] JR. Nurse, "Cybersecurity Awareness," arXiv preprint arXiv (arXiv):2103.00474. 2021.

[52] F. Quayyum, DS. Cruzes, L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," International Journal of Child-Computer Interaction (jcci). vol. 30, pp. 1-14, 2021.

[53] K. Matyokurehwa, N. Rudhumbu, C. Gombiro, C. Mlambo, "Cybersecurity awareness in Zimbabwean universities: Perspectives from the students," Security and Privacy (SPY). vol. 4, no. 2, pp. e141, 2021.

[54] JV. Bino, "Cyber Security Awareness By Using Social Media Platforms Among Students," International Journal of Research (IJR), vol. 8, no. 5, pp. 581-589, 2021.

[55] AI. Al-Alawi, SA. Al-Bassam, "Assessing The Factors of Cybersecurity Awareness in the Banking Sector" AGJSR, vol. 37, no. 4, pp. 17-32, 2021.

[56] AG. Buja, SD. Wahid, TF. Rahman, NA. Deraman, MN. Jono, AA. Aziz, "Development of organization, social and individual cyber security awareness model (OSICSAM) for the elderly," International Journal of Advanced Technology and Engineering Exploration (IJATEE). vol. 8, no. 76, pp. 511-532, 2021.

[57] A. Georgiadou, S. Mouzakitis, D. Askounis, "Assessing mitre att&ck risk using a cyber-security culture framework," Sensors. Vol. 21, no. 9, pp. 1-14, 2021.

[58] I. Progoulakis, N. Nikitakos, P. Rohmeyer, B. Bunin, D. Dalaklis, S. Karamperidis, "Perspectives on Cyber Security for Offshore Oil and Gas Assets," Journal of Marine Science and Engineering (jmse). vol. 9, no. 2, pp. 112-125, 2021.

[59] MI. Alghamdi, "Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia," Materials Today: Proceedings (matpr). Vol. 1, 1-12, 2021.

[60] PR. Trim, YI. Lee, "The global cyber security model: counteracting cyber attacks through a resilient partnership arrangement," Big Data and Cognitive Computing (bdcc). vol. 5, no. 3, 32-45, 2021.

[61] VK. Viraja, P. Purandare, "A Qualitative Research on the Impact and Challenges of Cybercrimes," InJournal of Physics: Conference Series, vol. 1964, no. 4, pp. 1-18, 2021.

[62] BK. Mamade, DM. Dabala, "Exploring The Correlation between Cyber Security Awareness, Protection Measures and the State of Victimhood: The Case Study of Ambo University's Academic Staffs," Journal of Cyber Security and Mobility (csm). vol. 1, pp. 699-724, 2021.

[63] PT. Mai, A. Tick, "Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam," Acta Polytech. Hung (APH). vol. 18, pp. 67-89, 2021.

[64] A. H. Khan, P. B. Sawhney, S. Das, D. Pandey, "SartCyber Security Awareness Measurement Model (APAT)," International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), IEEE, pp. 298-302, 2020.

Cybersecurity in the Use of Social Media: An Initial Study," Information Systems Education Journal (isedj), vol. 18, no. 1, pp. 48-58, 2020.

[77] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," Computers & Security (cose), vol. 1, no. 98, pp. 1-26, 2020.

[78] AU. Walden, "Creating cybersecurity awareness," Strategic Finance. pp.1-24, 2020.

[79] G. Abebe, L. Lessa. "Human Factors Influence in Information Systems Security: Towards a Conceptual Framework," Proceedings of the 2nd African International Conference on Industrial Engineering and Operations Management Harare (IEOM), pp. 1-18, 2020

[80] I. Al-Shanfari, W. Yassin, R. Abdullah, "Identify of factors affecting information security awareness and weight analysis Process," International Journal of Engineering and Advanced Technology (IJEAT), vol. 9, no. 3, pp. 534-42, 2020.

[81] I. Legárd, "Building an effective information security awareness program," Central and Eastern European eDem and eGov Days (ocg), Vol. 15, no. 338, pp. 189-200, 2020.

[82] KL. Bethel, "An Evaluation of Organizational Culture: Its Influence on Security Culture: A Case Study (Doctoral dissertation, Northcentral University)," vol. 1, pp. 1-345, 2020,

[83] R. AlMindeel, JT. Martins. "Information security awareness in a developing country context: insights from the government sector in Saudi Arabia," Information Technology & People (ITP). Vol. 6, pp. 1-17, 2020.

[84] W. Aljohani, N. Elfadil, "Measuring Cyber Security Awareness of Students: A Case Study at Fahad Bin Sultan University," International Journal of Computer Science and Mobile Computing (IJCSMC). vol. 9, no. 6, pp. 141-155, 2020.

[85] N. Tosun, M. Altinöz, E. Çay, T. Çinkiliç, S. Gülseçen, T. Yildirim, MA. Aydin, B. Metin, ZA. Reis, N. Ünlü, "A swot analysis to raise awareness about cyber security and proper use of social media: Istanbul sample," International Journal of Curriculum and Instruction (ijci). vol. 14, no. 12, pp. 271-94, 2020.

[86] P. Pavlova, "Enhancing the Organisational Culture related to Cyber Security during the University Digital Transformation," Information & Security (isij). vol. 46, no. 3, pp. 239-49, 2020.

[65] OS. Ahmed, "Teacher's awareness to develop student cyber security: A Case Study," Turkish Journal of Computer and Mathematics Education (TURCOMAT). vol. 12, no. 10, pp. 5148-156, 2021.

[66] Š. Orehek, G. Petrič, "A systematic review of scales for measuring information security culture," Information & Computer Security. vol. 1, pp. 1-10, 2020.

[67] S. Furnell, E. Collins, "Cyber security: what are we talking about?" Computer Fraud & Security (CFSe). vol. 7, pp. 6-11, 2021.

[68] A. Garba, MB. Sirat, S. Hajar, IB. Dauda, "Cyber security awareness among university students: A case study," Science Proceedings Series (SPS). vol. 2, no. 1, pp. 82-86, 2020.

[69] M. Butavicius, K. Parsons, M. Lillie, A. McCormac, M. Pattinson, D. Calic, "When believing in technology leads to poor cyber security: Development of a trust in technical controls scale," Computers & Security (cose). vol. 1, pp. 98-112, 2020.

[70] S. Enescu. "A Comparative Study on European Cyber Security Strategies," Redefining Community in Intercultural Context (RCIC). vol. 9, no. 1, pp. 277-82, 2020.

[71] J. Sebastian, P. Sakthivel, "Cyber Terrorism: A Potential Threat To Global Security," Pearsonjournal (PJ), vol. 6, no. 6, pp. 334-341, 2020.

[72] A. Wiley, A. McCormac, D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," Computers & Security (cose). vol. 1, no. 88, pp. 1-16, 2020.

[73] A. Kovačević, SD. Radenković, "SAWIT—security awareness improvement tool in the workplace," Applied Sciences (app). vol, 10, no. 9, pp. 30-65, 2020.

[74] G. Hatzivasilis, S. Ioannidis, M. Smyrlis, G. Spanoudakis, F. Frati, L. Goeke, T. Hildebrandt, G. Tsakirakis, F. Oikonomou, G. Leftheriotis, H. Koshutanski, "Modern aspects of cyber-security training and continuous adaptation of Programmes to trainees," Applied Sciences (app). vol. 10, no. 16, pp. 1-30, 2020.

[75] LV. Astakhova, "Issues of the culture of information security under the conditions of the digital economy," Scientific and Technical Information Processing (STIP). vol. 47, no. 1, pp. 56-64, 2020.

[76] N. Bhatnagar, M. Pry, "Student Attitudes, Awareness, and Perceptions of Personal Privacy and