Journal of Knowledge Studies
(Library and Information Science and Information Technology)
I. A. U. North Tehran Branch
Print ISSN: 2008-2754 Online ISSN: 2783-4115

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 Abromand[2] | Dariush Matlabi[3]

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

Article type:
Research Article

Article history:
Received:
10-12-2022
Received in revised form:
14-01-2023
Accepted:
09-02-2023
Published online:
19-06-2023

Keywords:
Behavioral Pattern,
Information Security,
Cyber Threats,
Futurism,
Hyper Combination

ABSTRACT

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.

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.

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.

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.

Publisher: Islamic Azad University North Tehran Branch

دانش شناسی
(علوم کتابداری و اطلاع رسانی و فناوری اطلاعات)
شاپا الکترونیکی: ۴۱۱۵-۲۷۸۳ شاپا چاپی: ۲۷۵۴-۲۰۰۸

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

صدیقه محمداسماعیل[1*] | محمدباقر رایین آبرومند[2] | داریوش مطلبی[3]

۱. دانشیار گروه علم اطلاعات و دانش شناسی، واحد علوم تحقیقات دانشگاه آزاد اسلامی، تهران. (نویسنده مسئول) m.esmaeili2@gmail.com
۲. دانشجو دکتری تخصصی علم اطلاعات و دانش شناسی، 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

نوع مقاله: مقاله پژوهشی

تاریخ دریافت: ۱۴۰۲/۵/۲۲
تاریخ بازنگری: ۱۴۰۲/۷/۱۸
تاریخ پذیرش: ۱۴۰۲/۹/۱۰
تاریخ انتشار آنلاین: ۱۴۰۳/۷/۸

واژه‌های کلیدی:
الگوی رفتاری،
امنیت اطلاعات،
تهدیدات سایبری،
آینده پژوهی،
فراترکیب.

چکیده

هدف: بیشتر تحقیقاتی که در زمینه امنیت سیستم‌های اطلاعاتی صورت گرفته، بر عوامل فنی پرداخته شده، ولی راه‌کارهای امنیت اطلاعات در مواجه 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 مواجه با تهدیدات سایبری نوظهور می‌پردازد.

روش پژوهش: ابتدا در مرحله کیفی از روش فراترکیب، جهت استخراج شاخص‌ها از منابع و سؤال‌های پژوهش استفاده شد و در مرحله کمی با کمک خبرگان و روش دلفی دو مرحله ای، 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.

یافته‌ها: از۱۱۲منبع،۱۴۲ شاخص استخراج و با کمک خبرگان اعتبارسنجی و پالایش شد. در مرحله اول و دوم دلفی۱۷ 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 دریافت۱۱۱ پاسخنامه از سوی کارشناسان امنیت اطلاعات و بررسی پایایی آنها، الگوی رفتاری مناسب پژوهش احصاء گردید.

نتیجه‌گیری: براساس وزن بعدها و مؤلفه‌های پژوهش، بعد«تهدیدات امنیتی» مؤلفه«خسارت‌های غیرعمدی» بیشترین وزن و بعد «عوامل فنی» مؤلفه «برنامه ریزی» و «پایش» کمترین وزن را داشته‌اند.

استناد: محمداسماعیل، ص.، رایین آبرومند، م.، مطلبی، د. (۱۴۰۲). بهبود الگوی رفتاری کارشناسان امنیت اطلاعات در مواجه با تهدیدات سایبری با رویکرد آینده پژوهی. *دانش‌شناسی*، ۱۶ (۶۱)، ۱۲۴-۱۰۱.

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 می شوند (پیوتو و همکاران[1]، ۲۰۲۱) و قابلیت اطمینان آن بسیار حائز اهمیت است. این پارادایم مبتنی بر استفاده از فناوری‌های توانمندکننده ویژه است. باتوجه 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[2]، 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[3] درمورد نقض داده‌ها ادعا می کندکه 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 می کند که شامل ارائه آموزش به کارکنان و استفاده از سناریوهای شبیه سازی برای شناسایی کمپین‌های مهندسی اجتماعی و فیشینگ است (کورالو[4]، 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 به‌نفس بیشتری پیدا کنند (لی و همکاران[5]، ۲۰۱۹). تحلیل دیتا و داده‌کاوی در عصر فناوری کمک شایانی به مدیریت مؤثر و پاسخ‌گویی به تهدیدات و مخاطرات در حوزه سایبری کرده‌است. به طورکلی داده‌کاوی 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 افزاری‌هایی مانند SPSS ، MATLAB و RapidMiner استفاده می‌شود، همچنین تکنیک‌های داده-کاوی را می‌توان برای تجزیه و تحلیل روی داده‌های ساخت‌یافته، غیرساخت‌یافته اعمال کرد. باید توجه داشت که الگوها از تجزیه تحلیلی که بر روی داده‌ها صورت می‌گیرد به دست می آیند، (وو و یانگ[6]، ۲۰۲۳) و آینده پژوهی مجموعه تلاش‌هایی است که با نگاهی به آینده بر منابع، الگوها و روند حال و گذشته می پردازد. 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 آیندهٔ محتمل است (بنگستون[7]، ۲۰۱۸). جیم دیتور[8]، 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[9] (۲۰۲۲) در زمینه رفتار متخصصین امنیت اطلاعات در کشور چین، با استفاده از ۸۰۴ پرسش نامه و تحلیل عاملی و نتایج حاصله نشان می دهد 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 پیش‌بینی‌کننده 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[1] (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 سه‌کشور اسلوونی، 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. یافته های مطالعه همچنین نشان می دهد 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 بیبو[2] (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 داده ها، 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 سازمان ها، 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 برمطالعات 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 آگاه سازی، 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[3] , افندی[4], و آفرینا[5] ۲۰۲۱) نشان دهنده اهمیت آموزش و آگاه‌سازی است.

---

[1]. Moti Zwilling
[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 ارزیابی های 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 پیاده سازی 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[1] 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 حسابرسی، کاهش ریسک های فنی، مالی، حقوقی و قضایی امنیت فضای تبادل اطلاعات، جلوگیری از حملات و دسترسی‌های غیرمجاز ناشی از عدم رعایت مسائل امنیتی، مهار خسارت های ناشی از ناامنی، تأمین محرمانگی، صحت و قابلیت دسترسی برای ارتباطات، اطلاعات، نرم افزارها و سخت افزارها همگی از مزایای پیاده سازی سیستم مدیریت امنیت اطلاعات (ISMS) به شمار می‌روند و سازمان‌ها را برآن می‌دارند تا اقدام به ایجاد این سیستم نمایند (ایلداریم[2]، 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 مواجه 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 سئوال 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 نامرتبط مشخص شوند و اسنادی که موضوع پژوهش را کامل پوشش می‌دهند به عنوان اسناد مرتبط انتخاب شوند. در (شکل۱) می‌توان خلاصه‌ای از فرایند ارائه شده را همراه با نتایج به دست آمده از پژوهش حاضر مشاهده کرد.

---

[1]. سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور

[2]. Yildirim, et al

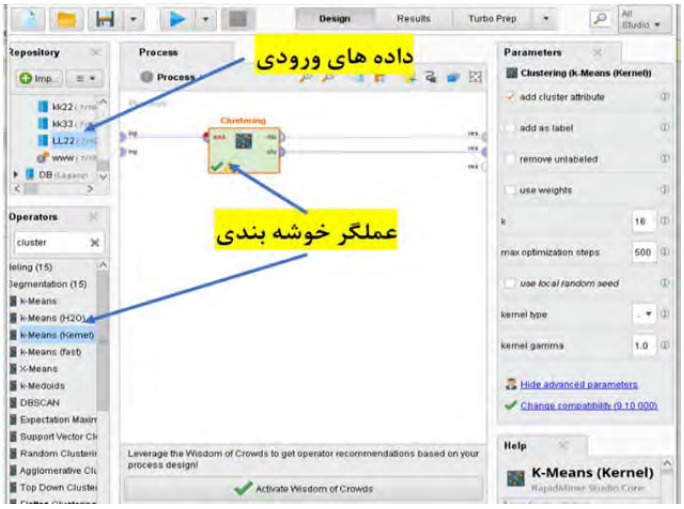
شکل ۱. فرایند نتایج جستجو و انتخاب اسناد مناسب در پژوهش حاضر

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 تحلیل های صورت گرفته به کمک روش فراترکیب در گام اول کدهای مشترک و شاخص های الگوی رفتاری در مواجهه با تهدیدات امنیتی و سایبری از پیشینه پژوهش شناسایی و استخراج شد. شاخص‌های امنیتی استخراج شده در اکثر مستندات برگرفته از خانواده استانداردهای بین المللی سیستم مدیریت امنیت اطلاعات می‌باشدکه از جنبه‌های مختلف از نگاه پژوهشگران مورد ارزیابی قرار گرفته است. در این مرحله تعداد ۱۴۲ شاخص می‌تواند با شاخص های الگوی رفتاری کارشناسان امنیت اطلاعات در مواجه با تهدیدات سایبری و امنیتی مطابقت داشته باشد. بنابر کیفی بودن ماهیت پژوهش حاضر، برای انتخاب نمونه آماری و تعیین حجم نمونه (تعداد خبرگان مشارکت کننده) از روش نمونه گیری گلوله برفی، برای تعیین افراد مشارکت کننده 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 واحد های 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 دعوت نامه‌ای 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 داده محور و کارشناسان امنیت اطلاعات تهیه شد که پس از فیلتر شدن با معیار حداقل ۵ سال سابقه‌کار مرتبط برای کارشناسان امنیت اطلاعات، جامعه آماری پژوهش در این مرحله به تعداد ۱۵۶ نفر مشارکت کننده رسید، با استفاده از فرمول کوکران[1] حداقل حجم نمونه برابر۱۱۱ نفر محاسبه گردید ولی پرسشنامه‌ها به هر ۱۵۶ نفر ارسال و پس از دریافت ۱۱۱ پرسشنامه تکمیل شده ، فرایند تحلیل آغاز شد.

[1]. Cocharan



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 می بایست توانایی خوشه‌بندی متن را داشته باشد و همچنین با توجه فراوانی شاخص‌ها درخوشه-بندی‌های شکل گرفته ، شاخص‌های پرت را تشخیص دهد، با درنظرگرفتن 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 ۱۶مولفه 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 قرارگرفت. پس از تحلیل پاسخ پرسشنامه، شاخص‌ها ارزش‌گزاری شده و شاخص‌های خارج از ارزش‌گزاری در لیست حذف قرار گرفت. ملاک ارزش‌گزاری شاخص‌ها پارامتر CVR و CVI 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[1] 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 ۱۴۲به ۱۲۵ شاخص کاهش یافت.

جدول ۱. ارزیابی و تحلیل ۱۴۲ شاخص و ١٦ مولفه در پرسشنامه مرحله اول و دوم دلفی

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

[1] T -Test یا آماره‌ی تی برای مقایسه نسبت دو نمونه جمع‌آوری شده از دو گروه مختلف می باشد که از رابطه زیر پیروی می کند 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 آماره‌ی T می باشد. همچنین سطح معنی‌داری میزان خطای پذیرفته شده می‌باشدکه در این پژوهش خطا صفر در نظر گرفته شده است.

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

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

	q22	سرقت هویت(حساب)/کلاه برداری	16	0/0000	100%	100%	تایید
	q23	دریافت پست الکرونیکی ناخواسته (هرزنامه)	10/583	0/0000	100%	100%	تایید
	q24	انسداد سرویس	16	0/0000	100%	100%	تایید
	q25	اجرا(تزریق) کد/نرم افزار/فعلیت مخرب	10/247	0/0000	93%	87%	تایید
	q26	مهندسی اجتماعی	12/475	0/0000	100%	100%	تایید
	q27	دست کاری سخت افزار و نرم افزار	11/225	0/0000	100%	100%	تایید
	q28	دست کاری اطلاعات	12/475	0/0000	100%	100%	تایید
	q29	سوء استفاده از ابزارهای ممیزی	8/29	0/0000	93%	87%	تایید
	q30	نصب و راه اندازی غیر مجاز نرم افزار	16	0/0000	100%	100%	تایید
	q31	سوء استفاده از اطلاعات محرمانه	11/225	0/0000	100%	100%	تایید
	q32	فعالیت مخرب از راه دور	12/475	0/0000	100%	100%	تایید
	q33	حملات هدفمند	11/22حذف5	0/0000	100%	100%	تایید
	q34	جستجوی جامع	-1	0/3340	60%	20%	حذف
تهدیدات قانونی	q35	استفاده غیر مجاز از منابع حفاظت شده	11/225	0/0000	100%	100%	تایید
	q36	سوء استفاده از داده های خصوصی	-1/468	0/1640	53%	7%	حذف
دسترسی فیزیکی غیرمجاز (عمدی/سهوی)	q37	ضعف در آموزش کارکنان	16	0/0000	100%	100%	تایید
	q38	احراز هویت ناکارآمد.	12/475	0/0000	100%	100%	تایید
	q39	قابلیت خواندن حافظه دردستگاه قابل حمل	8/264	0/0000	93%	87%	تایید
ضعف در نگهداری منابع اطلاعاتی	q40	مدیریت خطا به شیوه نادرست	10/717	0/0000	100%	100%	تایید
	q41	امکان تغییر در اطلاعات سامانه	10/717	0/0000	100%	100%	تایید
	q42	تفویض اختیار ناکارآمد	12/475	0/0000	100%	100%	تایید

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

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

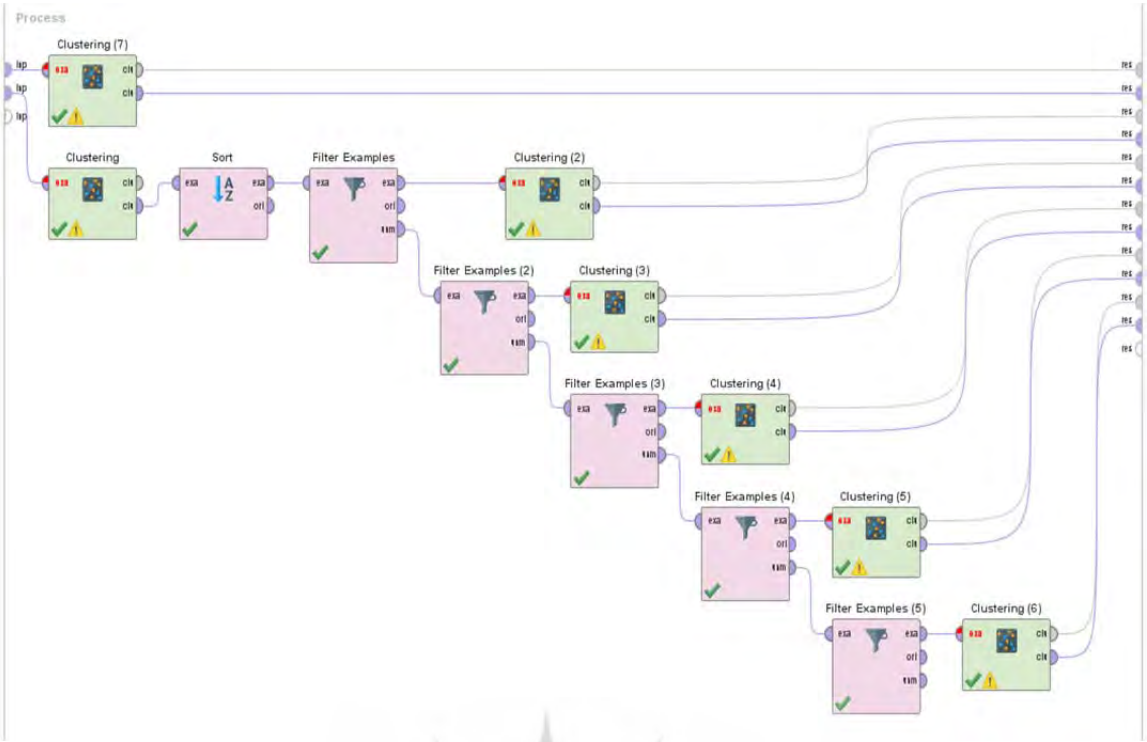
	امنیتی در سطح سازمان						
q78	تعهد و وفاداری کارمندان به سازمان	5/123	0/0000	87%	73%	تایید	
q79	غربالگری و ارزیابی دوره ای کارمندان	11/225	0/0000	100%	100%	تایید	
q80	تعریف کاربری های مجاز و حقوق دسترسی	11/225	0/0000	87%	73%	تایید	
q81	فرهنگ سازی برنامه های امنیتی سازمان	12/475	0/0000	100%	100%	تایید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

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

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

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

جهت خوشه‌بندی و احصاء ابعاد و مؤلفه‌های نهایی پژوهش، به کمک نرم افزار رپیدماینر 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.



شکل۳. اجرای خوشه‌بندی طبقه‌ای در رپیدماینر

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

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

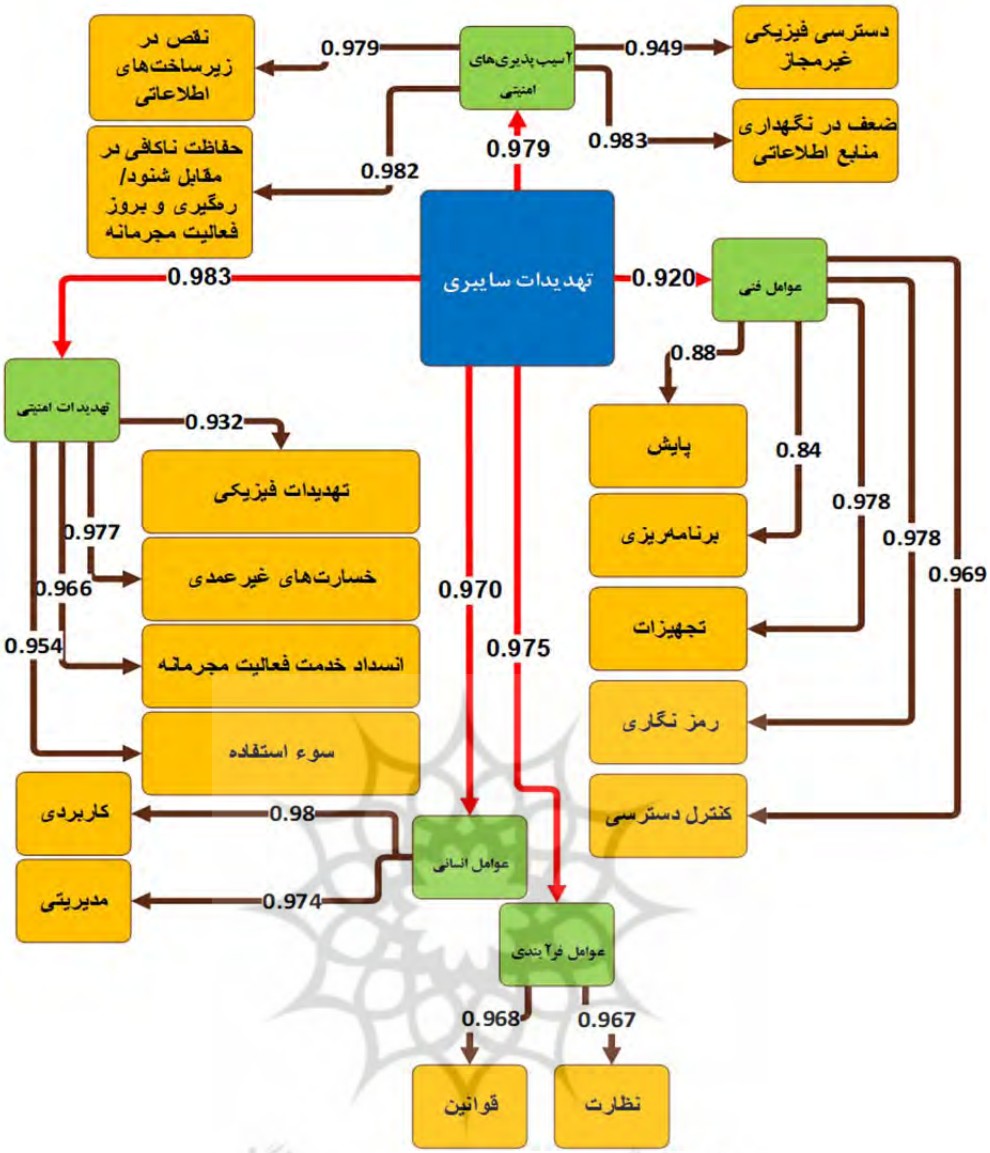
ابعاد	مؤلفه
آسیب‌پذیری‌های امنیتی	حفاظت ناکافی در مقابل شنود/ره‌گیری و بروز فعالیت مجرمانه
	دسترسی فیزیکی غیرمجاز
	ضعف در نگهداری منابع اطلاعاتی
	نقص در زیرساخت‌های اطلاعاتی
تهدیدات امنیتی	انسداد خدمت فعالیت مجرمانه
	تهدیدات فیزیکی
	خسارت‌های غیرعمدی
	سوء استفاده
عوامل انسانی	مدیریتی
	کاربردی
عوامل فرایندی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

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

در این مرحله پاسخ‌ها به کمک نرم‌افزارهای MATLAB و SPSS مورد تجزیه‌وتحلیل 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[1] 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.

[1] Lambda

بار عاملی یا لامبدا۱ در حقیقت یک ضریب همبستگی بین متغیر های پنهان و متغیر های آشکار است. این ضریب تعیین می کند 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 ٤. 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 لزوما برای مقابله با تهدیدات سایبری کافی نیستند. با بررسی مشخصه‌های مؤلفه «تهدیدات امنیتی»، مطابق پارامتر بار عاملی مرتبه دوم مشخصه «خسارت‌های غیر عمدی» قوی ترین وزن را دارد و این نتیجه بیانگر این موضوع می باشدکه 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 درنظرگرفتن 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 می گردد:

- 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 ره گیری 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.

❖ بر اساس داده‌های پژوهش در خصوص «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 خط مشی‌های امنیت اطلاعات سازمان؛
- پرورش حس پاسخگویی، خود ارزیابی و خود گزارش‌دهی؛
- هم‌سو کردن مدیریت عالی به منظور حمایت از برنامه‌ها، پروژه‌ها و خط مشی‌های 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 امنیت؛
- تدوین و اجرای برنامه‌های آموزشی در حوزه امنیت اطلاعات (تکنیک‌های نفوذ، هک، اخلاقیات، قوانین و مقررات، ممیزی و)؛

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

- به‌کارگیری 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 قابل‌حمل سازمانی و سامانه‌ها؛
- استفاده از پویشگرها 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؛
- محدودکردن 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 به‌کارگیری 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 فضاهای 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 دسترس پذیری و ظرفیت حافظه پشتیبان؛
- تدوین اصول پایش و کنترل کاربران؛
- بررسی مداوم صحت، محرمانگی و دسترس 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 وبه روزرسانی منظم قوانین و خط مشی‌های 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؛
- عایت اصول طبقه‌بندی داده‌ها و منابع اطلاعاتی؛
- ایجاد رویه‌های تشخیص، گزارش‌دهی و پاسخ به رخداد و استفاده از چک لیست‌های امنیتی؛
- تعیین راهبردها در صورت عدم پیروی از خط مشی‌های 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» مجددا بررسی گردید و هر شاخصه و عامل پیشگیری کننده از آن شاخصه بصورت ضمنی در جدول (۳) اشاره شد که برآورد می‌گردد تمام این شاخصه ها به کمک آموزش، بازآموزی و آگاه‌سازی قابل پیشگری هستند و این موضوع بیانگر اهمیت آموزش، بازآموزی و آگاه‌سازی در حیطه امنیت اطلاعات می باشد.

جدول ۳. بررسی شاخص‌های خسارت‌های غیر عمدی

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

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[1]" (دانینگ[2] ۲۰۱۱) و "توهم بوقلمون[3]" 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 زننده 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 درکمین 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

- برگزاری دوره‌های عمومی، تخصصی و کارگاه های مهارت‌افزایی در حوزه امنیت سایبری برای متخصصین و جامعه هدف آموزشی سازمان با استفاده از ظرفیت مراکز دارای پروانه و استادان مجرب؛
- اخذ گواهی آموزش از مراکز دارای پروانه ارائه خدمان آموزشی (افتا) برای کلیه شرکت‌کنندگان در دوره‌های آموزشی؛
- برگزاری همایش‌های عمومی به منظور ارتقای فرهنگ امنیت سایبری در سازمان و آگاهی عموم کارکنان از تهدیدات سایبری ویژه کسب و کار سازمان؛
- ارائه سازو کار به منظور اشتراک‌گذاری اطلاعات، تجارب و دانش امنیت سایبری در سازمان؛

---

[1]. Dunning–Kruger

[2]. Dunning

[3]. اولین بار توسط برتراند راسل معرفی شد: بوقلمونی که برای روز شکرگزاری تعیین شده است، هر روز تغذیه و مراقبت می شود تا زمانی که ذبح شود. با هر تغذیه، اطمینان یا اعتمادبه نفس آن که هیچ اتفاقی برای ان 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. بااین‌حال، ان روز توسط همان کسی که از او مراقبت می‌کرد، کشته می‌شود.

- ارائه سازو کار به منظور اطلاع رسانی و آگاهی رسانی به جامعه هدف سازمان و نهادینه سازی امنیت در فرآیندهای کاری کارکنان؛
- پایش و اطلاع‌رسانی اخبار تهدیدات، آسیب‌پذیری‌ها و حوادث سایبری در حوزه کسب و کار سازمان به صورت مستمر؛
- ارزیابی دوره‌ای 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 روش‌های مقابله با حملات جعل در ارتباطات شبکه‌های خودرویی. *نشریهفناوری اطلاعات و ارتباطات انتظامی*، ۳(۱۱)، ۴۱

دی پیر, م. (۱۴۰۱). ارائه معیاری برای محاسبه خطر امنیتی لینک‌ها برای جلوگیری از کلاهبرداری‌های اینترنتی. *فصلنامه فناوری اطلاعات و ارتباطات انتظامی*، ۳(۱۱)، ۲۳

رجبی، ف. وحاجیه علیپور, ع. (۱۴۰۱). تاثیر اجرای خط‌مشی‌گذاری عمومی بر فرهنگ سازمانی .*نشریه خط‌مشی‌گذاری عمومی در مدیریت* ، ۱۳(۴۵)، ۱۰۳-۱۲۱

شعبانی، م.، رفعتی‌اصل, 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)، ۳۱۵-۳۵۳.

کریمی, ز. و پیکری. ح.ر. (۱۳۹۸). مدیریت امنیت اطلاعات: تاثیر تعهد سازمانی و عواقب ادراک‌شده افشای اطلاعات محرمانه بر قصد نقض امنیت اطلاعات بیماران. *اخلاق پزشکی*, ۴۴(۱۳), ۲۰-۲۹.

منصوری،ع. و جعفری، ع .(۱۳۹۴). نقش آموزش‌های 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 رشنوادی, ی. (۱۳۹۹). شناسایی و تبیین راهبردهای ترفیع در رسانه‌های اجتماعی (مورد مطالعه: اینستاگرام) .*تحقیقات بازاریابی نوین. مجله تحقیقات بازاریابی نوین*، ۱۰(۳).

حبیبی، آ. و سرآبادانی، م. (۱۴۰۱). *آموزش کاربردی SPSS . انتشارات نارون*.

کمائی، 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 1401 شماره ۱۷*

مصلح شیرازی، ع.، محمدی،ع .، رعنایی، ح.، و هنرپروران، ح. (۱۳۹۶). طراحی مدل پویاشناسی سیستم برای سیاستگذاری ارتقای شاخص‌های 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 سازمان‌ها . *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.FutureInternet,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 peformance 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)