



Improving the Behavioral Pattern of Information Security Experts in the Face of Emerging Cyber Threats with a Future Research Approach

Sedigheh Mohammad E-smaeil^{1*} | Mohammad Bagher Raen Abromand² |
Dariush Matlabi³

1. Associate Professor, Department of Information Science and Epistemology, Research Sciences Unit, Islamic Azad University, Tehran, Iran. (Corresponding Author) sm.esmaeili2@gmail.com

2. Ph.D. student in Information Science and Epistemology, Islamic Azad University Research Science Unit, Tehran, Iran. itmanager@tsfc.ir

3. Associate Professor, Department of Educational Sciences, Yadgar Imam Khomeini (RA) Shahrari Unit, Islamic Azad University, Tehran, Iran. dariushmatlabi@yahoo.com

Article Info	ABSTRACT
Article type: Research Article	Objective: Most of the research conducted in the field of information systems security has been focused on technical factors, but information security solutions in the face of cyber threats should be explained in a comprehensive and forward-looking manner so that they have the necessary efficiency against emerging threats. The current applied-developmental research, with a future research approach, after examining the indicators, deals with the improvement of the correct behavior pattern of information security experts in the face of emerging cyber threats.
Article history:	
Received: 10-12-2022	
Received in revised form: 14-01-2023	
Accepted: 09-02-2023	Methodology: First, in the qualitative phase, meta-composite method was used to extract indicators from research sources and questions, and in the quantitative phase, with the help of experts and the two-stage Delphi method, the indicators were validated, refined and clustered. After statistical analysis and confirmatory factor analysis, it was examined and with the help of second and third order factorial software, the components and indices of each dimension were obtained.
Published online: 19-06-2023	Results: 142 indicators were extracted from 112 sources and validated and refined with the help of experts. In the first and second stage of Delphi, 17 indicators were removed due to the low CVR/CVI and finally 125 indicators were finalized and with the help of software and class clustering, the dimensions and components of the research were explained. Then, in the survey stage, after receiving 111 responses from information security experts and checking their reliability, the appropriate behavioral pattern for the research was calculated.
Keywords: Behavioral Pattern, Information Security, Cyber Threats, Futurism, Hyper Combination	Conclusion: Based on the weight of the dimensions and components of the research, the "security threats" dimension of the "unintentional damages" component had the highest weight and the "technical factors" dimension of the "planning" and "monitoring" component had the lowest weight.

Cite this article: Mohammad E-smaeil, S., Raen Abromand, M. B., Matlabi, D. (2023). Improving the Behavioral Pattern of Information Security Experts in the Face of Emerging Cyber Threats with a Future Research Approach. *Journal of Knowledge Studies*, 16(61), 101-124.





بهبود الگوی رفتاری کارشناسان امنیت اطلاعات در مواجهه با تهدیدات سایبری با رویکرد آینده پژوهی

صدیقه محمد اسماعیل^{۱*} | محمد باقر رایین آبرومند^۲ | داریوش مطلبی^۳

۱. دانشیار گروه علم اطلاعات و دانش‌شناسی، واحد علوم تحقیقات دانشگاه آزاد اسلامی، تهران. (نویسنده مسئول) m.esmaeili2@gmail.com

۲. دانشجوی دکتری تخصصی علم اطلاعات و دانش‌شناسی، واحد علوم تحقیقات دانشگاه آزاد اسلامی، تهران، ایران. ITmanager@tsfc.ir

۳. دانشیار گروه علوم تربیتی، واحد یادگار امام خمینی (ره) شهرری، دانشگاه آزاد اسلامی، تهران، ایران. dariushmatlabi@yahoo.com

اطلاعات مقاله	چکیده
نوع مقاله: مقاله پژوهشی	هدف: بیشتر تحقیقاتی که در زمینه امنیت سیستم‌های اطلاعاتی صورت گرفته، بر عوامل فنی پرداخته شده، ولی راه کارهای امنیت اطلاعات در مواجهه با تهدیدات سایبری باید به گونه‌ای جامع و آینده‌نگرانه تبیین شود تا در مقابل تهدیدات نوظهور نیز کارایی لازم را داشته باشند. پژوهش کاربردی-توسعه‌ای حاضر با رویکرد آینده‌پژوهی پس از بررسی شاخص‌ها، به بهبود الگوی رفتاری و صحیح کارشناسان امنیت اطلاعات در مواجهه با تهدیدات سایبری نوظهور می‌پردازد.
تاریخ دریافت: ۱۴۰۲/۵/۲۲	روش پژوهش: ابتدا در مرحله کیفی از روش فزاینده، جهت استخراج شاخص‌ها از منابع و سؤال‌های پژوهش استفاده شد و در مرحله کمی با کمک خبرگان و روش دلفی دو مرحله‌ای، شاخص‌ها اعتبارسنجی، پالایش و خوشه بندی شد، در مرحله پیمایشی پاسخ پرسشنامه‌ها پس از تجزیه و تحلیل آماری و تحلیل عاملی تأییدی، مورد بررسی قرار گرفت و با کمک نرم افزار بار عاملی مرتبه دوم و سوم هر بعد، مؤلفه‌ها و شاخص‌ها، به دست آمد.
تاریخ بازنگری: ۱۴۰۲/۷/۱۸	یافته‌ها: از ۱۱۲ منبع، ۱۴۲ شاخص استخراج و با کمک خبرگان اعتبارسنجی و پالایش شد. در مرحله اول و دوم دلفی ۱۷ شاخص به دلیل پایین بودن CVR/CVI حذف و در نهایت ۱۲۵ شاخص نهایی گردید و به کمک نرم افزار و خوشه بندی طبقه‌ای، ابعاد و مؤلفه پژوهش تبیین شد. سپس در مرحله پیمایشی، پس از دریافت ۱۱۱ پاسخنامه از سوی کارشناسان امنیت اطلاعات و بررسی پایایی آنها، الگوی رفتاری مناسب پژوهش احصاء گردید.
تاریخ پذیرش: ۱۴۰۲/۹/۱۰	نتیجه‌گیری: براساس وزن بعدها و مؤلفه‌های پژوهش، بعد «تهدیدات امنیتی» مؤلفه «خسارت‌های غیر عمدی» بیشترین وزن و بعد «عوامل فنی» مؤلفه «برنامه ریزی» و «پایش» کمترین وزن را داشته‌اند.
تاریخ انتشار آنلاین: ۱۴۰۳/۷/۸	
واژه‌های کلیدی: الگوی رفتاری، امنیت اطلاعات، تهدیدات سایبری، آینده پژوهی، فزاینده	

استناد: محمد اسماعیل، ص، رایین آبرومند، م، مطلبی، د. (۱۴۰۲). بهبود الگوی رفتاری کارشناسان امنیت اطلاعات در مواجهه با تهدیدات سایبری با رویکرد

آینده پژوهی. دانش‌شناسی، ۱۶ (۶۱)، ۱۲۴-۱۰۱.



حق مؤلف © نویسنده‌گان.

ناشر: دانشگاه آزاد اسلامی واحد تهران شمال

مقدمه

دنیای صنعتی به سمت پارادایم صنعتی اینترنت اشیا می‌رود که به اینترنت صنعتی نیز معروف است و شامل تعداد فزاینده‌ای از سیستم‌های فیزیکی است که با هدف افزایش کارایی و اثربخشی فرایندهای تجاری به اینترنت متصل می‌شوند (پیتو و همکاران^۱، ۲۰۲۱) و قابلیت اطمینان آن بسیار حائز اهمیت است. این پارادایم مبتنی بر استفاده از فناوری‌های توانمندکننده ویژه است. با توجه به اهمیت دیتا در دنیای جدید، لزوم داده کاوی و پردازش داده، حفاظت از داده را لازم و ملزوم دنیای داده پردازی پیشرو کرده است. طبق مطالعات آزمایشگاه کسپرسکی^۲، ۵۲ درصد از شرکت‌ها گزارش می‌دهند که کارکنان مهم ترین ضعف را از نظر امنیت سایبری تشکیل می‌دهند. مطابق با این بیانیه، گزارش سالانه وریزون^۳ درمورد نقض داده‌ها ادعا می‌کند که ۸۵٪ از چنین نقض‌هایی شامل یک عنصر انسانی است. اگرچه نقض داده‌های ناشی از تلاش‌های مخرب گران‌تر است، نقض داده‌های ناشی از سیستم یا خطای انسانی همچنان هزینه قابل توجهی با ارزش متوسط ۲/۷۴ میلیون یورو دارد. در میان بردارهای کاهش حملات و حوادث مرتبط با داده، به اهمیت تعریف یک طرح آگاهی از امنیت سایبری اشاره می‌کند که شامل ارائه آموزش به کارکنان و استفاده از سناریوهای شبیه سازی برای شناسایی کمپین‌های مهندسی اجتماعی و فیشینگ است (کورالو^۴، ۲۰۲۲). کارکنان می‌توانند مهارت‌های امنیت سایبری لازم برای مدیریت مؤثر و پاسخ‌گویی به تهدیدات و خطرات امنیت سایبری را کسب کنند. به این ترتیب، کارکنان می‌توانند درک درستی از تهدیدات و خطرات امنیت سایبری که شرکت‌ها با آن مواجه هستند به دست آورند و در مدیریت وظایف امنیت سایبری اعتماد به نفس بیشتری پیدا کنند (لی و همکاران^۵، ۲۰۱۹). تحلیل دیتا و داده کاوی در عصر فناوری کمک شایانی به مدیریت مؤثر و پاسخ‌گویی به تهدیدات و مخاطرات در حوزه سایبری کرده است. به طور کلی داده کاوی را می‌توان به عنوان مجموعه‌ای از مکانیسم‌ها و تکنیک‌ها تعریف کرد که برای استخراج اطلاعات پنهان از داده‌ها تحقق می‌یابد و برای این منظور از نرم افزارهایی مانند SPSS، MATLAB و RapidMiner استفاده می‌شود، همچنین تکنیک‌های داده-کاوی را می‌توان برای تجزیه و تحلیل روی داده‌های ساخت یافته، غیرساخت یافته اعمال کرد. باید توجه داشت که الگوها از تجزیه تحلیلی که بر روی داده‌ها صورت می‌گیرد به دست می‌آیند، (وو و یانگ^۶، ۲۰۲۳) و آینده پژوهی مجموعه تلاش‌هایی است که با نگاهی به آینده بر منابع، الگوها و روند حال و گذشته می‌پردازد. در آینده پژوهی به چندین آینده محتمل می‌اندیشیم تا روند امروز را متناسب با آینده احتمالی تصحیح کنیم. اصل اساسی در آینده پژوهی، غافلگیر نشدن و آماده شدن برای هر آینده محتمل است (بنگستون^۷، ۲۰۱۸). جیم دیتور^۸، یکی از آینده پژوهان غربی آینده را حاصل برهم کنش چهار عامل می‌داند: رویدادها، روندها، تصویرها و اقدام‌ها. با نگاهی به پیشینه‌ها، استفاده از عبارت «درصد بالایی» در پژوهش، دی پیر تصدیق کننده این موضوع است که زیرساخت و فناوری به تنهایی نمی‌تواند تضمین کننده امنیت اطلاعات باشد و در نهایت به نیروی انسانی آموزش دیده نیاز است. اتصال و تبادل داده‌ها با دیگر دستگاه‌ها و سیستم‌ها از طریق اینترنت، امنیت اطلاعات را در معرض خطرات روبه‌رشد قرار می‌دهد. طی مطالعات انجام شده شیائوفن^۹ (۲۰۲۲) در زمینه رفتار متخصصین امنیت اطلاعات در کشور چین، با استفاده از ۸۰۴ پرسش نامه و تحلیل عاملی و نتایج حاصله نشان می‌دهد که «نگرش‌های امنیت اطلاعات و هنجارهای ذهنی، به طور قابل توجهی بر رفتارهای حفاظتی کارشناسان امنیت اطلاعات تأثیر می‌گذارد، ارزیابی‌های مقابله‌ای و خودکارآمدی به طور قابل توجهی پیش‌بینی کننده رفتارهای حفاظتی کارشناسان امنیت اطلاعات است.» قطعاً آموزش، بازآموزی و آگاه‌سازی نقش بسزایی در ارتقای نگرش‌های امنیت اطلاعاتی و هنجارهای ذهنی کارشناسان امنیت اطلاعات دارد، همان

1. Pivoto

2. Kaspersky

3. Verizon

4. Corallo

5. Li

6. Wu, & Yang

7. Bengston

8. Jim Dator

9. Xiaofen

گونه که موتی زویلینگ^۱ (۲۰۲۲) در پژوهش خود به این موضوع پرداخته است، حملات سایبری نشان دهنده یک تهدید بالقوه برای امنیت اطلاعات است. با افزایش نرخ استفاده از داده‌ها و مصرف اینترنت، آگاهی سایبری به یک مسئله حیاتی تبدیل شده است. در مطالعه انجام شده، بر روابط بین آگاهی امنیت سایبری، دانش و رفتار با ابزارهای حفاظتی در میان افراد سه کشور اسلوانی، لهستان و ترکیه به طور ویژه متمرکز است. نتایج مطالعات نشان می‌دهد که کاربران اینترنت دارای آگاهی کافی از تهدید سایبری هستند؛ اما به طور معمول حداقل اقدامات حفاظتی به نسبت رایج و ساده را اعمال می‌کنند. یافته‌های مطالعه همچنین نشان می‌دهد که مستقل از جنسیت و کشور، دانش سایبری بالاتر به سطح آگاهی سایبری مرتبط است؛ ولی مطالعات انجام شده، نشان می‌دهد، از نظر تعامل بین آگاهی، دانش، و رفتارها، تفاوت‌هایی بین کشورهای کاوش شده وجود داشته است. کمائی (۲۰۲۲) در پژوهش خود توصیف می‌کند که چگونه آگاهی از امنیت سایبری می‌تواند کاهش حملات فیشینگ را تضمین کند و اثربخشی آموزش آگاهی از امنیت سایبری مبتنی بر هوش مصنوعی و چگونگی تأثیر آن بر حملات سایبری را به نمایش می‌گذارد. آموزش و آگاهی امنیتی نقشی پویا برای سازمان‌ها در تأیید دسترسی به منابع دارد. در پژوهش ببو^۲ (۲۰۲۲)، میت آموزش و آگاهی امنیتی در مقابله با تهدیدات سایبری بررسی شده است و اثربخشی برنامه‌های آموزشی آگاهی امنیتی را بر رفتار کارکنان به صورت کیفی مورد بررسی قرار داده و نشان می‌دهد، رفتار کارکنان در معرض خطر حملات سایبری و اجرای آموزش و آگاه‌سازی در زمینه امنیت اطلاعات، رابطه معنی داری با هم دارند. اهمیت حفاظت از منابع اطلاعاتی سازمان‌ها از جنبه‌های اقتصادی و سیاسی و استراتژیک دارای اهمیت فوق العاده و بعضاً حیاتی است. بدیهی است که انتشار یا سوءاستفاده از چنین اطلاعاتی، نه تنها از نظر اقتصادی زیان‌بار خواهد بود، بلکه تبعات منفی سیاسی و اجتماعی وسیعی برای کشور به همراه خواهد داشت؛ و با عنایت به این ویژگی‌ها امن‌سازی سرمایه‌های درون سازمان‌ها اعم از داده‌ها، اطلاعات و منابع سخت‌افزاری و نرم‌افزاری و فضای تبادل اطلاعات الکترونیکی باید مورد اهتمام جدی قرار بگیرد؛ و نیز با نگاهی به سند راهبردی امنیت فضای تبادل اطلاعات کشور و به استناد به بند ج ماده ۴۴ قانون برنامه چهارم و پنجم توسعه اقتصادی، اجتماعی، فرهنگی و علمی کشور پرداختن به امنیت تبادل اطلاعات به عنوان یک ضرورت و اولویت تلقی شده است. به اذعان متخصصان حوزه اقتصاد و مدیریت داشتن نیروی انسانی باکیفیت یکی از مهم‌ترین رموز بقای، سازمان‌ها در هزاره سوم است. دانشمندان و صاحب نظران معتقدند که کارکنان در حفظ امنیت اطلاعات سازمان‌ها، نقش کلیدی ایفا می‌کنند؛ لذا یکی از مهم‌ترین حوزه‌ها در بحث سیستم مدیریت امنیت اطلاعات، مدیریت بر منابع انسانی است و ساده‌ترین و مؤثرترین راه مقابله با تهدیدات امنیت اطلاعات آموزش‌های تخصصی کارکنان می‌باشد؛ که در واقع بدون آموزش و آشنایی کلیه کاربران رایانه و شبکه دسترسی به این هدف امکان‌پذیر نمی‌باشد. با مرور اجمالی بر مطالعات انجام شده در زمینه مدیریت سیستم‌های امنیت اطلاعات و نتایج تحقیقات در این رابطه حاکی از این است که انجام ارزیابی مؤلفه‌های آن به هیچ وجه امر ساده‌ای نیست در پژوهش علی جعفری سعی شده که نقش تأثیر آموزش‌های تخصصی عوامل انسانی بر پیاده‌سازی سیستم مدیریت امنیت اطلاعات سازمان را مورد بررسی قرار دهد (جعفری ۱۳۹۴). تحقیقات نشان دهنده آن است که آموزش و آگاه‌سازی، نقش بسزایی در امنیت و حفاظت اطلاعات دارد با این وجود، شعبانی (۱۴۰۰) در نتایج پژوهش خود به این طبقه‌بندی دست یافته است که «فرهنگ سازمانی با رتبه میانگین ۱۶/۲۶ رتبه اول، «ساختار سازمانی» با رتبه میانگین ۱۳ رتبه دوم، «منابع انسانی» با رتبه میانگین ۱۲/۱۱ رتبه سوم، «زیرساخت فناوری اطلاعات» با رتبه میانگین ۱۱/۶۳ رتبه چهارم، «آموزش و بازآموزی» با رتبه میانگین ۱۰/۹۸ رتبه پنجم و «جنبه راهبردی و رهبری» با رتبه میانگین ۹/۴۸ در رتبه ششم قرار دارد، در صورتی که سایر پژوهش‌ها وزن بالاتری به آموزش و آگاه‌سازی داده‌اند ولی با توجه به اینکه نظر مدیران و کاربران ملاک وزن دهی و رتبه بندی بوده و در همین پژوهش هم «فرهنگ سازمانی» که تبیین کننده خط فکری مدیران و کاربران است، بالاترین وزن و رتبه را دارد و لازم و ملزوم بودن فرهنگ سازمانی و آموزش (سوگیونو^۳، افندی^۴، و آفرینا^۵ ۲۰۲۱) نشان دهنده اهمیت آموزش و آگاه‌سازی است.

1. Moti Zwillling

2. Bibhu

3. Sugiono

4. Efendi

5. Afrin

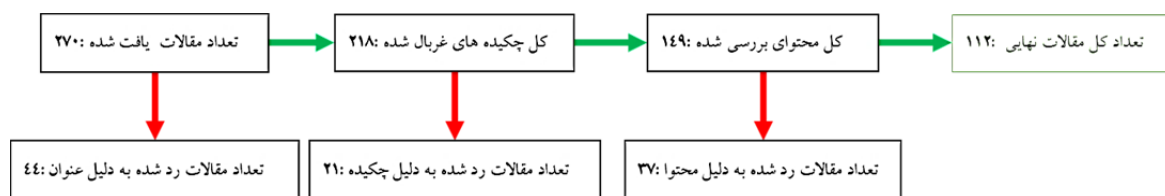
امروزه به نظر می‌رسد، موفقیت امنیت اطلاعات تا حد زیادی به رفتار اثربخش کاربران وابسته است. رفتارهای درست و سازنده کاربران، مدیران سیستم و افراد دیگر می‌تواند اثربخشی امنیت اطلاعات را تا حد زیادی بالا ببرد؛ درحالی که رفتارهای نادرست و مخرب، در حقیقت می‌تواند مانع اثربخشی آن شود. باتوجه به اینکه، پیچیدگی‌های عوامل انسانی بر دسترس بودن، قابلیت اعتماد، و تمامیت سیستم‌های اطلاعاتی مؤثر است (حسندوست، ۱۴۰۲). باتوجه به نبود یا کمبود عمومی پژوهش در این زمینه و نظر به اهمیت امنیت اطلاعات برای سازمان‌های امروزی و اثر مستقیم مدیریت عوامل انسانی بر امنیت اطلاعات سازمان پژوهش حاضر بر آن بوده است که رویکرد متفاوتی را به امنیت اطلاعات با تمرکز بر "امنیت اطلاعات رفتاری، متخصصان و مدیران" ارائه نماید و با شناسایی و بررسی عوامل آشکار و پنهان مؤثر بر امنیت اطلاعات در سازمان‌ها، یک الگوی رفتار حرفه‌ای صحیح برای کارشناسان امنیت اطلاعات در مواجهه با تهدیدات سایبری با ارزیابی‌های کمی و کیفی ارائه نماید. در خصوص ضرورت و اهمیت پیاده‌سازی الگوی رفتاری در پژوهش حاضر می‌توان به سند راهبردی امنیت اطلاعات کشور اشاره نمود که در آن پیاده‌سازی سیستم مدیریت امنیت اطلاعات به عنوان یکی از اقدامات اساسی برای راهبردهای ایمن‌سازی زیرساخت‌های حیاتی کشور در قبال حملات الکترونیکی، ایجاد و توسعه نظام‌های فنی فرابخشی افتا^۱ در نظر گرفته شده است که اجرای آن باید توسط تمام سازمان‌های دولتی مدنظر قرار گیرد (سازمان فناوری اطلاعات ایران، ۱۴۰۰). ایجاد اعتماد در مشتریان و ارباب‌رجوع، ایجاد شفافیت، قابلیت پیگیری و حساسی، کاهش ریسک‌های فنی، مالی، حقوقی و قضایی امنیت فضای تبادل اطلاعات، جلوگیری از حملات و دسترسی‌های غیرمجاز ناشی از عدم رعایت مسائل امنیتی، مهار خسارت‌های ناشی از ناامنی، تأمین محرمانگی، صحت و قابلیت دسترسی برای ارتباطات، اطلاعات، نرم افزارها و سخت افزارها همگی از مزایای پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) به شمار می‌روند و سازمان‌ها را بر آن می‌دارند تا اقدام به ایجاد این سیستم نمایند (ایلداریم^۲، ۲۰۲۱). افزون بر این در باب اهمیت انجام پژوهش می‌توان به آگاه‌سازی، تعلیم و آموزش مستمر و مناسب کارشناسان امنیت اطلاعات در سازمان‌ها و در باب ضرورت انجام تحقیق کاهش خطاهای انسانی و جلوگیری از بروز آسیب‌های محتمل بر روی دارایی‌های داده‌ای سازمان‌ها و همچنین اعتماد به فرهنگ سازمانی قالب را نام برد. این پژوهش با هدف شناسایی ابعاد، مؤلفه‌ها و شاخص‌های مؤثر بر الگوی رفتار حرفه‌ای کارشناسان امنیت اطلاعات در مواجهه با تهدیدات سایبری در سازمان‌ها و شناسایی رابطه آنها می‌پردازد.

روش پژوهش

پژوهش حاضر به روش کمی، کیفی و آمیخته انجام شده است. در مرحله اول از روش فراترکیب برای بررسی و پالایش منابع و اسناد به منظور استخراج شاخص‌ها، ایجاد سؤال و تولید پرسشنامه استفاده شد. برای بررسی اعتبار اسناد، معیارهایی مانند نظام‌مندی محتوای ارائه شده، مشخص بودن منابع مورد استفاده و اطلاعات منابع مورد توجه قرار گرفته شد. از آنجائی که بسیاری از اسناد به دست آمده حاوی اطلاعات کلی در زمینه الگوی رفتاری بوده و اطلاعات مفیدی برای ایجاد مؤلفه در این حوزه ارائه نمی‌کرد، نتایج به دست آمده در این مرحله طی چند فرایند پالایش شدند تا اسناد نامرتب مشخص شوند و اسنادی که موضوع پژوهش را کامل پوشش می‌دهند به عنوان اسناد مرتبط انتخاب شوند. در (شکل ۱) می‌توان خلاصه‌ای از فرایند ارائه شده را همراه با نتایج به دست آمده از پژوهش حاضر مشاهده کرد.

^۱ سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور

^۲ Yildirim, et al



شکل ۱. فرایند نتایج جستجو و انتخاب اسناد مناسب در پژوهش حاضر

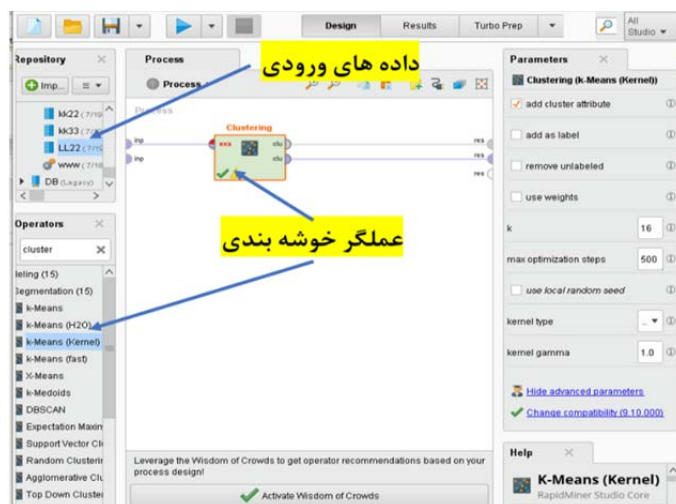
از بین ۱۱۲ منبع نهایی شده ۲۹ منبع به زبان انگلیسی و ۸۳ منبع به زبان فارسی می باشند. منابع انگلیسی بین سال‌های ۲۰۱۷-۲۰۲۱ و منابع فارسی بین سال‌های ۱۳۹۵-۱۴۰۰ می‌باشند. در تحلیل‌های صورت گرفته به کمک روش فراترکیب در گام اول کدهای مشترک و شاخص‌های الگوی رفتاری در مواجهه با تهدیدات امنیتی و سائیری از پیشینه پژوهش شناسایی و استخراج شد. شاخص‌های امنیتی استخراج شده در اکثر مستندات برگرفته از خانواده استانداردهای بین‌المللی سیستم مدیریت امنیت اطلاعات می‌باشد که از جنبه‌های مختلف از نگاه پژوهشگران مورد ارزیابی قرار گرفته است. در این مرحله تعداد ۱۴۲ شاخص می‌تواند با شاخص‌های الگوی رفتاری کارشناسان امنیت اطلاعات در مواجهه با تهدیدات سائیری و امنیتی مطابقت داشته باشد. بنابر کیفی بودن ماهیت پژوهش حاضر، برای انتخاب نمونه آماری و تعیین حجم نمونه (تعداد خبرگان مشارکت‌کننده) از روش نمونه‌گیری گلوله برفی، برای تعیین افراد مشارکت‌کننده استفاده شد. روش کار در این شیوه بدین صورت است که با توجه به موضوع تحقیق از افراد متخصص خواسته می‌شود تا افراد حرفه‌ای خبره و باتجربه دیگر بر اساس معیارهای یادشده را معرفی کنند که برای مشارکت در این پژوهش مناسب هستند. از میان افراد معرفی شده، ۱۱۲ نفر واجد شرایط تشخیص داده شدند. انتخاب افراد و اعضای پانل برای فرآیند دلفی و پاسخ به پرسشنامه در این پژوهش، وابسته به تجربه و تخصص‌های مورد نیاز در موضوع مورد مطالعه بوده و همچنین واجد شرایط یک یا چند ویژگی زیر بودند:

- مدیران واحد‌های سازمانی حوزه امنیت اطلاعات؛

- استادان دانشگاهی مرتبط با علم رایانش امن.

گام بعدی، جلب مشارکت نامزدها برای انجام پژوهش بود که به صورت حضوری، تماس تلفنی و ارسال نامه الکترونیکی انجام شد. سپس دعوت‌نامه‌ای به همراه پرسشنامه در اختیارشان قرار گرفت که شامل چگونگی انجام پژوهش و دریافت موافقت آنها برای مشارکت بود. از این میان در مجموع ۳۰ نفر موافقت خود را برای مشارکت در کارگروه دلفی اعلام کردند اعلام کردند که ۱۵ نفر برای دور اول و ۱۵ نفر دیگر برای دور انتخاب و پرسشنامه اولیه برای ایشان ارسال شد. همچنین برای بخش کمی و مرحله پیمایشی پژوهش لیستی از شرکت‌های داده‌محور و کارشناسان امنیت اطلاعات تهیه شد که پس از فیلتر شدن با معیار حداقل ۵ سال سابقه کار مرتبط برای کارشناسان امنیت اطلاعات، جامعه آماری پژوهش در این مرحله به تعداد ۱۵۶ نفر مشارکت‌کننده رسید، با استفاده از فرمول کوکران^۱ حداقل حجم نمونه برابر ۱۱۱ نفر محاسبه گردید ولی پرسشنامه‌ها به هر ۱۵۶ نفر ارسال و پس از دریافت ۱۱۱ پرسشنامه تکمیل شده، فرایند تحلیل آغاز شد.

^۱. Cochran



شکل ۲. عملیات خوشه بندی اولیه در نرم افزار رپیدماینر

برای خوشه بندی اولیه شاخص‌های مستخرج از بخش فراترکیب در پژوهش حاضر، از نرم افزار رپیدماینر استفاده شد، برای انجام عملیات فوق عملگرهایی مورد استفاده بودند که می‌بایست توانایی خوشه‌بندی متن را داشته باشد و همچنین با توجه فراوانی شاخص‌ها در خوشه-بندی‌های شکل گرفته، شاخص‌های پرت را تشخیص دهد، با در نظر گرفتن این موارد مطابق شکل (۲) اپراتور k-Means (Kernel) بهترین پاسخ را داشته است. پس از اجراء نرم افزار، ۱۴۲ شاخص اولیه خوشه‌بندی و به تفکیک ۱۶ مولفه وارد مرحله آماده سازی جهت پرسشنامه مرحله اول دلفی برای ارسال به خبرگان شد. در دور اول روایی شاخص‌ها با مشارکت و همراهی ۱۵ نفر از خبرگان مورد بررسی قرار گرفت. پس از تحلیل پاسخ پرسشنامه، شاخص‌ها ارزش‌گذاری شده و شاخص‌های خارج از ارزش‌گذاری در لیست حذف قرار گرفت. ملاک ارزش‌گذاری شاخص‌ها پارامتر CVI و CVR بوده است و شاخص‌های با CVR بالای ۷۴٪ و CVI بیش از ۵۹٪ مورد تایید قرار گرفته‌اند (بالان و همکاران ۲۰۲۰). در مرحله دوم شاخص‌هایی که از دید خبرگان مرحله اول دلفی مورد ارزیابی و اجماع قرار گرفته بودن، به همراه ۱۱ شاخص حذف شده به صورت پرسشنامه‌های الکترونیکی و کاغذی در اختیار گروه دوم ۱۵ نفره خبرگان قرار گرفت تا مورد ارزیابی و پایش مجدد قرار گیرد. در مرحله دوم بخش کیفی مطابق با پاسخ پرسشنامه‌ها از سوی خبرگان و ارزش‌گذاری و محاسبه روایی مجدد شاخص‌ها و سایر پارامترهای مورد ارزیابی از جمله آماره‌تی^۱ و سطح معنی‌داری، مطابق با جدول شماره (۱) در نهایت ۱۷ شاخص از جدول کل، حذف شد و در مجموع پس از اجرای کامل مراحل دلفی، شاخص‌ها از ۱۴۲ به ۱۲۵ شاخص کاهش یافت.

جدول ۱. ارزیابی و تحلیل ۱۴۲ شاخص و ۱۶ مولفه در پرسشنامه مرحله اول و دوم دلفی

نتیجه	CVI	CVR	سطح معناداری	آماره تی	نام شاخص	کد	مولفه
حذف	7%	53%	0/3340	-1	کلاه برداری	q01	تهدیدات فیزیکی
حذف	7%	53%	0/0820	-1/871	تخریب	q02	

T-Test یا آماری تی برای مقایسه نسبت دو نمونه جمع‌آوری شده از دو گروه مختلف می‌باشد که از رابطه زیر پیروی می‌کند که در آن، D برابر اختلاف بین نمره هر گویه در دو مرحله دلفی بوده و N تعداد کل گویه‌ها می‌باشد و در این پژوهش ملاک تایید مثبت بودن آماری T می‌باشد. همچنین سطح معنی‌داری میزان خطای پذیرفته شده می‌باشد که در این

$$T = \{(\sum D)/N\} / \sqrt{\sum D^2 - (\sum D)^2 / N} / (N - 1) - N.$$

پژوهش خطا صفر در نظر گرفته شده است.

تایید	100%	100%	0/0000	16	سرقت دارایی	q03	
تایید	73%	87%	0/0000	6/959	نشت/اشتراک اطلاعات	q04	
تایید	100%	100%	0/0000	11/225	دسترسی فیزیکی غیر مجاز(ورود غیر مجاز)	q05	
حذف	7%	53%	0/1640	-1/468	اخاذی	q06	
تایید	100%	100%	0/0000	10/717	نشت اطلاعات به دلیل خطای انسانی	q07	خسارت های غیر عمدی
تایید	87%	93%	0/0000	10/247	استفاده/مدیریت نادرست سیستم	q08	
تایید	87%	93%	0/0000	10/247	استفاده از اطلاعات منابع غیر قابل اعتماد	q09	
حذف	-33%	33%	0/0410	-2/256	تغییر از اطلاعات منابع غیر قابل اعتماد	q10	
تایید	73%	87%	0/0000	11/225	تغییر غیر عمدی داده در سیستم	q11	
تایید	100%	100%	0/0000	16	خسارت ناشی از رفتار طرف ثالث	q12	
تایید	73%	87%	0/0000	10/583	خسارت ناشی از تست نفوذ	q13	
تایید	100%	100%	0/0000	10/583	از دست رفتن اطلاعات در فضای ابر	q14	
تایید	73%	87%	0/0000	11/225	از دست رفتن/تخریب/مخدوش شدن دارایی	q15	
تایید	100%	100%	0/0000	11/225	خرابی یا اختلال لینک ها/شبکه های ارتباطی	q16	شکست/خرابی
حذف	20%	60%	0/1640	-1/468	خرابی یا اختلال زنجیره تامین خدمت	q17	
حذف	20%	60%	0/0820	-1/871	خرابی تجهیزات(دستگاه یا سیستم)	q18	
تایید	100%	100%	0/0000	16	استراق سمع در مسیر انتقال داده ها	q19	انسداد خدمت فعالیت مجرمانه
تایید	100%	100%	0/0000	10/717	گشت زنی در شبکه های بی سیم بی حفاظ	q20	
تایید	100%	100%	0/0000	16	دست کاری ترافیک شبکه	q21	

تایید	100%	100%	0/0000	16	سرقت هویت (حساب)/کلاه برداری	q22	
تایید	100%	100%	0/0000	10/583	دریافت پست الکترونیکی ناخواسته (هرزنامه)	q23	
تایید	100%	100%	0/0000	16	انسداد سرویس	q24	
تایید	87%	93%	0/0000	10/247	اجرا (تزریق) کد/نرم افزار/فعالیت مخرب	q25	
تایید	100%	100%	0/0000	12/475	مهندسی اجتماعی	q26	
تایید	100%	100%	0/0000	11/225	دست کاری سخت افزار و نرم افزار	q27	
تایید	100%	100%	0/0000	12/475	دست کاری اطلاعات	q28	
تایید	87%	93%	0/0000	8/29	سوء استفاده از ابزارهای ممیزی	q29	
تایید	100%	100%	0/0000	16	نصب و راه اندازی غیر مجاز نرم افزار	q30	
تایید	100%	100%	0/0000	11/225	سوء استفاده از اطلاعات محرمانه	q31	
تایید	100%	100%	0/0000	12/475	فعالیت مخرب از راه دور	q32	
تایید	100%	100%	0/0000	11/22 حذف 5	حملات هدفمند	q33	
حذف	20%	60%	0/3340	-1	جستجوی جامع	q34	
تایید	100%	100%	0/0000	11/225	استفاده غیر مجاز از منابع حفاظت شده	q35	تهدیدات قانونی
حذف	7%	53%	0/1640	-1/468	سوء استفاده از داده های خصوصی	q36	
تایید	100%	100%	0/0000	16	ضعف در آموزش کارکنان	q37	دسترسی فیزیکی غیرمجاز (عمدی/سهوی)
تایید	100%	100%	0/0000	12/475	احراز هویت ناکارآمد.	q38	
تایید	87%	93%	0/0000	8/264	قابلیت خواندن حافظه دردستگاه قابل حمل	q39	
تایید	100%	100%	0/0000	10/717	مدیریت خطا به شیوه نادرست	q40	ضعف در نگهداری منابع اطلاعاتی
تایید	100%	100%	0/0000	10/717	امکان تغییر در اطلاعات سامانه	q41	
تایید	100%	100%	0/0000	12/475	تفویض اختیار ناکارآمد	q42	

تایید	100%	100%	0/0000	10/717	پیکر بندی ضعیف سامانه	q43	
تایید	100%	100%	0/0000	12/475	ارزیابی امنیتی ناکارآمد فناوری ها	q44	
تایید	87%	93%	0/0000	10/247	خط مشی و دستور العمل های ناکارآمد	q45	
تایید	60%	80%	0/0000	4/583	سازو کار نادرست در قفل گذاری منابع	q46	محیطی
حذف	20%	60%	0/0820	-1/871	مکان یابی ناکارآمد تجهیزات	q47	
حذف	20%	60%	0/0820	-1/871	تاثیر تجهیزات از شرایط آب و هوایی	q48	
تایید	73%	87%	0/0000	12/475	شکست در اجرای سازو کار حفاظتی	q49	ضعف در کنترل
تایید	100%	100%	0/0000	11/225	ضعف در مدیریت انرژی تجهیزات	q50	
تایید	73%	87%	0/0000	5/172	طراحی ضعیف سیستم	q51	نقص در زیر ساخت ارتباطی
تایید	100%	100%	0/0000	16	از دسترس خارج شدن شبکه ارتباطی	q52	
تایید	100%	100%	0/0000	16	در دسترس نبودن پشتیبان خدمات ارتباطی	q53	
تایید	100%	100%	0/0000	16	شبکه اینترنتی ناامن	q54	
تایید	100%	100%	0/0000	12/475	طراحی و برنامه ریزی ناکارآمد	q55	
تایید	87%	93%	0/0000	5/906	وجود شبکه ارتباطی بیسیم نا امن	q56	حفاظت ناکافی در مقابل شنود
تایید	73%	87%	0/0000	5/172	انتقال نا امن اطلاعات	q57	
تایید	100%	100%	0/0000	12/475	مدیریت نادرست ارتباطات و سرقت نشست	q58	
تایید	100%	100%	0/0000	11/225	ضعف در سازو کار های کنترل دسترسی	q59	بروز فعالیت مجرمانه / سوء استفاده
تایید	100%	100%	0/0000	11/225	اجرای کدها/ دستورات غیر مجاز	q60	
تایید	100%	100%	0/0000	10/717	عدم به کار گیری الگوریتم های معتبر	q61	

					رمزنگاری		
حذف	7%	53%	0/0090	-3/055	امکان دست کاری در ورودی ها	q62	
تایید	60%	80%	0/0000	11/225	ضعف در مواجهه با روشهای مهندسی اجتماعی	q63	
تایید	87%	93%	0/0000	11/225	ضعف در شناسائی شبکه های طعمه	q64	
حذف	33%	67%	0/0040	-3/5	حفاظت ناکافی در مقابل چالش حریم خصوصی	q65	مسائل قانونی
حذف	33%	67%	0/0040	-3/5	خلا های قانونی پیرامون فعالیت طرف ثالث	q66	
حذف	7%	53%	0/0820	-1/871	قوانین بازدارنده و ناکارآمد	q67	
تایید	73%	87%	0/0000	10/583	همراهی کارکنان با خط مشی های امنیت	q68	عوامل انسانی
تایید	60%	80%	0/0000	6/089	حمایت مدیریت عالی از برنامه ها و خط مشی ها	q69	
تایید	60%	80%	0/0000	6/5	حمایت مهارت، تجربه، آگاهی و آموزش کاربران	q70	
تایید	100%	100%	0/0000	10/717	درک نیازهای امنیتی در سطوح مختلف سازمان	q71	
تایید	100%	100%	0/0000	12/475	رفتار محافظه کارانه کاربران در زمینه امنیت	q72	
تایید	87%	93%	0/0000	9/025	پیروی از استانداردها و دستورالعمل های امنیتی	q73	
تایید	100%	100%	0/0000	11/225	حس پاسخگویی، خود ارزیابی	q74	
تایید	100%	100%	0/0000	10/583	تدوین و اجزای برنامه های آموزشی	q75	
تایید	73%	87%	0/0000	12/475	تشویق کارمندان به گزارش مخاطرات	q76	
تایید	100%	100%	0/0000	12/475	تعیین مسئولیت های	q77	

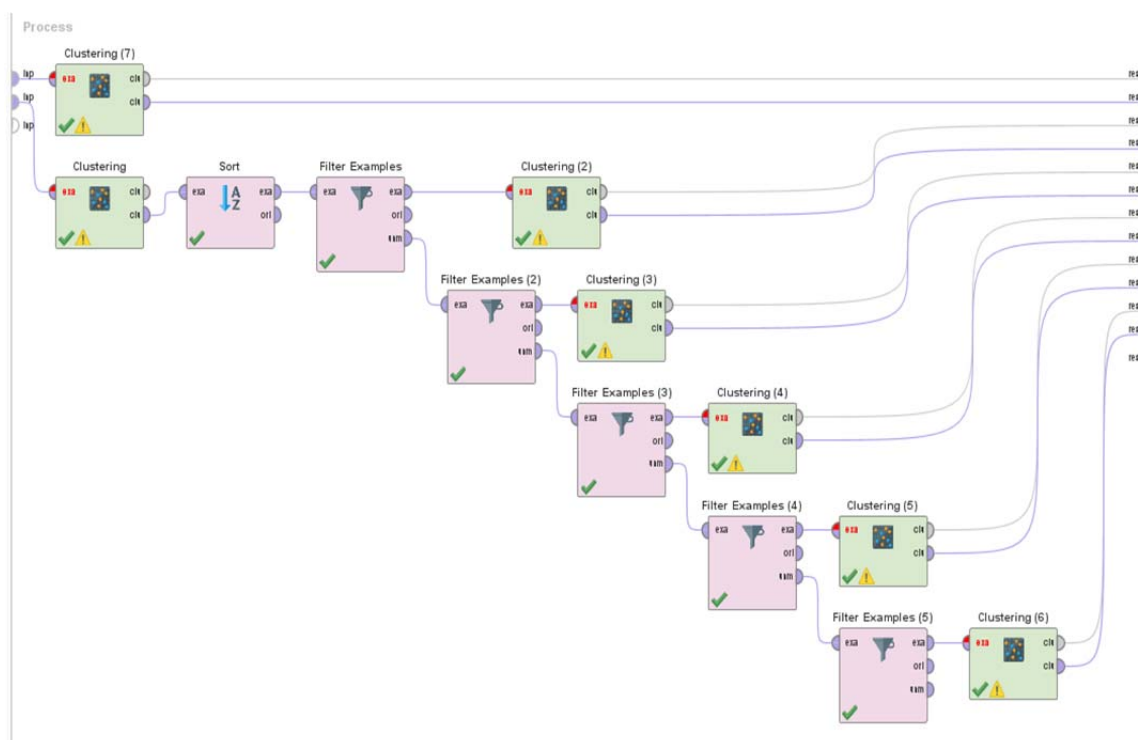
					امنیتی در سطح سازمان		
تایید	73%	87%	0/0000	5/123	تعهد و وفاداری کارمندان به سازمان	q78	
تایید	100%	100%	0/0000	11/225	غربالگری و ارزیابی دوره ای کارمندان	q79	
تایید	73%	87%	0/0000	11/225	تعریف کاربری های مجاز و حقوق دسترسی	q80	
تایید	100%	100%	0/0000	12/475	فرهنگ سازی برنامه های امنیتی سازمان	q81	
تایید	73%	87%	0/0000	11/225	نظارت و پایش مستمر فعالیت های طرف ثالث	q82	عوامل فنی
تایید	73%	87%	0/0000	10/717	استفاده موثر و کارا از سازو کار کنترل دسترسی	q83	
تایید	73%	87%	0/0000	10/717	استفاده از کلمه های عبور قوی	q84	
تایید	100%	100%	0/0000	12/475	استفاده از کارت های هوشمند و توکن امنیتی	q85	
تایید	100%	100%	0/0000	12/475	صدور مجبور و تفویض اختیار	q86	
تایید	100%	100%	0/0000	10/717	دسترسی افراد بیرونی به داده های سیستم	q87	
تایید	100%	100%	0/0000	12/475	حفاظت از منابع در مقابل دسترسی و نفوذ	q88	
تایید	87%	93%	0/0000	10/247	محدود کردن دسترسی کاربران	q89	
تایید	100%	100%	0/0000	16	تعیین خط مشی های حقوق دسترسی کاربران	q90	
تایید	100%	100%	0/0000	11/225	استفاده از سازو کار کنترل دسترسی منطقی	q91	
تایید	100%	100%	0/0000	16	کنترل دسترسی طرف ثالث و پیمانکاران	q92	
تایید	100%	100%	0/0000	11/225	سازو کار امنیت ارتباطات	q93	
تایید	73%	87%	0/0000	10/693	استفاده از سیستم های پایش و سامانه نظارتی	q94	

تایید	100%	100%	0/0000	11	به کارگیری پروتکل های امنیت اطلاعات	q95
تایید	73%	87%	0/0000	12/475	استفاده از الگوریتم های رمزنگاری	q96
تایید	73%	87%	0/0000	12/475	کابل کشی امن مابین سیستم ها/تجهیزات	q97
تایید	100%	100%	0/0000	12/475	کنترل و کدگذاری رسانه های قابل حمل	q98
تایید	100%	100%	0/0000	11/225	محرمانگی (امنیت اطلاعات)	q99
تایید	73%	87%	0/0000	12/475	مدیریت ارتباطات دربرون سپاری خدمات امنیتی	q100
تایید	100%	100%	0/0000	11/225	مدیریت تجهیزات و رسانه های ارتباطی	q101
تایید	87%	93%	0/0000	11/225	گمنام سازی داده ها و لینک های ارتباطی	q102
تایید	73%	87%	0/0000	10/717	سازو کارهای امنیت اطلاعات و سامانه ها	q103
تایید	87%	93%	0/0000	10/583	استفاده از پوششگر ها و سیستمهای تشخیص نفوذ	q104
تایید	87%	93%	0/0000	11/225	استفاده از دیواره آتش و سازکار مدیریت تهدید	q105
تایید	100%	100%	0/0000	10/693	مدیریت، انتقال و نگهداری امن داده ها	q106
تایید	87%	93%	0/0000	12/22	صیانت از صحت و یکپارچگی داده ها	q107
تایید	100%	100%	0/0000	11	امضاها و دیجیتال	q108
تایید	87%	93%	0/0000	10/693	فناوری های نهان نگاری	q109
تایید	100%	100%	0/0000	11/225	سازو کار پاسخگویی و عدم انکار	q110
تایید	87%	93%	0/0000	10/717	سازو کار پالایش محتوا	q111
تایید	100%	100%	0/0000	10/583	سازو کارهای پایش عملیات	q112

تایید	73%	87%	0/0000	10/583	بازرسی سیستم های اطلاعاتی/تجهیزات	q113	
تایید	73%	87%	0/0000	10/717	ممیزی امنیت اطلاعات	q114	
تایید	100%	100%	0/0000	11/5	سازو کار امنیت فیزیکی/ محیطی	q115	
تایید	100%	100%	0/0000	14/666	مدیریت انرژی (پشتیبان برق و شرایط اضطرار)	q116	
تایید	73%	87%	0/0000	10/583	سامانه های اطفاء حریق و اعلام هشدار حرارتی	q117	
تایید	87%	93%	0/0000	11/225	سازو کارهای مقاوم سازی	q118	
تایید	100%	100%	0/0000	11/225	ایمن سازی فیزیکی دستگاه های الکترونیکی	q119	
تایید	100%	100%	0/0000	11/225	ایمن سازی اماکن و فضاهای حساس	q120	
تایید	87%	93%	0/0000	11	استانداردها و سازو کارهای کنترل دما و رطوبت	q121	
تایید	100%	100%	0/0000	10/583	سازو کار پشتیبان گیری و دسترس پذیری	q122	
تایید	100%	100%	0/0000	12/22	استفاده از دارایی ها و تجهیزات اضافی	q123	
تایید	100%	100%	0/0000	10/693	پشتیبان گیری منظم از سیستم ها	q124	
حذف	33%	67%	0/0040	-3/5	افزایش ظرفیت حافظه	q125	
تایید	100%	100%	0/0000	12/22	استفاده از چک لیست های امنیتی	q126	عوامل فرآیندی
تایید	100%	100%	0/0000	11	تدوین قوانین، خط مشی ها، دستورالعمل	q127	
تایید	60%	80%	0/0000	11/5	عضویت و تعامل بانجمن های حرفه ای امنیت	q128	
تایید	100%	100%	0/0000	11	تعیین جریمه برای عدم پیروی از خط مشی ها	q129	
تایید	60%	80%	0/0000	12/22	تعیین راهبردها و اهداف مدیریتی	q130	

تایید	100%	100%	0/0000	12/22	برنامه ریزی، تحلیل پیامد و بودجه بندی امنیتی	q131
تایید	87%	93%	0/0000	11	سازمان دهی سایت های مشکوک توسط کاربران	q132
تایید	100%	100%	0/0000	12/22	تدوین اصول و روال های پایش و کنترل کارمند	q133
تایید	87%	93%	0/0000	11/5	ارزیابی و بروزرسانی قوانین، خط مشی	q134
تایید	100%	100%	0/0000	10/693	اصول جمع آوری، نظارت و تحلیل اطلاعات	q135
تایید	100%	100%	0/0000	11	بررسی صحت، محرمانگی و دسترس پذیری	q136
تایید	100%	100%	0/0000	10/583	اصول طبقه بندی داده ها و منابع اطلاعاتی	q137
تایید	100%	100%	0/0000	10/717	روش شناسایی و طبقه بندی دارایی ها	q138
تایید	100%	100%	0/0000	16	طراحی معماری امن	q139
تایید	100%	100%	0/0000	12/475	برنامه ریزی آموزشی و آگاهی رسانی امنیتی	q140
حذف	7%	53%	0/0090	-3/055	رویه های تشخیص، گزارش دهی و پاسخ رخداد	q141
حذف	7%	53%	0/0820	-1/871	تدوین استانداردهای امنیتی	q142

جهت خوشه‌بندی و احصاء ابعاد و مؤلفه‌های نهایی پژوهش، به کمک نرم افزار رییدماینر مرتب سازی شاخص‌ها توسط عملگر Sort انجام شد و سپس به کمک عملگر Filter شاخص‌های با صفت خوشه مربوطه جداسازی شده و مجدد وارد عملگر K-Means گردید تا مولفه های هر بعد احصا شود. کل فرایند فوق الذکر به شرح شکل (۳) پیاده سازی گردید.



شکل ۳. اجرای خوشه‌بندی طبقه‌ای در ریدماینر

مجدداً به کمک عملگر K-Means برای شاخص‌های نهایی‌شده، خوشه‌های کلی به دست آمد که شامل ۵ بعد اصلی این پژوهش است، سپس با در نظر گرفتن فراوانی شاخص‌ها در هر بعد، خوشه‌ها به خوشه‌های کوچک‌تری تقسیم شده و در مرحله دوم، برای دست‌آوردن مؤلفه‌های پژوهش، خوشه‌های فیلترشده، هر کدام مجدداً خوشه‌بندی و مؤلفه‌های هر بعد احصاء گردید، در نهایت با خوشه‌بندی انجام شده در نرم‌افزار، ابعاد و مؤلفه‌ها و شاخص‌های این پژوهش شامل ۵ بعد، ۱۷ مؤلفه و ۱۲۵ شاخص مطابق با **جدول (۱)**، منتج به آماده‌سازی ۱۲۵ سؤال طبقه‌بندی شده برای ارسال به ۱۱۱ نفر از کارشناسان امنیت اطلاعات در جامعه آماری در مرحله پیمایشی و بخش کمی گردید.

جدول ۲. ابعاد و مؤلفه‌های احصاء شده توسط نرم افزار ریدماینر

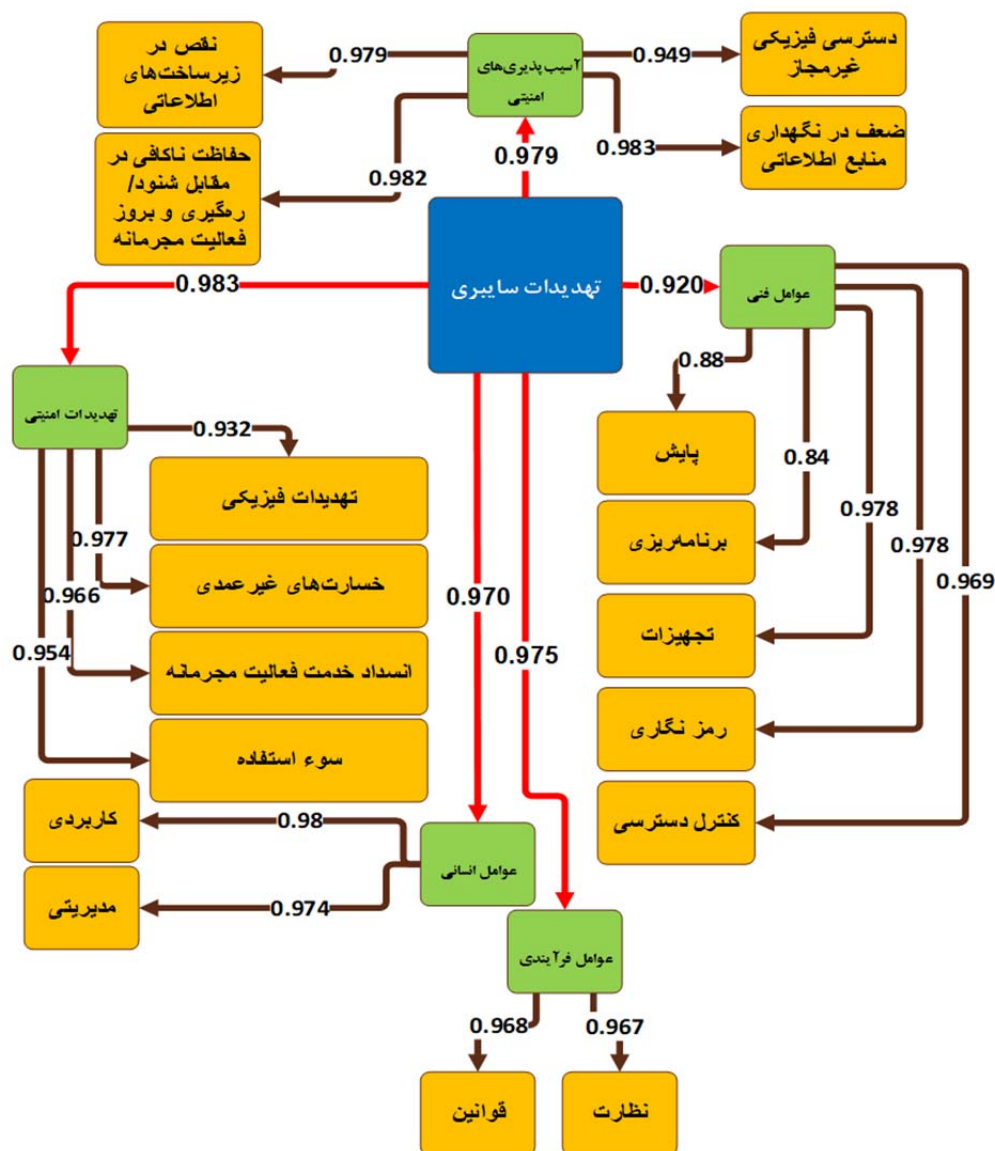
مؤلفه	ابعاد
حفاظت ناکافی در مقابل شنود/ره‌گیری و بروز فعالیت مجرمانه	آسیب‌پذیری‌های امنیتی
دسترسی فیزیکی غیرمجاز	
ضعف در نگهداری منابع اطلاعاتی	
نقص در زیرساخت‌های اطلاعاتی	
انسداد خدمت فعالیت مجرمانه	تهدیدات امنیتی
تهدیدات فیزیکی	
خسارت‌های غیرعمدی	
سوء استفاده	
مدیریتی	عوامل انسانی
کاربردی	
قوانین	عوامل فرایندی

مؤلفه	ابعاد
نظارت	
برنامه‌ریزی	عوامل فنی
تجهیزات	
رمز نگاری	
پایش	
کنترل دسترسی	

در این مرحله پاسخ‌ها به کمک نرم‌افزارهای MATLAB و SPSS مورد تجزیه و تحلیل آماری قرار گرفتند، در ابتدا پایایی پاسخ‌ها به کمک نرم‌افزار MATLAB و ضریب آلفای کرونباخ محاسبه گردید و سپس برای هر بعد و مؤلفه‌های آن، بار عاملی یا لامبدا^۱ مرتبه دوم و سوم محاسبه و بر اساس وزن بعدها و مؤلفه‌ها میزان اثرگذاری هر بعد و مؤلفه‌های آن به دست آمد. در ادامه تحلیل‌های مشروح ارائه گردیده است.

^۱ Lambda

بار عاملی یا لامبدا^۱ در حقیقت یک ضریب همبستگی بین متغیرهای پنهان و متغیرهای آشکار است. این ضریب تعیین می‌کند که متغیر پنهان چقدر از واریانس متغیرهای آشکار را تبیین می‌کند و از آن جا که یک ضریب همبستگی است باید از نظر آماری معنادار باشد.



شکل ۴. سنجش میزان وزن مؤلفه و شاخص‌های تهدیدات سایبری

متناسب با بارعاملی مرتبه دوم از بین ۵ مؤلفه اصلی این پژوهش، مؤلفه «تهدیدات امنیتی» بیشترین وزن را دارد و برخلاف دیدگاه عمومی، مؤلفه «عوامل فنی» کمترین وزن را به خود تخصیص داده و بیانگر این موضوع است که ابزارهای محافظت اطلاعات لزوماً برای مقابله با تهدیدات سایبری کافی نیستند. با بررسی مشخصه‌های مؤلفه «تهدیدات امنیتی»، مطابق پارامتر بارعاملی مرتبه دوم مشخصه «خسارت‌های غیر عمدی» قوی‌ترین وزن را دارد و این نتیجه بیانگر این موضوع می‌باشد که مطابق نظر کارشناسان امنیت اطلاعات، برای مقابله و یا پیشگیری از تهدیدات سایبری، کاهش خطای رفتاری کارکنان امنیت اطلاعات از اهمیت بالاتری برخوردار است.

بحث و نتیجه‌گیری

با در نظر گرفتن مراحل پژوهش، یافته‌ها و نتایج پژوهش، براساس وزن ابعاد و مؤلفه‌ها و شاخص‌ها، اولویت بندی ارائه شده در الگوی پیشنهادی رفتار حرفه‌ای و صحیح کارشناسان امنیت اطلاعات در مواجهه با تهدیدات سایبری به شرح ذیل قابل تفسیر است.

❖ بر اساس داده‌های پژوهش در خصوص «تهدیدات امنیتی» موارد زیر جهت تبیین کارشناسان امنیت اطلاعات پیشنهاد می‌گردد:

- شناسایی و پایش مداوم تهدیدات فیزیکی و دسترسی‌های غیرمجاز سازمان؛

- هوشیاری در مقابل خسارت‌های غیرعمدی ناشی از خطای انسانی؛
 - انسداد خدمت در صورت مشاهده فعالیت مجرمانه؛
 - هوشیاری در مقابل خسارت‌های غیرعمدی ناشی از خطای انسانی؛
 - ایجاد حساسیت در ارکان سازمانی به منظور خنثی‌سازی سوء استفاده‌های احتمالی مانند مهندسی اجتماعی.
- ❖ براساس داده‌های پژوهش درخصوص «آسیب‌پذیری‌های امنیتی» موارد زیر جهت تبیین کارشناسان امنیت پیشنهاد می‌گردد:
- جلوگیری از دسترسی فیزیکی غیرمجاز با استفاده از ابزارهای احراز هویت و آموزش‌های لازم کارکنان؛
 - تمهیدات لازم در حفاظت کافی در مقابل شنود اطلاعات و ره‌گیری در صورت بروز فعالیت مجرمانه؛
 - طراحی و برنامه‌ریزی کارآمد در خصوص حفاظت از زیر ساخت‌های اطلاعاتی؛
 - تدوین خط‌مشی و دستورالعمل نگهداری کارآمد از منابع اطلاعاتی.
- ❖ براساس داده‌های پژوهش درخصوص «عوامل انسانی» موارد زیر جهت تبیین کارشناسان امنیت اطلاعات پیشنهاد می‌گردد:
- تعریف و پایش مداوم کاربری‌های مجاز سیستم و بررسی سطوح دسترسی
 - غربالگری و ارزیابی دوره‌ای کارمندان از منظر ملاحظات امنیت اطلاعات؛
 - رفتارمحافظه کارانه در زمینه امنیت سیستم‌های اطلاعاتی؛
 - هم‌سو کردن کارکنان با خط‌مشی‌های امنیت اطلاعات سازمان؛
 - پرورش حس پاسخگویی، خود ارزیابی و خود گزارش‌دهی؛
 - هم‌سو کردن مدیریت عالی به منظور حمایت از برنامه‌ها، پروژه‌ها و خط‌مشی‌های امنیتی سازمان؛
 - ایجاد روحیه تعهد و وفاداری کارمندان سازمان به رعایت ملاحظات امنیتی رایج؛
 - پیروی از استانداردها و دستورالعمل‌های امنیتی؛
 - پذیرش مسئولیت‌های امنیتی سازمان؛
 - نظارت و پایش مستمر فعالیت‌های طرف ثالث در حوزه امنیت اطلاعات؛
 - درک نیازهای امنیتی در سطوح مختلف سازمان؛
 - فرهنگ‌سازی سازمانی در خصوص برنامه‌های امنیتی سازمان؛
 - تلاش برای افزایش آگاهی کارکنان در زمینه امنیت اطلاعات؛
 - ترقیب کارمندان سازمان به گزارش مخاطرات و مشکلات امنیتی؛
 - تدوین و اجرای برنامه‌های آموزشی در حوزه امنیت اطلاعات (تکنیک‌های نفوذ، هک، اخلاقیات، قوانین و مقررات، ممیزی و)؛
- ❖ براساس داده‌های پژوهش درخصوص «عوامل فرآیندی» موارد زیر جهت تبیین کارشناسان امنیت اطلاعات پیشنهاد می‌گردد:
- به کارگیری پروتکل‌های امنیت اطلاعات به‌منظور ایجاد ارتباط امن؛
 - استفاده مؤثر و کارا از سازوکار کنترل دسترسی و صدور مجوز؛
 - استفاده از سیستم‌های پایش و سامانه‌های جامع نظارت اطلاعات سازمانی؛
 - کنترل و کدگذاری رسانه‌های قابل حمل سازمانی و سامانه‌ها؛
 - استفاده از پوششگرها و سیستم‌های بروز تشخیص نفوذ؛
 - نظارت و کنترل دسترسی طرف ثالث و پیمانکاران؛
 - گمنام‌سازی داده‌ها و لینک‌های ارتباطی؛
 - حفاظت از منابع در مقابل دسترسی و نفوذ فیزیکی؛
 - استفاده از دیواره آتش و ساز کار یک‌پارچه مدیریت تهدید؛

- استفاده از الگوریتم‌های رمزنگاری در زیرساخت اطلاعاتی؛
- محدود کردن دسترسی کاربران در طرح سطح‌بندی اطلاعات؛
- مدیریت، انتقال و نگهداری امن داده‌های سازمانی؛
- تدوین سازوکار و بازرسی امنیت ارتباطات و تجهیزات ارتباطی؛
- نظارت بر دسترسی افراد بیرونی به اطلاعات سیستم؛
- حفظ محرمانگی و صیانت از صحت و یکپارچگی داده‌های سازمانی (امنیت اطلاعات سازمانی)؛
- مدیریت ارتباطات در برون‌سپاری خدمات امنیتی؛
- مدیریت و تعیین خط‌مشی‌های حقوق دسترسی کاربران؛
- سازوکار پالایش محتوا و پایش عملیات؛
- رعایت استانداردها و سازوکارهای کنترل دما و رطوبت دستگاه‌های الکترونیکی؛
- استفاده از امضاهای دیجیتالی در سامانه‌های سازمانی و به کارگیری فناوری‌های نهان‌نگاری؛
- مدیریت انرژی (پشتیبان برق و مدیریت شرایط اضطرار و سامانه‌های اطفای حریق و اعلام هشدار حرارتی)؛
- ایمن‌سازی و مقاوم‌سازی فیزیکی و محیطی اماکن و فضاها حساس؛
- ممیزی ادواری امنیت اطلاعات سازمانی.

❖ بر اساس داده‌های پژوهش در خصوص «عوامل فنی» موارد زیر جهت تبیین کارشناسان امنیت اطلاعات پیشنهاد می‌گردد:

- پشتیبان‌گیری منظم از سیستم‌ها و بررسی دسترسی پذیری و ظرفیت حافظه پشتیبان؛
- تدوین اصول پایش و کنترل کاربران؛
- بررسی مداوم صحت، محرمانگی و دسترسی پذیری اطلاعات سازمان؛
- عضویت و تعامل با انجمن‌های حرفه‌ای امنیت؛
- سازمان دهی قواعد استفاده از اینترنت توسط کاربران؛
- برنامه ریزی‌های آموزشی و آگاهی رسانی امنیتی؛
- ارزیابی و به روزرسانی منظم قوانین و خط‌مشی‌های سازمان؛
- استفاده از روش‌های کارآمد در شناسایی و طبقه‌بندی دارایی‌ها؛
- تدوین قوانین، خط‌مشی‌ها، دستورالعمل‌ها و استانداردهای امنیتی؛
- برنامه‌ریزی و بودجه‌بندی امنیتی سازمان و ارائه گزارش به مدیریت عالی؛
- رعایت اصول طبقه‌بندی داده‌ها و منابع اطلاعاتی؛
- ایجاد رویه‌های تشخیص، گزارش دهی و پاسخ به رخداد و استفاده از چک لیست‌های امنیتی؛
- تعیین راهبردها در صورت عدم پیروی از خط‌مشی‌های امنیتی توسط کاربران؛
- طراحی معماری امن؛
- رعایت اصول جمع آوری، نظارت و تحلیل اطلاعات.

به دلیل حائز اهمیت بودن خسارت‌های غیرعمدی در بعد تهدیدات امنیتی و برآورد عوامل مؤثر بر آن، شاخصه‌های «خسارت‌های غیرعمدی» مجدداً بررسی گردید و هر شاخصه و عامل پیشگیری کننده از آن شاخصه بصورت ضمنی در جدول (۳) اشاره شد که برآورد می‌گردد تمام این شاخصه‌ها به کمک آموزش، بازآموزی و آگاه‌سازی قابل پیشگیری هستند و این موضوع بیانگر اهمیت آموزش، بازآموزی و آگاه‌سازی در حیطه امنیت اطلاعات می‌باشد.

جدول ۳. بررسی شاخص‌های خسارت‌های غیر عمدی

آگاه سازی	نشت اطلاعات به دلیل خطای انسانی	تهدیدات امنیتی	خسارت های غیر عمدی
آموزش	استفاده/مدیریت نادرست سیستم		
آگاه سازی	استفاده از اطلاعات منابع غیر قابل اعتماد		
آگاه سازی	تغییر غیر عمدی داده در سیستم		
آموزش	خسارت ناشی از رفتار طرف ثالث		
آموزش	خسارت ناشی از تست نفوذ		
آموزش	از دست رفتن اطلاعات در فضای ابر		
آگاه سازی	از دست رفتن/تخریب/مخدوش شدن دارایی		

با توجه به نتایج بدست آمده از این کار پژوهشی، نیاز است که شرکت‌های داده‌محور، علاوه بر استخدام متخصصین آموزش دیده، رویکرد بازآموزی و آگاه‌سازی را در خط‌مشی امنیت اطلاعاتی خود تبیین کرده و مصر بر اجرای آن باشند. دو خطای مهیب که می‌بایست توسط آموزش و آگاه‌سازی در کارمندان امنیت اطلاعات تقلیل یا حذف گردد خطاهای روان شناختی "اثر دانینگ کروگر"^۱ (دانینگ ۲۰۱۱) و "توهم بوقلمون"^۲ است، در مورد اول کارمندان با کمی یادگیری در یک زمینه دچار توهم تخصص و خبرگی در آن زمینه می‌شوند و این خطای ادراکی می‌تواند به شدت آسیب زنده باشد و در مورد دوم زمانی رخ می‌دهد که کارمند امنیت اطلاعات چندین بار سهل‌انگاری کرده و هیچ اتفاقی رخ نداده است و نمی‌داند که ممکن است با یک بار دیگر تکرار آن سهل‌انگاری یک فاجعه در کمین باشد.

همان‌گونه که از نتایج پژوهش حاضر مشخص شد، پاشنه آشیل امنیت اطلاعات، کارمندان هستند نه ابزار، برای مقابله با تهدیدات آینده نمی‌توان منتظر ظهور تهدیدات نوین ایستاد و در مرحله بعد ابزاری متناسب تهیه کرد بلکه از آنجایی که منشاء بسیاری از حملات سایبری عامل انسانی است که به صورت ناخواسته و ناآگاهانه زمینه را برای نفوذ و حمله فراهم می‌کند. از این رو آموزش و فرهنگ‌سازی می‌تواند در بسیاری از حوادث سایبری نقش پیشگیرانه داشته باشد. از طرف دیگر آگاهی از حوادث سایبری در زیر ساخت‌های مشابه، آمادگی سازمان را در مواجهه با وضعیت مشابه افزایش می‌دهد. بدون شک کارکنان دارای دانش و آگاهی، یکی از مهم‌ترین خطوط دفاعی در تامین امنیت سازمان هستند. در این خصوص سازمان وظیفه دارد تا سیاست‌های لازم را در خصوص آموزش کارشناسان و کاربران خود را تدوین کند. برای دریافت نتیجه مطلوب می‌توان سیاست‌های زیر را دنبال کرد:

برنامه آموزش امنیت اطلاعات سازمان براساس نیاز سنجی و متناسب با نقش و مسئولیت کارشناسان

۰ برگزاری دوره‌های عمومی، تخصصی و کارگاه‌های مهارت‌افزایی در حوزه امنیت سایبری برای متخصصین و جامعه هدف آموزشی سازمان با استفاده از ظرفیت مراکز دارای پروانه و استادان مجرب؛

۰ اخذ گواهی آموزش از مراکز دارای پروانه ارائه خدمات آموزشی (افتا) برای کلیه شرکت‌کنندگان در دوره‌های آموزشی؛

۰ برگزاری همایش‌های عمومی به منظور ارتقای فرهنگ امنیت سایبری در سازمان و آگاهی عموم کارکنان از تهدیدات سایبری ویژه کسب و کار سازمان؛

۰ ارائه سازو کار به منظور اشتراک‌گذاری اطلاعات، تجارب و دانش امنیت سایبری در سازمان؛

^۱. Dunning-Kruger

^۲. Dunning

^۳. اولین بار توسط برتراند راسل معرفی شد: بوقلمونی که برای روز شکرگزاری تعیین شده است، هر روز تغذیه و مراقبت می‌شود تا زمانی که ذبح شود. با هر تغذیه، اطمینان یا اعتماد به نفس آن که هیچ اتفاقی برای آن رخ نخواهد داد، بر اساس تجربه گذشته افزایش می‌یابد. از نقطه نظر بوقلمون، اطمینان از اینکه روز بعد دوباره تغذیه و مراقبت خواهد شد، در شب قبل از مرگ آن، از همه روزها بیشتر است. باین حال، آن روز توسط همان کسی که از او مراقبت می‌کرد، کشته می‌شود.

- 0 ارائه سازو کار به منظور اطلاع رسانی و آگاهی رسانی به جامعه هدف سازمان و نهادهای سازی امنیت در فرآیندهای کاری کارکنان؛
- 0 پایش و اطلاع رسانی اخبار تهدیدات، آسیب پذیری ها و حوادث سایبری در حوزه کسب و کار سازمان به صورت مستمر؛
- 0 ارزیابی دوره ای میزان آمادگی و آگاهی کارکنان و کارشناسان در حوزه امنیت سایبر.

منابع

- حسینی، ص.، حبیبی، ح. و حسن پور، م. (۱۳۹۳). مدل استرس شغلی در محیط های آموزشی - دانشگاهی. پژوهش های نوین روانشناختی. فصلنامه پژوهش های نوین روانشناختی، ۹ (۳۳)، ۲۱.
- خطایی، ن.، هدایتی، ع. و آغازاریان، و. (۱۴۰۱). بررسی روش های مقابله با حملات جعل در ارتباطات شبکه های خودرویی. نشریه فناوری اطلاعات و ارتباطات انتظامی، ۳ (۱۱)، ۴۱.
- دی پیر، م. (۱۴۰۱). ارائه معیاری برای محاسبه خطر امنیتی لینک ها برای جلوگیری از کلاهبرداری های اینترنتی. فصلنامه فناوری اطلاعات و ارتباطات انتظامی، ۳ (۱۱)، ۲۳.
- رجبی، ف. و حاجیه علیپور، ع. (۱۴۰۱). تاثیر اجرای خط مشی گذاری عمومی بر فرهنگ سازمانی. نشریه خط مشی گذاری عمومی در مدیریت، ۱۳ (۴۵)، ۱۰۳-۱۲۱.
- شعبانی، م.، رفعتی اصل، م. و سهرابی، ش. (۱۴۰۰). امکان سنجی استقرار مدیریت دانش در سازمان هوشمند فناور محور. نشریه فناوری اطلاعات و ارتباطات انتظامی، ۲ (۴)، ۶۷-۸۴.
- قربانی، و. و ثقفی، ک. (۱۳۹۸). ارائه مدل کلان امنیت اطلاعات فضای سایبر در جمهوری اسلامی ایران. فصل نامه امنیت ملی، ۹ (۳۳)، ۳۵۳-۳۱۵.
- کریمی، ز. و پیکری، ح. ر. (۱۳۹۸). مدیریت امنیت اطلاعات: تاثیر تعهد سازمانی و عواقب ادراک شده افشای اطلاعات محرمانه بر قصد نقض امنیت اطلاعات بیماران. اخلاق پزشکی، ۴۴ (۱۳)، ۲۰-۲۹.
- منصوری، ع. و جعفری، ع. (۱۳۹۴). نقش آموزش های تخصصی IT در پیاده سازی سیستم مدیریت امنیت اطلاعات در سازمان. دومین همایش ملی علوم مدیریت و برنامه ریزی، آموزش و استاندارد سازی ایران. دومین همایش ملی علوم مدیریت و برنامه ریزی، آموزش و استاندارد سازی ایران - ۱۳۹۴
- نوروزی، ح.، سمیعی، م.، و رشوادی، ی. (۱۳۹۹). شناسایی و تبیین راهبردهای ترفیع در رسانه های اجتماعی (مورد مطالعه: اینستاگرام). تحقیقات بازاریابی نوین. مجله تحقیقات بازاریابی نوین، ۱۰ (۳).
- حبیبی، آ. و سرآبادانی، م. (۱۴۰۱). آموزش کاربردی SPSS. انتشارات نارون.
- کمانی، م. (۱۴۰۱). بررسی تغییر از جرائم خیابانی به جرائم سایبری در آغاز همه گیری کووید-۱۹، رویکردی به نظریه فعالیت های روزانه. سومین کنفرانس ملی پدافند سایبری ۱۴۰۱ شماره ۱۷
- مصلح شیرازی، ع.، محمدی، ع.، رعنائی، ح.، و هنرپروران، ح. (۱۳۹۶). طراحی مدل پویاشناسی سیستم برای سیاستگذاری ارتقای شاخص های شبکه فناوری اطلاعات و ارتباطات ایران. نشریه فناوری اطلاعات و ارتباطات ایران، (۳۰-۲۹).
- نوده فراهانی، س.، جباری، ح.، پناهیان، ح. (۱۴۰۰). ارائه مدل مفهومی مؤلفه ها و شاخص های سرمایه انسانی مؤثر بر امنیت اطلاعات سازمان ها. نشریه پژوهش های حفاظتی - امنیتی، ۹ (۳۵).

Referencse

- Ahmed, S., & Hassan, M. (2003). Survey and case investigations on application of quality management tools and techniques in SMIs. *International Journal of Quality & Reliability Management*, 20(7), 795-826.

- AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in human behavior*, 49, 567-575.
- Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, 11(8), 3383.
- Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, 102003.
- Angelo, C., Mariangela, L., Marianna, L., Angela, L. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, 137.
- Ansari, Meraj F. Sharma, P. K. & Dash, Bibhu (2022). Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. *International Journal of Smart Sensor and Adhoc Network*, 3(3).
- Bengston, D. N. (2018). Principles for thinking about the future and foresight education. *World Futures Review*, 10(3), 193-202.
- Bibhu, D., Meraj F. Ansari, (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy. *International Research Journal of Engineering and Technology* e-ISSN: 2395-0056
- Chen, X., & Tyran, C. K. (2023). A Framework for Analyzing and Improving ISP Compliance. *Journal of Computer Information Systems*, 1-16.
- Colwill, C. (2009). Human factors in information security: The insider threat-Who can you trust these days? *Information Security Technical Report*, 14(4), 186-196.
- Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, 137, 103614.
- Dator, J., & Dator, J. (2019). *Futures studies as applied knowledge*. Jim Dator: A Noticer in Time: Selected work, 1967-2018, 7-16.
- Day Pir, M. (1401). Providing a measure to calculate the security risk of links to prevent Internet fraud. *Police Information and Communication Technology Quarterly*, (11), 23 [In Persian].
- Dunning, D. (2011). The Dunning-Kruger effect: On being ignorant of one's own ignorance. *In Advances In Experimental Social Psychology*, 44, 247-296
- Deal, T. & Kennedy, A. (1999). *The New Corporate Cultures: Revitalizing the workplace after Downsizing, Mergers, and Reengineering*. Cambridge: Basic Books, a member of the Perseus Books Group
- Ernest Chang, S. and Lin, C. (2007), Exploring organizational culture for information security management, *Industrial Management & Data Systems*, Vol. 107 No. 3, pp. 438-458. <https://doi.org/10.1108/02635570710734316>
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, 18(1), 39-50.
- Ghorbani, Gh. & Thaghafi, K. (2018), Presenting the macro model of cyber space information security in the Islamic Republic of Iran. *National Security Quarterly*, 9(33), 315-353 [In Persian].
- Habibi, A. & Sarabadani, M. (1401). *SPSS practical training*. Naron Publications. [In Persian].
- Hosseini, S., Habibi, H. and Hasanpour, M. (2013). Occupational stress model in educational-university environments. New psychological research. *New Psychological Research Quarterly*, 9(33), 21 [In Persian].
- James A. O'Brien, & George M. Marakas, (2011). *Management information systems*. Print Book, McGraw-Hill/Irwin
- Kamai, M. (1401). Investigating the change from street crimes to cyber crimes at the beginning of the Covid-19 pandemic, an approach to the theory of daily activities. *Third National Cyber Defense Conference* 1401 No. 17 [In Persian].
- Karlsson, M., Karlsson, F., Åström, J. and Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance, *Information and Computer Security*, 30(33), 382-401. <https://doi.org/10.1108/ICS-06-2021-0073>
- Khotaei, N., Hedayati, A., and Achararian, V. (1401). Examining the methods of dealing with forgery attacks in car network communications. *Police information and communication technology magazine*, (11), 41 [In Persian].
- Karimi, Z. and peykari, H. (2018). Information security management: the effect of organizational commitment and the perceived consequences of disclosure of confidential information on the intention to violate patients' information security. *Medical ethics*, 44(13), 20-29 [In Persian].
- Lee, I. (2020) Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, 12, 157. <https://www.mdpi.com/1999-5903/12/9/157> <https://doi.org/10.3390/fi12090157>
- Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, 13-24. <https://doi.org/10.1016/j.ijinfomgt.2018.10.017>
- Mansouri, A. & Jafari, A. (2014). The role of specialized IT training in the implementation of the information security management system in the organization. *The second national conference of management sciences and planning, education and standardization of Iran. The second national conference of management sciences and planning, education and standardization of Iran – 2014*. [In Persian].
- M. Lezzi et al. (2018). Cybersecurity for Industry 0/4 in the current literature: a reference framework. *Comput. Ind.*

- Mosleh Shirazi, A., Mohammadi, A., Ranaei, H., and Hanparvaran, H. (2016). Designing a system dynamics model for policy-making to improve the indicators of Iran's information and communication technology network. *Iranian Information and Communication Technology Journal*, (29-30). [In Persian].
- Moti Zwilling et al. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 62(1).
- Niekerk, J. v., & Solms, R. v. (2005). A holistic framework for the fostering of an information security sub-culture in organizations. *Nelson Mandela Metropolitan University*.
- Nodeh Farahani, S., Jabari, H., Panahian, H. (Spring 1400). Presenting a conceptual model of the components and indicators of human capital effective on the information security of organizations. *Journal Of Protection-Security Research*, 9(35). [In Persian].
- Nowrozi, H., Samii, M., and Rashnavidi, Y. (2019). Identifying and explaining promotion strategies in social media (case study: Instagram). Modern marketing research. *Modern Marketing Research Journal*, 10(3). [In Persian].
- Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The Influence of Organizational Information Security Culture on Information Security Decision Making. *Journal of Cognitive Engineering and Decision Making*, 9(2), 117–129. <https://doi.org/10.1177/1555343415575152>
- Pivoto, D. G., de Almeida, L. F., da Rosa Righi, R., Rodrigues, J. J., Lugli, A. B., & Alberti, A. M. (2021). Cyber-physical systems architectures for industrial internet of things applications in Industry 0/4: A literature review. *Journal Of Manufacturing Systems*, 58, 176-192.
- Rahimli, Ailar. (2012). Knowledge Management and Competitive Advantage. *Information and Knowledge Management*. 37-43.
- Rajabi, F. & Hajieh Alipour, A. (1401). The effect of public policy implementation on organizational culture. *Journal Of Public Policy In Management*, 13(45), 103. [In Persian].
- Shabani, M., Rifati -Assal, -M. and Sohrabi, Sh. (1400). The feasibility of establishing knowledge management in a technology-oriented intelligent organization. *Police Information And Communication Technology Publication*, 2(4), 67-84. [In Persian]
- Solomon, G. and Brown, I. (2021), The influence of organisational culture and information security culture on employee compliance behaviour, *Journal of Enterprise Information Management*, 34 (4), 1203-1228. <https://doi.org/10.1108/JEIM-08-2019-0217>
- Sugiono, E., Efendi, S., & Afrina, Y. (2021). The effect of training, competence and compensation on the performance of new civil servants with organizational culture as intervening: Studies at the ministry of health of the republic of Indonesia. *International Journal of Science and Society*, 3(1), 262-279.
- Stanton, J., Mastrangelo, P. R., Stam, K. R., & Jolton, J. (2004). *Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices*. Proceedings of the Tenth Americas Conference on Information Systems. New York.
- Tejay, G. P., & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management*, 60(3), 103751.
- Wu, J., & Yang, T. (2023). *Knowledge Discovery from Online Reviews*. In *Knowledge Technology and Systems: Toward Establishing Knowledge Systems Science*, 71-104. Springer Nature Singapore.
- Xiaofen, M. (2022). IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing & Management*, 59(1)