

Qualitative Analysis of the Behavioral Pattern of Information Security Experts in Facing Cyber Threats

MohammadBagherRaenAbromand^{ID}

Ph.D. Student, Department of Knowledge and Information Science, Science and Research Branch, Islamic Azad University, Tehran, Iran. ITmanager@tsfc.ir

Sedigheh MohammadEsmail^{ID}

Associate Professor, Department of Knowledge and Information Science, Science and Research Branch, Islamic Azad University, Tehran, Iran (**Corresponding author**). Sm.esmaili2@gmail.com

Dariush Matlabi^{ID}

Associate Professor, Department of Educational Sciences, Yadgar Imam Khomeini Shahrari Branch, Islamic Azad University, Tehran, Iran. dariushmatlabi@yahoo.com

Abstract

Purpose: Simultaneously with the developments of the 20th century and the process of globalization in the present era, information and communication technology has facilitated the emergence of a networked society. The new world has evolved into a network whose primary structure is information and electronic communication systems. The transformation of social interactions into virtual communities has led to the rise of social insecurity and new forms of crimes and misdemeanors in virtual spaces. Gradually, with the expansion of information and communication technology, especially the Internet, and subsequently the proliferation of threats and risks associated with it, the concepts of information security, information systems security, and cyber security were also developed. Just as soldiers are trained to handle various threats in war, the world of information is a real battlefield, with hackers and cyber-attacks posing significant risks. Information security experts should be equipped with the necessary skills to effectively deal with cyber-attacks, much like expert soldiers. The current applied developmental research is focused on identifying key indicators to design effective behavioral patterns for information security experts dealing with cyber threats.

Method: In this study, a purposeful and development-oriented approach was employed, using a meta-composite and qualitative-quantitative (sequential-exploratory) method. Initially, 112 sources were selected from 270 primary sources using a library method and were the focus of the work. To identify the security components of information systems, the Barroso and Sandlowski 2007 seven-step technique was utilized, resulting in the calculation of 142 indicators from the selected documents. After clustering the indicators using RapidMiner software, the research identified 5 dimensions and 17 components. Subsequently, a two-stage Delphi method involving two groups of 15 experts was employed to evaluate the questions, value assessment, and validity. Following the completion of the qualitative phase, the study progressed to the quantitative or exploratory stage. An invitation letter and questionnaire, comprising 125 verified indicators, were then prepared and sent to 156 information security experts. And after receiving 111 complete questionnaires, which meets Cochran's requirement

<https://doi.org/10.22091/STIM.2023.9205.1933>

Received: 2022-11-12 ; **Revised:** 2023-02-16 ; **Accepted:** 2023-02-24 ; **Published online:** 2023-12-23

© The Author(s).

Article type: Research Article

Published by: University of Qom.



for a minimum statistical population size of 111 people, the questionnaire collection phase concluded, and the analysis process commenced with the assistance of SPSS and MATLAB software.

Findings: In this study, the dimension of "security threats" has the highest factor load weight of 0.983 among all other dimensions. Within the "security threats" dimension, the component of "unintentional damages" has the highest weight compared to other components. The dimension of "security vulnerabilities" follows with a factor load weight of 0.979, ranking second. The "process factors" dimension ranks third with a factor load weight of 0.975, and the "human factors" dimension also has a factor load weight of 0.975. The fourth rank is held by the dimension of "0.970," and finally, the "technical factors" dimension, with a factor loading of 0.920, ranks last among the dimensions of this research. Despite receiving the lowest score and weighting overall, the "technical factors" dimension has the highest factor load weight assigned to the components of "encryption" and "equipment," with a score of 0.978, and the lowest score assigned to the components of "monitoring" with a weight of 0.88 and "planning" with a weight of 0.84. In the following, the obtained results and prioritizations were compared with those of other studies, and the validity of the results was confirmed based on the validation and verification of the comparisons.

Conclusion: In general, it should be noted that, contrary to the opinion of most data-oriented companies that prioritize "technical factors" in information security, the results obtained in this study have shown that this assumption was incorrect. The importance of the behavioral patterns of information security experts has been confirmed, which is influenced by laws, organizational structure, organizational culture, and training. Finally, with the assistance of the weights assigned to the obtained components and indicators, suggestions were made to modify the behavioral patterns of information security experts after ranking and prioritizing the components and characteristics.

Keywords: Information Security, Behavioral Pattern, Cyber-Attacks, Cyber Threats, Hybrid Method, Delphi Method, Data Mining.



تحلیل کیفی الگوی رفتاری کارشناسان امنیت اطلاعات در رویارویی با تهدیدات سایبری

محمدباقر رایین آبرومند ^{id}

دانشجو دکتری، گروه علم اطلاعات و دانش‌شناسی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران.
ITmanager@tsfc.ir

صدیقه محمداسماعیل ^{id}

دانشیار، گروه علم اطلاعات و دانش‌شناسی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران (نویسنده
مسئول). Sm.esmaili2@gmail.com

داریوش مطلبی ^{id}

دانشیار، گروه علوم تربیتی، واحد یادگار امام خمینی شهری، دانشگاه آزاد اسلامی، تهران، ایران.
dariushmatlabi@yahoo.com

چکیده

هدف: همزمان با تحولات قرن بیستم و فرایند جهانی‌شدن در عصر حاضر، فناوری اطلاعات و ارتباطات، امکان ظهور جامعه شبکه‌ای را فراهم آورده است. جهان جدید به‌صورت شبکه‌ای درآمده که بافت اصلی آن را اطلاعات و نظام ارتباطات الکترونیک تشکیل می‌دهد. تغییر ماهیت مراودات اجتماعی به شکل جوامع مجازی، باعث پیدایش نوعی ناامنی اجتماعی و جرایم و بزهکاری‌های جدید در فضاهای مجازی شده است. به‌تدریج با گسترش فناوری اطلاعاتی و ارتباطی، به‌ویژه اینترنت و متعاقباً گسترش نوع تهدیدات و مخاطرات مرتبط با آن، مفاهیم امنیت اطلاعات، امنیت سیستم‌های اطلاعاتی و امنیت سایبری نیز توسعه یافت. همانگونه که در جنگ، به سربازان رفتار صحیح مقابله با انواع خطر را آموزش می‌دهند، دنیای اطلاعات با وجود هکرها^۱ و حملات سایبری، یک میدان جنگ واقعی است و کارشناسان امنیت اطلاعات می‌بایست همانند یک سرباز خبره، رفتار صحیح مقابله با حملات سایبری را بشناسند. پژوهش کاربردی- توسعه‌ای حاضر، با رویکرد رسیدن به شاخص‌های اساسی برای طراحی الگوی رفتاری صحیح کارشناسان امنیت اطلاعات در مواجهه با تهدیدات سایبری انجام شده است.

روش: در این پژوهش با هدف و رویکرد کاربردی- توسعه‌ای، به کمک روش فراترکیب و کیفی- کمی (متوالی- اکتشافی)، ابتدا به روش کتابخانه‌ای، از ۳۷۰ منبع اولیه، ۱۱۲ منبع غربال شده و به‌عنوان محور کار قرار گرفت، و به‌منظور

استناد به این مقاله: بختیاری، رایین آبرومند، محمدباقر؛ محمداسماعیل، صدیقه؛ مطلبی، داریوش (۱۴۰۲). تحلیل کیفی الگوی رفتاری کارشناسان امنیت اطلاعات در رویارویی با تهدیدات سایبری. *علوم و فنون مدیریت اطلاعات*، ۹(۴): ۴۱۹-۴۵۷.

<https://doi.org/10.22091/STIM.2023.9205.1933>

تاریخ دریافت: ۱۴۰۱/۰۸/۲۱؛ تاریخ اصلاح: ۱۴۰۱/۱۱/۲۷؛ تاریخ پذیرش: ۱۴۰۱/۱۲/۰۵؛ تاریخ انتشار آنلاین: ۱۴۰۲/۱۰/۰۲

ناشر: دانشگاه قم

نوع مقاله: پژوهشی

© نویسندگان.

۱. نفوذگرها



شناسایی مؤلفه‌های امنیت سیستم‌های اطلاعاتی، از تکنیک هفت مرحله‌ای باروسو^۱ و ساندلوسکی^۲ (۲۰۰۷) استفاده شده است. ۱۴۲ شاخص از اسناد غربال شده احصاء گردید و پس از خوشه‌بندی شاخص‌ها به کمک نرم‌افزار ریپید ماینر، ابعاد و مؤلفه‌های پژوهش مشتمل بر ۵ بعد و ۱۷ مؤلفه استخراج شد. سپس به کمک روش دلفی دومرحله‌ای، با استفاده از دو گروه ۱۵ نفره از خبرگان، سؤالات، ارزش‌سنجی و روایی‌سنجی شده و پس از اتمام بخش کیفی، وارد مرحله کمی یا اکتشافی شده و یک دعوتنامه و پرسش‌نامه با ۱۲۵ شاخص تأیید شده، آماده گردید و برای ۱۵۶ کارشناس امنیت اطلاعات ارسال شد. با دریافت ۱۱۱ پرسش‌نامه کامل، به دلیل اینکه مطابق رابطه کوکران، حداقل حجم جامعه آماری برابر ۱۱۱ نفر است، جمع‌آوری پرسش‌نامه‌ها پایان یافت و فرایند تحلیل به کمک نرم‌افزارهای اس.پی.اس.اس.^۳ و متلب^۴ آغاز شد.

یافته‌ها: در این پژوهش بعد «تهدیدات امنیتی» با وزن ۰٫۹۸۳، بالاترین وزن بار عاملی را از بین سایر ابعاد داشته و مؤلفه «خسارت‌های غیرعمدی» از میان سایر مؤلفه‌های بعد «تهدیدات امنیتی»، بالاترین وزن را داشته است. «آسیب‌پذیری‌های امنیتی» با وزن بار عاملی ۰٫۹۷۹، رتبه دوم، «عوامل فرایندی» با وزن بار عاملی ۰٫۹۷۵، رتبه سوم، بعد «عوامل انسانی» با وزن بار عاملی ۰٫۹۷۰، رتبه چهارم، و در نهایت بعد «عوامل فنی» با وزن بار عاملی ۰٫۹۲۰، رتبه آخر را به خود اختصاص داده است. باوجود اینکه بعد «عوامل فنی» در مجموع پایین‌ترین امتیاز و وزن‌دهی را کسب کرده است؛ ولی در همین بعد، بالاترین وزن بار عاملی را مؤلفه‌های «رمزنگاری» و «تجهیزات» با امتیاز ۰٫۹۷۸، به خود اختصاص داده و پایین‌ترین امتیاز را مؤلفه‌های «پایش» با وزن ۰٫۸۸ و «برنامه‌ریزی» با وزن ۰٫۸۴، به خود اختصاص داده است.

نتیجه‌گیری: برخلاف پنداشت اکثر شرکت‌های داده‌محور مبنی بر اینکه بعد «عوامل فنی» را رتبه اول در امنیت اطلاعات می‌پندارند؛ ولی از نتایج به‌دست آمده این پنداشت نقض گردید و اهمیت الگوی رفتاری کارشناسان امنیت اطلاعات احراز شد که ناشی از قوانین، ساختار سازمانی، فرهنگ سازمانی و آموزش است. در نهایت، به کمک وزن مؤلفه‌ها و شاخص‌های به‌دست آمده، پس از رتبه‌بندی و اولویت‌بندی مؤلفه‌ها و مشخصه‌ها، پیشنهادهایی برای اصلاح الگوی رفتاری کارشناسان امنیت اطلاعات ارائه شد.

کلیدواژه‌ها: امنیت اطلاعات، الگوی رفتاری، حملات سایبری، تهدیدات سایبری، روش فراترکیب، روش دلفی، داده‌کاوی، تحلیل کیفی، تهدیدات امنیتی.

۱. مقدمه

دنیای دیجیتال، از کوچک‌ترین خانه‌های شهرهای کوچک تا بزرگ‌ترین شرکت‌ها را دربرگرفته و به فرهنگ تبدیل شده است و هر فرهنگی رفتار مختص به خود را می‌طلبد. همه ما از افراد معمولی جامعه تا متخصصان امنیت اطلاعات، به گونه‌ای درگیر فرهنگ دنیای دیجیتال هستیم. از بارزترین نمونه این درگیری، انواع کلاهبرداری‌های اینترنتی از جمله فیشینگ^۱ می‌باشد که اگر رفتار صحیح مواجهه با حملات سایبری فیشینگ را ندانیم، در چشم‌به‌هم‌زدنی، به گروه عظیم مال‌باختگان اینترنتی خواهیم پیوست. اینترنت اشیاء در حال تبدیل شدن به یک عنصر کلیدی از اینترنت آینده و یک زیرساخت حیاتی ملی و بین‌المللی است (شاهینی و همکاران، ۱۴۰۱). بنابراین، الگوی رفتاری صحیح کارشناسان امنیت اطلاعات می‌تواند از درز و نشر اطلاعات جلوگیری کرده و از خسارات متعاقب آن جلوگیری کند.

امروزه، سازمان‌ها با محیطی متلاطم و ناآرام روبرو هستند و خطرات محیطی، از هر سو حیات و بقای آن‌ها را مورد هجوم قرار می‌دهد. در چنین شرایطی امکان حضور و دوام در صحنه فعالیت‌ها مستلزم این است تا سازمان‌ها جایگاه فعلی خود را شناخته و باتکیه بر نقاط قوت خود، از فرصت‌های محیطی استفاده کرده و خود را برای مقابله با تهدیدها و مخاطرات آماده نمایند. فقدان روال صحیح حفاظت از اطلاعات می‌تواند نتایج مخربی به بار آورد. بنابراین، ضرورت توجه به امنیت اطلاعات و مدیریت امنیت اطلاعات بیش از پیش احساس می‌شود (Pathari & Sonar, 2012).

به گزارش شرکت پی.سی.اچ. تکنولوژی^۲ در سایت رسمی خود، هزینه‌ای که شرکت‌های بزرگ برای امنیت سایبری پرداخت می‌کنند در سال ۲۰۲۰ تا ۵ میلیارد دلار در سال عنوان شده و این رقم برای شرکت‌های کوچک تا ۵۰۰ هزار دلار در سال کاهش پیدا می‌کند. این ارقام در کنار تحقیقاتی که نشان می‌دهد، حدود ۷۰٪ از تقلب‌ها توسط خودی‌ها و نه توسط مجرمان خارجی انجام می‌شود، اما ۹۰٪ از کنترل‌های امنیتی و نظارت بر تهدیدات خارجی متمرکز است (Colwill, 2009)، این نکته را روشن می‌کند که شرکت‌ها میلیاردها دلار برای مقابله با تهدیدات سایبری خارج از شرکت خرج می‌کنند؛ در صورتی که حدود ۷۰ درصد از زیان‌های ناشی از تهدیدات کاملاً به الگوی رفتاری ناصحیح کارشناسان امنیت اطلاعات بازمی‌گردد. این موضوع نشان‌دهنده خطای ساختاری و فرهنگ سازمانی ناصحیح بوده و بیانگر آن است که همچنان نیاز به اصلاح خط‌مشی و تصحیح ساختار سازمانی احساس می‌شود. از سوی دیگر، تصمیم‌گیری فرایندی بسیار مهم و پایه‌ای در فعالیت‌های

<http://stun.gom.ac.ir>

1. Phishing
2. PCHtechnologies

مدیران است که اساس آن به دست آوردن و پردازش اطلاعاتی می باشد که باید سه صفت محرمانگی، صحت و در دسترس بودن را داشته باشد، در غیر این صورت خسارات بزرگی برای سازمان به بار می آید.

استدلال می شود که توسعه فرهنگ امنیت اطلاعات متعاقباً به یک سازمان امن منجر خواهد شد. با این حال، مطالعات محدودی برای درک فرهنگ امنیت اطلاعات انجام شده است. فرهنگ ایده آل یا قوی امنیت اطلاعات می تواند در به حداقل رساندن تهدید انسان ها به حفاظت از اطلاعات و در نتیجه کمک در کاهش نقض داده ها یا حوادث در سازمان ها کمک کند. تقریباً همه سازمان ها اطلاعات حساس را به شکلی جمع آوری و نگهداری می کنند. برخی از سازمان های دولتی کنترل های نظارتی بر استفاده و توزیع انواع خاصی از اطلاعات حساس ایجاد کرده اند. برخی از سازمان های جنایی با مهارت های فنی پیشرفته سازمان دهی می شوند و مصمم هستند که به طور غیرقانونی انواع خاصی از اطلاعات حساس را برای سود خود به دست آورند. خطرات مرتبط با از دست دادن اطلاعات حساس، یک نگرانی بسیار واقعی برای سازمان های امروزی است. اگر اشتباهی در الگوی رفتاری یا استانداردهای اخلاقی یک کارشناس امنیت اطلاعات وجود داشته باشد، ممکن است منجر به از دست دادن شهرت یا کاهش مزیت رقابتی برای سازمان شود (AlHogail, 2015).

۲. بیان مسئله

امنیت اطلاعات مبحث بسیار مهمی است؛ زیرا هدف آن حفاظت از اطلاعات سازمان در برابر تهدیدها و ریسک ها، در دسترسی کاربران به اطلاعات امن، مطمئن و محرمانه است و برای اطمینان از امنیت آن، سازمان باید سیاست ها و خط مشی های امنیت اطلاعات را شناسایی و تبیین کند. شکست های مداوم امنیت اطلاعات در سازمان ها باعث تمرکز بیشتر بر فرهنگ سازمانی شده است. همچنین، یکی دیگر از نگرانی های بزرگ برای امنیت اطلاعات یک سازمان، رفتار کارکنان است؛ زمانی که برای سیاست امنیت اطلاعات ارزش قائل نیستند و از آن مهم تر رفتار کارشناسان امنیت اطلاعات می باشد. عدم رعایت سیاست های امنیتی سیستم های اطلاعاتی کارشناسان امنیت اطلاعات یک نگرانی عمده برای مدیران امنیت فناوری اطلاعات است. سازمان ها به سیاست ها و شیوه های امنیت اطلاعات برای ایجاد مدیریت مناسب و استفاده از اطلاعات حساس به منظور کاهش خطرات مرتبط نیاز دارند. سیاست های امنیت اطلاعات فقط به اندازه افرادی که باید آنها را اعمال کنند، مؤثر هستند (Niekerk & Solms, 2005). فرهنگ یک سازمان تأثیر زیادی بر ارزش ها، اسطوره ها، قهرمانان و نمادهای کارمندان دارد که برای کارمند معنا می بخشد (Deal & Kennedy, 1999). این امکان وجود دارد که سیستم ها و نمادهای ارزش فرهنگی بتوانند بر نگرش کارکنان نسبت به

سیاست‌های امنیت اطلاعات سازمان تأثیر بگذارند. در بسیاری از سازمان‌ها، خط‌مشی‌ها و رویه‌های سیستم امنیت اطلاعات دارای عنصری از انطباق کارکنان است که برای اطمینان از راه‌حل امن‌تر مورد نیاز است. این امر برای پاسخگویی به تهدیدات مداوم پیشرفته‌ای که دارایی‌های اطلاعاتی ارزشمند سازمان را هدف قرار می‌دهد، مورد نیاز است. هنگامی که یک روش حمله کشف و متوقف می‌شود، روش دیگری راه‌اندازی می‌گردد. ماهیت غیرقابل پیش‌بینی تهدیدات مداوم پیشرفته برای اطلاعات حساس سازمان، نیاز به راه‌حل‌های تطبیقی را معرفی می‌کند. وابستگی پذیرفته شده به پذیرش و انطباق کارشناسان امنیت اطلاعات با سیاست‌ها و رویه‌های امنیت اطلاعات سازمان نشان می‌دهد که نیاز به درک بهتر تأثیرات احتمالی بر پذیرش و انطباق کارکنان وجود دارد. در این راستا، هدف مطالعه حاضر رسیدن به رابطه‌ای معنی‌دار بین عوامل مؤثر در الگوی صحیح رفتاری کارشناسان امنیت اطلاعات و رفتار آنان نسبت به سیاست امنیت اطلاعات در مواجهه با تهدیدات امنیتی و سایبری می‌باشد.

۳. پیشینه پژوهش

باتوجه به گسترش استفاده از اینترنت، تبدلات اطلاعاتی و هزینه‌های صرف شده به‌منظور یکپارچگی اطلاعاتی، امروزه محث و مدیریت جابه‌جایی‌های اطلاعاتی و برخورداری از سامانه‌ی جامعی برای مدیریت امنیت اطلاعات، بیش‌ازپیش احساس می‌شود (شهریاری و همکاران، ۱۳۹۸). اکثر قریب به اتفاق سازمان‌ها در معرض انواع تهدیدات داخلی و خارجی خرابکاران اطلاعاتی هستند؛ تهدیداتی چون دستکاری اطلاعات مرجع، سرقت اطلاعات حیاتی و سرمایه‌های اطلاعاتی. در چنین شرایطی، عواملی مانند سرعت و قابلیت دسترسی بالا، اگر تحت کنترل نباشند، ممکن است باعث بروز آسیب‌پذیری شوند و سوءاستفاده افراد از آنها به نفوذ، خرابکاری و کلاهبرداری بیانجامد. علاوه بر این، مشکلات طبیعی و خطاهای غیرعمدی که توسط کاربران رایانه‌ای رخ می‌دهد، در صورت فقدان روال صحیح برای حفاظت از اطلاعات می‌تواند نتایج مخربی به بار آورد. بنابراین، ضرورت توجه به امنیت اطلاعات و مدیریت امنیت اطلاعات بیش‌ازپیش احساس می‌شود (Pathari & Sonar, 2012). در پژوهش آهانگر و همکاران (۱۴۰۱)، مشخص شد که مفاهیم «امنیت»، «امنیت اطلاعات»، «سیستم‌های اطلاعاتی»، «حریم خصوصی»، «اطلاعات»، «ارتباطات از راه دور»، «رمزنگاری»، «رمزگذاری»، «احراز هویت»، «امنیت سایبری»، «شبکه»، «پردازش ابری»، «حملات ضد امنیتی»، «کنترل دسترسی‌ها»، «سیستم‌های تشخیص نفوذ»، «پروتکل‌های امنیت»، «ریسک»، «مدیریت ریسک و چارچوب‌های آن»، و «قراردادها و توافقات سطح دسترسی»، از مهم‌ترین مفاهیم این شبکه و دارای بالاترین میزان

مرکزیت بینابینی در شبکه هستند. نحوه ارتباطات و پیوندهای درونی آن‌ها با یکدیگر از نوع مستقیم است.

سازمان‌ها به‌منظور کارآمدتر، مؤثرتر و پاسخگوتر شدن، به استفاده از شبکه‌ها و سیستم‌های اطلاعاتی مبتنی بر رایانه اهمیت می‌دهند. باین‌حال، استفاده از فناوری اطلاعات و ارتباطات، حوادث سوءاستفاده از رایانه را افزایش داده است. بررسی اخیر مؤسسه امنیت رایانه‌ای نشان داد که شرکت‌های مورد بررسی، ۱۲۴ میلیون دلار ضرر کرده‌اند. در انگلستان، کمیسیون حسابرسی، ضرر و زیان را در حدود ۲ میلیارد دلار برآورد کرد. در واقع تلفات به این بزرگی مستلزم توجه جدی به محل‌هایی است که امنیت اطلاعات براساس آن طراحی شده است (Dhillon & Backhouse, 2000). باین‌حال تامسون و همکاران در یافته‌های خود بیان می‌کنند که امنیت اطلاعات هم تکنولوژی و هم فرد را دربرمی‌گیرد (Thomson & Niekerk, 2012). به نظر می‌رسد، در گذشته، سازمان‌ها راه‌حل‌های فنی را پاسخ فوری به مشکلات امنیتی خود می‌دانسته‌اند، در حالی‌که موانع زیادی برای یک رویکرد فنی وجود دارد و حتی در نتایج به‌دست آمده در پژوهش شفيعی نیک‌آبادی و همکاران (۱۴۰۱)، به‌کارگیری سامانه مدیریت امنیت اطلاعات، موجب افزایش یکپارچگی فرایندهای سازمانی در زنجیره تأمین و از آن‌رو، موجب افزایش یکپارچه‌سازی زنجیره تأمین می‌شود و در نتیجه، موجب بهبود عملکرد زنجیره تأمین می‌گردد. این امر را می‌توان در بررسی رابطه یکپارچگی فرایندهای سازمانی بر میزان هماهنگی اطلاعات، جلوگیری از اشتباهات، و دقت و صحت اطلاعات در طول زنجیره تأمین مشاهده نمود. این نتایج بیانگر آن است که راه‌حل‌های فنی همچنان پاسخی سریع برای کاهش اشتباهات انسانی کارشناسان امنیت اطلاعات شناخته می‌شوند. باتاچاریا^۱ هم در تحقیقات خود اذعان دارد که عامل انسانی به‌عنوان پاشنه آشیل امنیت اطلاعات است (Bhattacharya & et al., 2011).

خطای انسانی بخش جدایی‌ناپذیر از امنیت اطلاعات است و راه‌حل‌های فنی، پاسخ کاملی به این مشکل نیست، و راه‌حل صحیح در تحقیقات هگل به‌درستی اشاره شده است. هگل در یافته‌های خود به این نتیجه رسیده است که رفتارهای درست و سازنده توسط کاربران، مدیران سیستم و افراد دیگر می‌تواند اثربخشی امنیت اطلاعات را تا حد زیادی بالا ببرد، در حالی‌که رفتارهای نادرست و مخرب، در حقیقت می‌تواند مانع اثربخشی آن شود (Hagen & et al., 2008). بنابراین، امنیت سایبری به مسائل اخلاق سایبری و ایمنی سایبری مربوط می‌شود. ایده امنیت سایبری باید از سنین جوانی به وجود بیاید و ریشه‌یابی شود. اقدامات متقابل امنیتی به حفظ محرمانه بودن، در دسترس

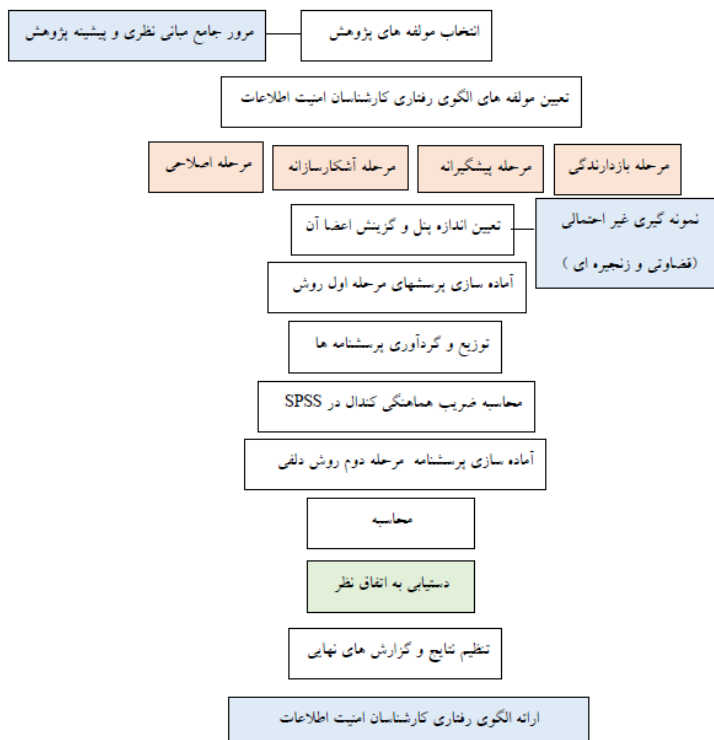
بودن و یکپارچگی سیستم‌های اطلاعاتی با جلوگیری یا کاهش تلفات دارایی ناشی از تهدیدات امنیت سایبری کمک می‌کند (Ragavendran, 2023). مارگیت شول^۱ برای حل مسئله الگوی صحیح رفتاری در خصوص امنیت اطلاعات، در یک پژوهش سه‌ساله در آلمان به کمک طیف وسیعی از داوطلبان و به‌وسیله روش‌های مختلفی ازجمله مصاحبه، نظرسنجی و بازی، آزمایش‌های مختلفی انجام داد و در نهایت به این نتیجه رسید که آموزش کلاسیک در ایجاد الگوی صحیح رفتاری ناموفق عمل کرده و راه‌حل را در طیف گسترده‌ای از اقدامات سیستماتیک و یکپارچه می‌بیند که به افزایش آگاهی مبتنی بر سیستم و به‌طور خاص به توسعه فرهنگ امنیتی کمک می‌کند (Scholl, 2023).

بررسی پیشینه پژوهش حاضر حاکی از آن است که برای ارتقای امنیت اطلاعات، با وجود اهمیت عامل انسانی، رجوع به راه‌حل‌های فنی، صرفاً پاک کردن صورت مسئله است و راه‌حل حقیقی کاهش خطای انسانی، و تبیین الگوی صحیح رفتاری می‌باشد. برای اثبات این موضوع در پژوهش حاضر به کمک روش دلفی و پیمایشی، نتایج مورد تحلیل و ارزیابی قرار گرفته و نتیجه‌گیری‌های استنباط شده ارائه شده است.

۴. روش تحقیق

پژوهش حاضر، بر مبنای هدف، کاربردی- توسعه‌ای و به لحاظ رویکرد، ترکیبی (متوالی-اکتشافی) است. داده‌های حاصل از مطالعه اسنادی، به‌صورت کیفی جمع‌آوری و تحلیل شده است. در این پژوهش از روش فراترکیب برای شناسایی مؤلفه‌های الگوی رفتاری مناسب کارشناسان امنیت اطلاعات استفاده شده است. به‌منظور شناسایی مؤلفه‌های حوزه امنیت سیستم‌های اطلاعاتی به‌وسیله روش فراترکیب از روش هفت مرحله‌ای باروسو و ساندلوسکی (۲۰۰۷) استفاده شده است.

پس از استخراج مؤلفه‌ها، با نظر و کمک خبرگان، مؤلفه‌ها و شاخص‌های پرسش‌نامه اعتبارسنجی شدند و سپس از طریق توزیع پرسش‌نامه در بین کارشناسان امنیت اطلاعات، پاسخ‌ها کنترل شده و تحلیل گردیدند. برای این منظور مطابق شکل (۱) از روش دلفی استفاده شده است که نوعی ارتباط گروهی بین مجموعه‌هایی از متخصصان و صاحب‌نظران است.



شکل ۱- مراحل روش دلفی

۴-۱. جامعه آماری

۴-۱-۱. جامعه آماری کیفی (دلفی)

بنابر کیفی- کمی بودن ماهیت پژوهش حاضر، برای انتخاب نمونه آماری کیفی و تعیین حجم نمونه تعداد خبرگان مشارکت کننده از روش نمونه گیری ترکیبی هدفمند استفاده شده است. روش نمونه گیری ترکیبی هدفمند، با استفاده از ترکیب دو یا بیش از دو روش هدفمند انجام می گیرد. در پژوهش حاضر با آگاهی از شیوه های مختلف نمونه گیری در پژوهش های کیفی، از ترکیب روش نمونه گیری همگن و گلوله برفی، برای تعیین افراد مشارکت کننده در پژوهش استفاده شد. پس از تعیین انواع مشارکت کنندگان، به منظور تعیین تعداد مشارکت کنندگان و اطمینان از دسترسی به داده های مورد نیاز پژوهش، از روش گلوله برفی استفاده گردید. روش کار در این شیوه بدین صورت است که باتوجه به موضوع تحقیق از افراد متخصص خواسته می شود تا افراد حرفه ای خبره و باتجربه دیگر را معرفی کنند. از میان افراد معرفی شده، ۵۸ نفر واجد شرایط تشخیص داده شدند. انتخاب افراد برای فرایند دلفی در این پژوهش، وابسته به تجربه ها و تخصص های مورد نیاز در موضوع مورد مطالعه بوده

است. برای انجام این پژوهش، انتخاب اعضای پانل واجد یک یا چند ویژگی زیر بودند:

♦ مدیران واحدهای سازمانی حوزه امنیت اطلاعات،

♦ اساتید دانشگاهی مرتبط با علم رایانش امن.

از این میان ۱۵ نفر از خبرگان برای دور اول دلفی، و ۱۵ نفر دیگر از خبرگان برای دور دوم دلفی تمایل و موافقت خود را برای مشارکت در کارگروه دلفی اعلام کردند.

۴-۲. جامعه آماری کمی (پیمایشی)

فهرست شرکت‌های داده‌محور و کارشناسان امنیت اطلاعات پس از فیلتر شدن با معیار حداقل ۵ سال سابقه کار مرتبط، به تعداد ۱۵۶ نفر رسیدند. با استفاده از فرمول کوکران، حداقل حجم نمونه برابر ۱۱۱ نفر شد. ولی پرسش‌نامه‌ها به هر ۱۵۶ نفر ارسال گردید و پس از دریافت ۱۱۱ پرسش‌نامه تکمیل شده، فرایند تحلیل آغاز شده و مطابق پیش‌بینی، حدود ۴۰ نفر به پرسش‌نامه پاسخ ندادند و یا پاسخ کامل ندادند و نیمه‌کاره رها کردند.

$$n = \frac{\frac{z^2 pq}{d^2}}{1 + \frac{1}{N} \left[\frac{z^2 pq}{d^2} - 1 \right]}$$

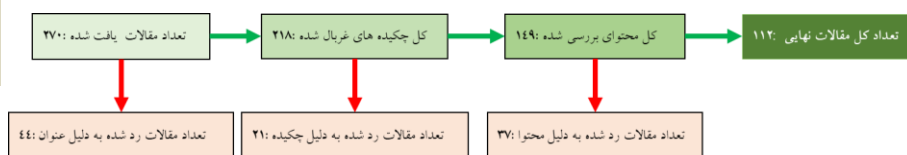
در این فرمول N حجم جامعه آماری و آماره p درصد توزیع صفت در جامعه، یعنی نسبت افرادی است که دارای صفت مورد مطالعه هستند و آماره q نیز درصد افرادی است که فاقد صفت مورد مطالعه هستند که اگر میزان p و q مشخص نباشد، از حداکثر مقدار آنها، یعنی ۰/۵ استفاده می‌شود. در سطح خطای ۵٪ مقدار z برابر ۱/۹۶ و Z^2 برابر ۳/۸۴۱۶ است. مقدار d نیز تفاضل نسبت واقعی صفت در جامعه با میزان تخمین پژوهشگر برای وجود آن صفت در جامعه است. دقت نمونه‌گیری به این عامل بستگی دارد و اگر بخواهیم نمونه‌گیری دارای بیشترین دقت باشد، از حداکثر مقدار d برابر ۰/۰۵ استفاده می‌شود.

در رویکرد دلفی، بنابر کیفی بودن ماهیت پژوهش حاضر، برای انتخاب نمونه آماری و تعیین حجم نمونه تعداد مشارکت‌کنندگان از روش نمونه‌گیری ترکیبی هدف‌مند استفاده شده است. روش نمونه‌گیری ترکیبی هدف‌مند، با استفاده از ترکیب دو یا بیش از دو روش هدف‌مند انجام می‌گیرد. همچنین، با آگاهی از شیوه‌های مختلف نمونه‌گیری در پژوهش‌های کیفی، از ترکیب روش نمونه‌گیری همگن و گلوله برفی، برای تعیین افراد مشارکت‌کننده در پژوهش استفاده شد. نمونه‌گیری همگن، بررسی دقیق و عمیق افراد با خصوصیات مشترک هدف اصلی است. پس از تعیین انواع مشارکت‌کنندگان، به‌منظور تعیین تعداد مشارکت‌کنندگان و اطمینان از دسترسی به داده‌های مورد نیاز پژوهش، از روش گلوله برفی استفاده گردید. روش کار در این شیوه بدین صورت است که باتوجه به

موضوع تحقیق از افراد متخصص خواسته می‌شود تا افراد حرفه‌ای خبره و باتجربه دیگر را معرفی کنند. انتخاب افراد برای فرایند دلفی در این پژوهش، وابسته به تجربه‌ها و تخصص‌های موردنیاز در موضوع مورد مطالعه بوده است. درمجموع ۳۰ نفر تمایل و موافقت خود را برای مشارکت در کارگروه دلفی اعلام کردند.

۴-۲. استخراج سؤالات پرسش‌نامه

هدف اصلی پژوهش حاضر ارائه الگوی رفتاری کارشناسان امنیت اطلاعات در مواجهه با تهدیدات سایبری است. در گام نخست با استفاده از روش فراترکیب، منابع کتابخانه‌ای و اسنادی، براساس کلیدواژه‌های مرتبط مانند امنیت سیستم‌های اطلاعاتی، اهداف امنیتی سازمانی، تهدیدات سایبری و... بوده است. ابتدا پرسش‌های اساسی مطرح شده و با پاسخگویی به آن‌ها محدوده کار مشخص گردید. پرسش‌های پژوهش به همراه پارامترهای چستی کار، جامعه مورد مطالعه، و محدوده زمانی، دربرگیرنده تمامی آثار موجود بین سال‌های محدوده زمانی سال‌های ۲۰۱۷ تا ۲۰۲۱ است، که به چگونگی روش شناسایی شاخص‌ها و مؤلفه‌های مرتبط با موضوع می‌پردازد. جستجوی پیشینه پژوهش در کلیه اسناد علمی و گزارش‌های پژوهشی چه در داخل و چه در خارج از کشور در خصوص شاخص‌های الگوی رفتاری کارشناسان امنیت اطلاعات و تهدیدات سایبری که طی سال‌های ۲۰۱۷ تا ۲۰۲۱ منتشر شده بودند، شامل ۲۷۰ عنوان و سند بود. از آنجایی که بسیاری از اسناد به‌دست آمده حاوی اطلاعات کلی در زمینه الگوی رفتاری بوده و اطلاعات مفیدی برای ایجاد مؤلفه در این حوزه ارائه نمی‌کرد، نتایج به‌دست آمده در این مرحله طی چند فرایند پالایش شدند. مطابق شکل (۲) می‌توان خلاصه‌ای از فرایند ارائه شده را همراه با نتایج به‌دست آمده از پژوهش حاضر مشاهده کرد.



شکل ۲ - خلاصه‌ای از فرایند تحقیق

۴-۳. مؤلفه‌ها و شاخص‌های الگوی رفتاری (استخراج شده با روش فراترکیب)

براساس مطالعه گسترده منابع داخلی و خارجی، شاخص‌های مرتبط با حوزه الگوی رفتاری در مواجهه با تهدیدات امنیتی و سایبری، ۱۴۲ شاخص از ۱۱۲ سند و مدرک معتبر استخراج گردید. شاخص‌های ارائه شده، علاوه بر دارا بودن ملاحظات سازمانی، جنبه کاربردی الگو را نیز در نظر

گرفته و دربردارنده شاخص‌های مهم الگوی رفتاری می‌باشد. پس از اعمال اصلاحات و پیشنهادهای اعضای خبرگان، برای افزایش دقت شاخص‌ها و نزدیک کردن آنها به ملاک‌های عینی و مورد استناد، برای اجرای دور دوم دلفی، پرسش‌نامه‌ای به کارشناسان ارشد سازمان ارسال و درخواست شد تا پرسش‌نامه را براساس مقیاس لیکرت رتبه‌بندی و ارزش‌گذاری کنند.

در پایان، به کمک داده‌کاوی و خوشه‌بندی با استفاده از نرم‌افزار رپیدماینر^۱، ابعاد و مؤلفه‌ها از شاخص‌های تخصصی الگوی رفتاری در مواجهه با تهدیدات سایبری و امنیتی، انتخاب و مورد تأیید اعضای خبرگان قرار گرفت. مؤلفه‌های «تهدیدات امنیتی» در ۶ بخش تهدیدات فیزیکی (عمدی/ غیرعمدی)، خسارت‌های غیرعمدی (مخدوش شدن منابع اطلاعاتی)، شکست و خرابی، انسداد خدمت، فعالیت مجرمانه / سوءاستفاده و تهدیدات قانونی تقسیم می‌شود. مؤلفه‌های «آسیب‌پذیری‌های امنیتی و سایبری» به ۷ بخش دسترسی فیزیکی غیرمجاز (عمدی/ سهوی)، ضعف در نگهداری منابع اطلاعاتی، محیطی، ضعف در کنترل شکست/ خرابی، نقص در زیرساخت ارتباطی، حفاظت ناکافی در مقابل شنود/ رهگیری، بروز فعالیت مجرمانه / سوءاستفاده و مسائل قانونی تقسیم می‌شود. «الزامات انسانی/ فنی/ فرایندی» شامل مؤلفه‌های رویه‌ای و انسانی، و همچنین فنی به ۷ بخش مستقل شامل استفاده مؤثر از سازوکارهای احراز هویت، استفاده مؤثر از سازوکار کنترل دسترسی، سازوکارهای امنیت ارتباطات، سازوکارهای امنیت اطلاعات سامانه‌ها، سازوکار پاسخگویی و عدم انکار، سازوکار امنیت فیزیکی/ محیطی و سازوکار پشتیبان‌گیری و دسترسی‌پذیری تقسیم می‌شود.

جدول ۱ - فراوانی عناوین شاخص‌ها در مراحل پژوهش

تعداد شاخص‌های استخراج شده	بعدها به تفکیک (در مرحله جمع‌آوری)
۳۶	تهدیدات امنیتی
۳۱	آسیب‌پذیری‌های امنیتی و سایبری
۱۵	عوامل انسانی
۴۳	عوامل فنی
۱۷	عوامل فرایندی

براساس فرایند فوق، ابتدا ۱۴۲ شاخص در ۵ بعد تهدیدات امنیتی شامل ۳۶ شاخص، آسیب‌پذیری‌های امنیتی و سایبری شامل ۳۱ شاخص، مؤلفه‌های انسانی شامل ۱۵ شاخص، مؤلفه‌های فنی شامل ۴۳ شاخص و مؤلفه‌های فرایندی شامل ۱۷ شاخص، جمع‌آوری گردید که شاخص‌های اصلی برای اجرای دلفی در نظر گرفته شد.

۵. نتایج

۵-۱. روش دلفی

در پژوهش حاضر الگوی رفتاری کارشناسان امنیت اطلاعات در مواجهه با تهدیدات دارای ۱۷ مؤلفه و ۱۴۲ شاخص در ۵ بعد می‌باشد. مطابق جدول (۲) پنل دلفی دو مرتبه انجام شد، که پس از انجام مرحله اول، برای بررسی توافق خبرگان از ضریب توافق کندال استفاده گردید و نتایج در ادامه آمده است.

جدول ۲- خبرگان شرکت کننده در مرحله اول و دوم دلفی

دور دلفی	امنیت اطلاعات	فناوری اطلاعات	فراوانی
مرحله اول	۹	۶	۱۵
درصد فراوانی	۶۰٪	۴۰٪	۱۰۰٪
مرحله دوم	۱۰	۵	۱۵
درصد فراوانی	۶۷٪	۳۳٪	۱۰۰٪

۵-۲. روایی و پایایی

باتوجه به مطالعات نظری، عوامل مؤثر در الگوی رفتاری در چهار مرحله (بازدارندگی، پیشگیری، آشکارسازی و اصلاحی) با تدوین پرسش‌نامه مناسبی در مورد داده‌های مؤلفه‌های الگوی رفتاری ارائه شد. سنجش روایی پرسش‌نامه و روایی محتوایی، توسط افرادی متخصص در موضوع مورد مطالعه تعیین می‌شود. در این پژوهش برای روایی‌سازی بخش کیفی از روایی صوری بهره گرفته است. ۱۵ نفر از خبرگان مرتبط براساس نمونه‌گیری هدف‌مند انتخاب و از آنها خواسته شد که پرسش‌نامه بدون ساختار مؤلفه‌های الگوی رفتاری را پاسخ دهند. سپس براساس پاسخ آنها، پرسش‌نامه به‌صورت ساختارمند براساس دسته‌بندی اولیه تهیه شده و در اختیار خبرگان قرار گرفت. مطابق جدول (۳) جهت ارزیابی نظرات پانل از شاخص میانگین و انحراف معیار، ضریب کندال و درصد توافق استفاده شده است. حداقل مقدار قابل قبول برای شاخص CVI برابر با ۰/۷۹ است و اگر کمتر از این مقدار باشد، آن گویه بایستی حذف و یا اصلاح شود. پس از استخراج سؤالات مربوط به هر یک از مؤلفه‌های الگوی رفتاری، به تهیه فرم‌های سنجش روایی مربوط بودن، ساده بودن و واضح بودن، مبادرت ورزیده شد. متخصصان در قالب طیف لیکرت ۵ تایی برای هر یک از سؤالات با در نظر گرفتن میزان مربوط بودن، ساده بودن و واضح بودن آنها با مؤلفه‌های الگوی رفتاری، امتیازی از ۱ تا ۵ در نظر گرفتند. پس از بررسی فرم‌های سنجش روایی تکمیل شده توسط متخصصان، شاخص CVI با استفاده از معادله زیر محاسبه گردید.

$$CVI = \frac{\sum_{i=1}^n CVR}{\text{Retained numbers}}$$

جدول ۳- نتایج دور اول دلفی

مؤلفه	کد	نام شاخص	تعداد پاسخ	بازبین	انحراف معیار	آماره تی	سطح معناداری	CVR	CVI	تغییرات کیفی
تهدیدات فیزیکی	q01	کلاهبرداری	۱۵	2.933	0.258	-1	0.334	53%	7%	حذف
	q02	تخریب	۱۵	2.8	0.414	-1.871	0.082	53%	7%	حذف
	q03	سرقت دارایی	۱۵	4.067	0.258	16	0	100%	100%	تأیید
	q04	نشت / اشتراک اطلاعات	۱۵	4.067	0.594	6.959	0	87%	73%	تأیید
	q05	دسترسی فیزیکی غیرمجاز (ورود غیرمجاز)	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q06	اخاذی	۱۵	2.867	0.352	-1.468	0.164	53%	7%	حذف
خسارت‌های غیرعمدی (مخدوش شدن منابع اطلاعاتی)	q07	نشت اطلاعات به دلیل خطای انسانی	۱۵	4.267	0.458	10.717	0	100%	100%	تأیید
	q08	استفاده / مدیریت نادرست سیستم	۱۵	4	0.378	10.247	0	93%	87%	تأیید
	q09	استفاده از اطلاعات منابع غیرقابل اعتماد	۱۵	4	0.378	10.247	0	93%	87%	تأیید
	q10	تغییر از اطلاعات منابع غیرقابل اعتماد	۱۵	2.733	0.458	-2.256	0.041	33%	-33%	حذف
	q11	تغییر غیرعمدی داده در سیستم	۱۵	4.2	0.414	11.225	0	87%	73%	تأیید
	q12	خسارت ناشی از رفتار طرف ثالث	۱۵	4.067	0.258	16	0	100%	100%	تأیید
	q13	خسارت ناشی از تست نفوذ	۱۵	4.333	0.488	10.583	0	87%	73%	تأیید
	q14	از دست رفتن اطلاعات در فضای ابر	۱۵	4.333	0.488	10.583	0	100%	100%	تأیید
	q15	از دست رفتن / تخریب / مخدوش شدن دارایی	۱۵	4.2	0.414	11.225	0	87%	73%	تأیید
	q16	خرابی یا اختلال لینک‌ها / شبکه‌های ارتباطی	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
شکست / خرابی	q17	خرابی یا اختلال زنجیره تأمین خدمت	۱۵	2.867	0.352	-1.468	0.164	60%	20%	حذف
	q18	خرابی تجهیزات (دستگاه یا سیستم)	۱۵	2.8	0.414	-1.871	0.082	60%	20%	حذف
انسان‌های خدمت فالت مجرمانه / سوء استفاده	q19	استراق سمع در مسیر انتقال داده‌ها / سرقت نشست / رهگیری اطلاعات مجرمانه	۱۵	4.067	0.258	16	0	100%	100%	تأیید
	q20	گشت‌زنی در شبکه‌های بی‌سیم بی‌حفاظ	۱۵	4.267	0.458	10.717	0	100%	100%	تأیید
	q21	دستکاری ترافیک شبکه / حمله مرد میانی / جمع‌آوری و دستکاری اطلاعات	۱۵	4.067	0.258	16	0	100%	100%	تأیید
	q22	سرقت هویت (حساب) / کلاهبرداری / استفاده از گواهی نامه تقلبی	۱۵	4.067	0.258	16	0	100%	100%	تأیید
	q23	دریافت پست الکترونیکی ناخواسته (هرزنامه)	۱۵	4.333	0.488	10.583	0	100%	100%	تأیید
	q24	انسداد سرویس	۱۵	4.067	0.258	16	0	100%	100%	تأیید
	q25	اجرا (تزریق) کد / نرم‌افزار / فعلیت مخرب	۱۵	4	0.378	10.247	0	93%	87%	تأیید
	q26	مهندسی اجتماعی	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید

<http://stjm.gom.ac.ir>

مؤلفه	کد	نام شاخص	تعداد پاسخ	میانگین	انحراف معیار	نمره نهی	سطح معناداری	CVR	CVI	تغییرات کیفی
	q27	دستکاری سخت افزار و نرم افزار	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q28	دستکاری اطلاعات	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
	q29	سوءاستفاده از ابزارهای ممیزی	۱۵	4.2	0.561	8.29	0	93%	87%	تأیید
	q30	نصب و راه اندازی غیرمجاز نرم افزار	۱۵	4.067	0.258	16	0	100%	100%	تأیید
	q31	سوءاستفاده از اطلاعات محرمانه	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q32	فعالیت مخرب از راه دور	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
	q33	حملات هدفمند	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
تهدیدات قانونی	q34	جستجوی جامع	۱۵	2.933	0.258	-1	0.334	60%	20%	حذف
	q35	استفاده غیرمجاز از منابع حفاظت شده	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q36	سوءاستفاده از داده های خصوصی	۱۵	4.333	0.488	10.583	0	100%	100%	تأیید
دسترسی فیزیکی غیرمجاز (اجدنی / سبوری)	q37	ضعف در آموزش کارکنان	۱۵	4.067	0.258	16	0	100%	100%	تأیید
	q38	احراز هویت ناکارآمد	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
	q39	قابلیت خواندن حافظه خارجی در دستگاه های قابل حمل	۱۵	4.267	0.594	8.264	0	93%	87%	تأیید
ضعف در نگهداری منابع اطلاعاتی	q40	مدیریت خطا به شیوه نادرست	۱۵	4.267	0.458	10.717	0	100%	100%	تأیید
	q41	امکان تغییر در اطلاعات سامانه	۱۵	4.267	0.458	10.717	0	100%	100%	تأیید
	q42	تفویض اختیار ناکارآمد	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
	q43	پیگیری ضعیف سامانه	۱۵	4.267	0.458	10.717	0	100%	100%	تأیید
	q44	ارزبایی امنیتی ناکارآمد فناوری ها	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
	q45	خطمشی و دستورالعمل های ناکارآمد	۱۵	4	0.378	10.247	0	93%	87%	تأیید
	q46	سازوکار نادرست در قفل گذاری منابع	۱۵	4	0.845	4.583	0	80%	60%	تأیید
محیط	q47	مکان یابی ناکارآمد تجهیزات	۱۵	2.8	0.414	-1.871	0.082	60%	20%	حذف
	q48	تاثیر تجهیزات از شرایط آب و هوایی	۱۵	2.8	0.414	-1.871	0.082	60%	20%	حذف
ضعف در کنترل شبکه / خرابی	q49	شکست در اجرای سازوکار حفاظتی	۱۵	4.133	0.352	12.475	0	87%	73%	تأیید
	q50	ضعف در مدیریت انرژی تجهیزات	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
نقص در زیر ساخت ارتباطی	q51	طراحی ضعیف سیستم	۱۵	4.067	0.799	5.172	0	87%	73%	تأیید
	q52	از دسترس خارج شدن شبکه ارتباطی	۱۵	4.067	0.258	16	0	100%	100%	تأیید
	q53	در دسترس نبودن پشتیبان خدمات ارتباطی	۱۵	4.067	0.258	16	0	100%	100%	تأیید
	q54	شبکه اینترنتی ناامن	۱۵	4.067	0.258	16	0	100%	100%	تأیید
	q55	طراحی و برنامه ریزی ناکارآمد	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید

مؤلفه	کد	نام شاخص	تعداد پاسخ	میانگین	انحراف معیار	آماره تی	سطح معناداری	CVR	CVI	تغییرات کیفی
حفاظت تاکتی در مقابل شنود/ رهگیری	q56	وجود شبکه ارتباطی بی سیم ناامن	۱۵	4.133	0.743	5.906	0	93%	87%	تأیید
	q57	انتقال ناامن اطلاعات	۱۵	4.067	0.799	5.172	0	87%	73%	تأیید
	q58	مدیریت نادرست ارتباطات و سرقت نشست	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
بروز فعالیت محرمانه / سوءاستفاده	q59	ضعف در سازوکارهای کنترل دسترسی	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q60	اجرای کدها/ دستورات غیرمجاز	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q61	عدم به کارگیری الگوریتم های معتبر رمزنگاری	۱۵	4.267	0.458	10.717	0	100%	100%	تأیید
	q62	امکان دستکاری در ورودی ها	۱۵	2.6	0.507	-3.055	0.009	53%	7%	حذف
	q63	ضعف در مواجهه با روش های مهندسی اجتماعی	۱۵	4.2	0.414	11.225	0	80%	60%	تأیید
	q64	ضعف در شناسایی شبکه های طعمه و فعالیت های مخرب	۱۵	4.2	0.414	11.225	0	93%	87%	تأیید
مسائل قانونی	q65	حفاظت تاکتی در مقابل چالش های حریم خصوصی	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
	q66	خلاءهای قانونی پیرامون فعالیت طرف ثالث	۱۵	4.267	0.458	10.717	0	87%	73%	تأیید
	q67	قوانین بازدارنده و ناکارآمد	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
عوامل انسانی	q68	همراهی کارکنان با خطمشی های امنیت اطلاعات سازمان	۱۵	4.333	0.488	10.583	0	87%	73%	تأیید
	q69	حمایت مدیریت عالی از برنامه ها، پروژه ها و خطمشی های امنیتی سازمان	۱۵	3.933	0.594	6.089	0	80%	60%	تأیید
	q70	حمایت مهارت، تجربه، آگاهی و آموزش کاربران در زمینه امنیت اطلاعات	۱۵	3.867	0.516	6.5	0	80%	60%	تأیید
	q71	درک نیازهای امنیتی در سطوح مختلف سازمان	۱۵	4.267	0.458	10.717	0	100%	100%	تأیید
	q72	رفتار محافظه کارانه کاربران در زمینه امنیت سیستم های اطلاعاتی	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
	q73	پیروی از استانداردها و دستورالعمل های امنیتی	۱۵	4.067	0.458	9.025	0	93%	87%	تأیید
	q74	حس پاسخگویی، خودارزیابی و خودگزارش دهی	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q75	تدوین و اجرای برنامه های آموزشی و حوزه امنیت اطلاعات	۱۵	4.333	0.488	10.583	0	100%	100%	تأیید
	q76	تشویق کارمندان به گزارش مخاطرات و مشکلات امنیتی	۱۵	4.133	0.352	12.475	0	87%	73%	تأیید
	q77	تعیین مسئولیت های امنیتی در سطح سازمان و استقرار سازمان امنیتی	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
	q78	تعهد و وفاداری کارمندان به سازمان و ملاحظات امنیتی رایج	۱۵	4	0.756	5.123	0	87%	73%	تأیید

مؤلفه	کد	نام شاخص	تعداد پاسخ	میانگین	انحراف معیار	نمره نهی	سطح معناداری	CVR	CVI	تغییرات کیفی
تأیید	q79	غربالگری و ارزیابی دوره‌ای کارمندان از منظر ملاحظات امنیت اطلاعات	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q80	تعریف کاربری‌های مجاز سیستم و حقوق دسترسی	۱۵	4.2	0.414	11.225	0	87%	73%	تأیید
	q81	حاکمیت فرهنگ‌سازی همکاری در فعالیت و برنامه‌های امنیتی سازمان	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
	q82	نظارت و پایش مستمر فعالیت‌های طرف ثالث در حوزه امنیت اطلاعات	۱۵	4.2	0.414	11.225	0	87%	73%	تأیید
	q83	استفاده مؤثر و کارا از سازوکار کنترل دسترسی	۱۵	4.267	0.458	10.717	0	87%	73%	تأیید
	q84	استفاده از کلمه‌های عبور قوی	۱۵	4.267	0.458	10.717	0	87%	73%	تأیید
	q85	استفاده از کارت‌های هوشمند و توکن‌های امنیتی	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
	q86	صدور مجوز و تفویض اختیار	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
	q87	دسترسی افراد بیرونی به داده‌های سیستم	۱۵	4.267	0.458	10.717	0	100%	100%	تأیید
	q88	حفاظت از منابع در مقابل دسترسی و نفوذ فیزیکی	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
تأیید	q89	محدود کردن دسترسی کاربران	۱۵	4	0.378	10.247	0	93%	87%	تأیید
	q90	مدیریت و تعیین خط‌مشی‌های حقوق دسترسی کاربران	۱۵	4.067	0.258	16	0	100%	100%	تأیید
	q91	استفاده از سازوکار کنترل دسترسی منطقی	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q92	کنترل دسترسی طرف ثالث و پیمانکاران	۱۵	4.067	0.258	16	0	100%	100%	تأیید
	q93	سازوکار امنیت ارتباطات	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q94	استفاده از سیستم‌های پایش و سامانه‌های جامع نظارتی	۱۵	4.4	0.507	10.693	0	87%	73%	تأیید
	q95	به‌کارگیری پروتکل‌های امنیت اطلاعات/ ارتباطات امن	۱۵	4.467	0.516	11	0	100%	100%	تأیید
	q96	استفاده از الگوریتم‌های رمزنگاری	۱۵	4.133	0.352	12.475	0	87%	73%	تأیید
	q97	کابل کشی امن مابین سیستم‌ها/تجهیزات	۱۵	4.133	0.352	12.475	0	87%	73%	تأیید
	q98	کنترل و کدگذاری رسانه‌های قابل حمل	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
	q99	محرمانگی (امنیت اطلاعات)	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q100	مدیریت ارتباطات در برون‌سپاری خدمات امنیتی	۱۵	4.133	0.352	12.475	0	87%	73%	تأیید
	q101	مدیریت تجهیزات و رسانه‌های ارتباطی	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q102	گمنام‌سازی داده‌ها و لینک‌های ارتباطی	۱۵	4.2	0.414	11.225	0	93%	87%	تأیید
	q103	سازوکارهای امنیت اطلاعات و سامانه‌ها	۱۵	4.267	0.458	10.717	0	87%	73%	تأیید

مؤلفه	کد	نام شاخص	بمقدار پاسخ	میانگین	انحراف معیار	آماره تی	سطح معناداری	CVR	CVI	تغییرات کیفی
عوامل فزاینده	q104	استفاده از پوششگرها و سیستم‌های تشخیص نفوذ	۱۵	4.333	0.488	10.583	0	93%	87%	تأیید
	q105	استفاده از دیواره آتش و سازوکار یکپارچه مدیریت تهدید	۱۵	4.2	0.414	11.225	0	93%	87%	تأیید
	q106	مدیریت، انتقال و نگهداری امن داده‌ها	۱۵	4.4	0.507	10.693	0	100%	100%	تأیید
	q107	صیانت از صحت و یکپارچگی داده‌ها	۱۵	4.6	0.507	12.22	0	93%	87%	تأیید
	q108	امضاءهای دیجیتال	۱۵	4.467	0.516	11	0	100%	100%	تأیید
	q109	فناوری‌های پنهان نگاری	۱۵	4.4	0.507	10.693	0	93%	87%	تأیید
	q110	سازوکار پاسخگویی و عدم انکار	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q111	سازوکار پالایش محتوا	۱۵	4.267	0.458	10.717	0	93%	87%	تأیید
	q112	سازوکارهای پایش عملیات	۱۵	4.333	0.488	10.583	0	100%	100%	تأیید
	q113	بازرسی سیستم‌های اطلاعاتی/تجهیزات	۱۵	4.333	0.488	10.583	0	87%	73%	تأیید
	q114	ممیزی امنیت اطلاعات	۱۵	4.267	0.458	10.717	0	87%	73%	تأیید
	q115	سازوکار امنیت فیزیکی/ محیطی	۱۵	4.533	0.516	11.5	0	100%	100%	تأیید
	q116	مدیریت انرژی (پشتیبان برق و مدیریت شرایط اضطرار)	۱۵	4.733	0.458	14.666	0	100%	100%	تأیید
	q117	سامانه‌های اطفاء حریق و اعلام هشدار حرارتی	۱۵	4.333	0.488	10.583	0	87%	73%	تأیید
	q118	سازوکارهای مقاوم‌سازی	۱۵	4.2	0.414	11.225	0	93%	87%	تأیید
	q119	ایمن‌سازی فیزیکی دستگاه‌های الکترونیکی/ سامانه	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q120	ایمن‌سازی اماکن و فضاهای حساس	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q121	استانداردها و سازوکارهای کنترل دما و رطوبت	۱۵	4.467	0.516	11	0	93%	87%	تأیید
	q122	سازوکار پشتیبان‌گیری و دسترس‌پذیری	۱۵	4.333	0.488	10.583	0	100%	100%	تأیید
	q123	استفاده از دارایی‌ها و تجهیزات اضافی	۱۵	4.6	0.507	12.22	0	100%	100%	تأیید
	q124	پشتیبان‌گیری منظم از سیستم‌ها	۱۵	4.4	0.507	10.693	0	100%	100%	تأیید
	q125	افزایش ظرفیت حافظه	۱۵	2.533	0.516	-3.5	0.004	67%	33%	حذف
عوامل فزاینده	q126	استفاده از چک‌لیست‌های امنیتی	۱۵	4.6	0.507	12.22	0	100%	100%	تأیید
	q127	تدوین قوانین، خط‌مشی‌ها، دستورالعمل‌ها و الزامات	۱۵	4.467	0.516	11	0	100%	100%	تأیید
	q128	عضویت و تعامل با انجمن‌های حرفه‌ای امنیت	۱۵	4.533	0.516	11.5	0	80%	60%	تأیید
	q129	تعیین جریمه برای عدم پیروی از خط‌مشی‌های امنیت	۱۵	4.467	0.516	11	0	100%	100%	تأیید

مؤلفه	کد	نام شاخص	تعداد پاسخ	میانگین	انحراف معیار	آماره تی	سطح معناداری	CVR	CVI	متغیرات کیفی
	q130	تعیین راهبردها و اهداف مدیریتی براساس شرایط حاکم	۱۵	4.6	0.507	12.22	0	80%	60%	تأیید
	q131	برنامه‌ریزی، تحلیل پیامد و بودجه‌بندی امنیتی	۱۵	4.6	0.507	12.22	0	100%	100%	تأیید
	q132	سازمان‌دهی سایت‌های مشکوک توسط کاربران	۱۵	4.467	0.516	11	0	93%	87%	تأیید
	q133	تدوین اصول و روال‌های پایش و کنترل کارمند	۱۵	4.6	0.507	12.22	0	100%	100%	تأیید
	q134	ارزیابی و به‌روزرسانی منظم قوانین، خط‌مشی‌ها و الزام‌ها	۱۵	4.533	0.516	11.5	0	93%	87%	تأیید
	q135	اصول جمع‌آوری، نظارت و تحلیل اطلاعات	۱۵	4.4	0.507	10.693	0	100%	100%	تأیید
	q136	روش‌های بررسی صحت، محرمانگی و دسترسی‌پذیری	۱۵	4.467	0.516	11	0	100%	100%	تأیید
	q137	اصول طبقه‌بندی داده‌ها و منابع اطلاعاتی	۱۵	4.333	0.488	10.583	0	100%	100%	تأیید
	q138	روش شناسایی و طبقه‌بندی دارایی‌ها	۱۵	4.267	0.458	10.717	0	100%	100%	تأیید
	q139	طراحی معماری امن	۱۵	4.067	0.258	16	0	100%	100%	تأیید
	q140	برنامه‌ریزی آموزشی و آگاهی‌رسانی امنیتی	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
	q141	رویه‌های تشخیص، گزارش‌دهی و پاسخ رخداد	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q142	تدوین استانداردهای امنیتی	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید

در مرحله اول دلفی، تعداد ۱۵ پرسش‌نامه تکمیل شده توسط خبرگان، جمع‌آوری گردید. ضریب آلفای کرونباخ برای دور اول ۰/۹۰۲ بدست آمد. در این مرحله شاخص‌هایی که دارای میانگین کمتر از ۳ و یا مقدار آماره تی برای آنها بیشتر از ۰/۰۵ بود، و نیز شاخص‌هایی که دارای CVI کمتر از ۴۹٪ و CVR کمتر از ۷۰٪ هستند، از دور اول حذف و در دور دوم وارد نمی‌شوند. شاخص‌های باقیمانده، برای دور دوم دلفی مجدداً آماده و در اختیار خبرگان گذاشته می‌شود. در بررسی‌های انجام شده و توافق نظر خبرگان، ۴ مرحله (بازدارندگی، پیشگیرانه، آشکارسازی، اصلاحی) به ارزیابی شاخص‌های الگوی رفتاری اضافه شد. در مرحله دوم دلفی، تعداد ۱۵ پرسش‌نامه بین خبرگان دور قبل توزیع گردید. ضریب آلفای کرونباخ برای دور دوم ۰/۹۳۳ بدست آمد. مطابق جدول (۴)، در مرحله دوم روش دلفی، شاخص‌ها در چهار وضعیت شامل مرحله بازدارندگی، مرحله پیشگیرانه، مرحله آشکارسازی و مرحله اصلاحی مورد ارزیابی قرار گرفتند. نتایج نشان می‌دهد که در هر چهار مرحله، تمامی شاخص‌ها دارای اعتبار کافی از منظر شاخص‌روایی (مقدار سی‌وی‌آی بالای ۴۹٪

جدول ۴- نتایج دور دوم دلفی

تهدیدات امنیتی															ایماد
تهدیدات فیزیکی															موانع
خسارت‌های غیر عمدی															مسئول
تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید
87%	47%	73%	87%	60%	60%	80%	80%	60%	80%	60%	80%	80%	60%	80%	80%
93%	73%	87%	80%	80%	80%	80%	80%	80%	80%	80%	80%	80%	80%	80%	80%
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	6,971	6,141	6	8,876	5,906	6,971	8,367	6,325	7,135	5,906	5,172	6,971	5,137	6,971	6,959
0.775	0.704	0.799	0.775	0.64	0.743	0.704	0.617	0.816	0.724	0.743	0.799	0.704	0.704	0.704	0.516
4.2	4.267	4.267	4.2	4.467	4.133	4.267	4.333	4.333	4.333	4.133	4.067	4.267	3.933	3.867	3.867
60%	73%	73%	73%	87%	87%	73%	100%	100%	73%	73%	73%	87%	73%	87%	87%
80%	87%	87%	87%	93%	93%	87%	100%	100%	87%	87%	87%	93%	87%	93%	93%
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7.135	6,971	6	8,367	6,971	5,123	5,123	7,135	4,675	5,264	8,573	5,392	5,87	5,137	6,959	6,959
0.72375	0.70373	0.7746	0.61721	0.70373	0.75593	0.75593	0.72375	0.88372	0.83381	0.63246	0.86189	0.70373	0.70373	0.59362	0.59362
4.3333	4.2667	4.2	4.3333	4.2667	4	4	4.3333	4.0667	4.1333	4.4	4.2	4.0667	3.9333	4.0667	4.0667
73%	73%	87%	87%	73%	100%	100%	73%	73%	73%	87%	73%	87%	87%	87%	73%
87%	87%	93%	93%	87%	100%	100%	87%	87%	87%	93%	87%	93%	93%	87%	87%
0.002	0	0.005	0	0	0	0	0.003	0.003	0.001	0	0.019	0.005	0.001	0	0
3.761	8.29	3.292	5.172	4.583	4.525	5.916	3.666	3.666	4.026	5.392	2.646	3.292	4.026	8.5	8.5
0.96115	0.56061	0.94112	0.79881	0.84515	0.79881	0.65465	0.91548	0.91548	0.83381	0.86189	0.9759	0.94112	0.83381	0.5164	0.5164
3.9333	4.2	3.8	4.0667	4	3.9333	4	3.8667	3.8667	3.8667	4.2	3.6667	3.8	3.8667	4.1333	4.1333
87%	87%	87%	100%	100%	87%	73%	60%	87%	87%	100%	87%	87%	87%	73%	73%
93%	93%	93%	100%	100%	93%	87%	80%	93%	93%	100%	93%	93%	93%	87%	87%
0	0.001	0	0	0	0	0	0	0.003	0	0	0	0.003	0	0.001	0.001
6	4,183	5.87	8,367	8,264	5,245	6.5	4,516	3,556	4,785	6	6,089	3,595	5,137	4.09	4.09
0.7746	0.92582	0.70373	0.61721	0.59362	0.63994	0.5164	0.74322	0.79881	0.59362	0.7746	0.59362	0.86189	0.70373	0.88372	0.88372
4.2	4	4.0667	4.3333	4.2667	3.8667	3.8667	3.7333	3.7333	3.7333	4.2	3.9333	3.8	3.9333	3.9333	3.9333
a33	a32	a31	a29	a28	a27	a26	a25	a24	a23	a22	a21	a13	a12	a11	شخص
اسناد خدمت فعالیت مجموعه															موانع

نقص در زیرساخت‌های اطلاعاتی										دسترسی فیزیکی غیرمجاز				موقعه		ایجاد
تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید
87%	87%	87%	73%	73%	73%	73%	73%	73%	73%	73%	73%	73%	73%	73%	73%	73%
93%	93%	93%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8,264	5,123	3,674	5,906	13,229	14,666	8,367	4,583	5,172	8,367	4,183	4,785	5,123	6,141	4,516	6,089	7,135
0.594	0.756	0.632	0.743	0.488	0.458	0.617	0.845	0.799	0.617	0.617	0.594	0.756	0.799	0.743	0.594	0.724
4.267	4	3.6	4.133	4.667	4.733	4.333	4	4.067	4.333	3.667	3.733	4	4.267	3.867	3.933	4.333
73%	87%	73%	73%	73%	87%	87%	73%	87%	73%	73%	87%	73%	73%	87%	73%	73%
87%	93%	87%	87%	87%	93%	93%	87%	93%	87%	87%	93%	87%	87%	93%	87%	87%
0	0	0.001	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6.959	4.516	4.036	5.906	14.666	16.837	8.876	5.906	8.876	8.876	5.527	5.137	5.87	5.172	5.245	5.916	6
0.59362	0.74322	0.70373	0.74322	0.45774	0.41404	0.63994	0.74322	0.63994	0.63994	0.56061	0.70373	0.70373	0.79881	0.63994	0.65465	0.7746
4.0667	3.8667	3.7333	4.1333	4.7333	4.8	4.4667	4.1333	4.4667	4.4667	3.8	3.9333	4.0667	4.0667	3.8667	4	4.2
73%	73%	73%	87%	87%	73%	73%	73%	73%	87%	73%	73%	87%	73%	73%	73%	73%
87%	87%	87%	93%	93%	87%	87%	87%	87%	93%	87%	87%	93%	87%	87%	87%	87%
0	0	0	0	0	0	0	0	0	0	0	0	0.003	0.068	0	0	0
6.859	5.137	4.583	6.971	7.122	5.137	5.392	4.026	8.367	9.28	4.583	6.859	3.666	1.974	5.137	5.245	5.264
0.63994	0.70373	0.50709	0.70373	0.83381	1.0556	0.86189	0.83381	0.61721	0.63994	0.67612	0.63994	0.91548	0.91548	0.70373	0.63994	0.83381
4.1333	3.9333	3.6	4.2667	4.5333	4.4	4.2	3.8667	4.3333	4.5333	3.8	4.1333	3.8667	3.4667	3.9333	3.8667	4.1333
100%	87%	87%	87%	73%	100%	87%	100%	87%	87%	87%	87%	87%	87%	87%	87%	87%
100%	93%	93%	93%	87%	100%	93%	100%	93%	93%	93%	93%	93%	93%	93%	93%	93%
0	0	0	0.002	0.001	0.001	0.001	0.033	0	0	0.005	0.002	0.001	0.001	0	0	0
6.971	8.367	6.5	3.756	4.183	4.012	4.294	2.358	4.583	4.75	3.292	3.761	4.026	4.036	6.5	10.247	4.525
0.70373	0.61721	0.5164	1.09978	1.24443	1.2228	1.08233	0.98561	1.01419	1.0328	0.94112	0.96115	0.83381	0.70373	0.5164	0.37796	0.79881
4.2667	4.3333	3.8667	4.0667	4.3333	4.2667	4.2	3.6	4.2	4.2667	3.8	3.9333	3.8667	3.7333	3.8667	4	3.9333
b45	b44	b43	b42	b41	b37	b36	b35	b34	b33	b32	b31	b23	b22	b21	b17	b16
شاخص																

[illegible]

[illegible]

عوامل فرایندی																								
نظارت												قوانین												
تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	
87%	100%	100%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	
93%	100%	100%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
5.245	4.785	6.141	5.87	8.264	5.916	4.525	6.971	4	6.959	7.359	6.141	8.367	9.798	5.551	5.264	5.916	5.245	5.245	5.245	5.245	5.245	5.245	5.245	
0.64	0.594	0.799	0.704	0.594	0.655	0.799	0.704	0.516	0.594	0.737	0.799	0.617	0.632	0.884	0.834	0.655	0.64	0.64	0.64	0.64	0.64	0.64	0.64	
3.867	3.733	4.267	4.067	4.267	4	3.933	4.267	3.533	4.067	4.4	4.267	4.333	4.6	4.267	4.133	4	3.867	3.867	3.867	3.867	3.867	3.867	3.867	
87%	100%	100%	100%	100%	73%	73%	73%	60%	60%	73%	87%	87%	87%	100%	87%	87%	73%	73%	73%	73%	73%	73%	73%	
93%	100%	100%	100%	100%	87%	87%	87%	80%	80%	87%	93%	93%	93%	100%	93%	93%	87%	87%	87%	87%	87%	87%	87%	
0	0	0	0	0	0	0	0	0.003	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
5.245	6.089	7.359	8.367	8.29	6.859	5.87	6.971	3.674	10.717	6.325	6.141	6.971	7.643	5.739	5.264	6.859	4.583	4.583	4.583	4.583	4.583	4.583	4.583	
0.63994	0.59362	0.73679	0.61721	0.56061	0.63994	0.70373	0.70373	0.63246	0.45774	0.8165	0.79881	0.70373	0.74322	0.89974	0.83381	0.63994	0.67612	0.67612	0.67612	0.67612	0.67612	0.67612	0.67612	
3.8667	3.9333	4.4	4.3333	4.2	4.1333	4.0667	4.2667	3.6	4.2667	4.3333	4.2667	4.2667	4.4667	4.3333	4.1333	4.1333	3.8	3.8	3.8	3.8	3.8	3.8	3.8	
100%	100%	100%	73%	73%	73%	60%	60%	73%	87%	87%	87%	87%	87%	93%	73%	73%	100%	100%	100%	100%	100%	100%	100%	
100%	100%	100%	87%	87%	87%	80%	80%	87%	93%	93%	93%	100%	93%	87%	87%	87%	100%	100%	100%	100%	100%	100%	100%	
0	0	0.001	0.003	0	0	0	0	0.001	0	0.001	0	0	0	0	0	0.003	0.003	0.003	0.003	0.003	0.003	0.003	0.003	
4.583	8.5	4.294	3.556	5.172	8.264	5.906	8.29	4.183	5.916	4	8.876	4.583	7.359	8.919	6.971	3.666	3.674	3.674	3.674	3.674	3.674	3.674	3.674	
0.67612	0.5164	1.08233	0.79881	0.79881	0.59362	0.74322	0.56061	0.61721	0.65465	1.0328	0.63994	0.84515	0.73679	0.72375	0.70373	0.91548	0.63246	0.63246	0.63246	0.63246	0.63246	0.63246	0.63246	
3.8	4.1333	4.2	3.7333	4.0667	4.2667	4.1333	4.2	3.6667	4	4.0667	4.4667	4	4.4	4.6667	4.2667	3.8667	3.6	3.6	3.6	3.6	3.6	3.6	3.6	
73%	73%	73%	73%	60%	60%	73%	87%	87%	87%	100%	60%	87%	73%	100%	73%	73%	73%	73%	73%	73%	73%	73%	73%	
87%	87%	87%	87%	80%	80%	87%	93%	93%	93%	100%	80%	93%	87%	100%	87%	87%	87%	87%	87%	87%	87%	87%	87%	
0	0	0.025	0	0	0	0	0	0	0	0	0	0.002	0	0	0	0	0	0	0	0	0	0	0	
9.025	10.717	2.514	12.475	10.583	11.225	10.717	11.225	6.205	12.475	11	11	3.873	11.5	16.837	11	11.225	7.483	7.483	7.483	7.483	7.483	7.483	7.483	
0.45774	0.45774	1.43759	0.35187	0.48795	0.41404	0.45774	0.41404	0.45774	0.35187	0.5164	0.5164	1	0.5164	0.41404	0.5164	0.41404	0.41404	0.41404	0.41404	0.41404	0.41404	0.41404	0.41404	
4.0667	4.2667	3.9333	4.1333	4.3333	4.2	4.2667	4.2	3.7333	4.1333	4.4667	4.4667	4	4.5333	4.8	4.4667	4.2	3.8	3.8	3.8	3.8	3.8	3.8	3.8	
e25	e24	e23	e22	e21	e18	e17	e16	e15	e14	e13	e12	e11	d58	d57	d56	d55	d54	d54	d54	d54	d54	d54	d54	
مؤلف																								
ابعاد																								

تایید	پیشگامان				تجربه				مؤلفه				ابعاد	
	تایید	تایید	تایید	تایید	تایید	تایید	تایید	تایید	تایید	تایید	تایید	تایید	تایید	تایید
تایید	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
تایید	0	0	0	0	0	0	0	0	0	0	0	0	0	0
تایید	5.906	5.916	5.906	5.906	5.906	5.906	5.906	5.906	5.906	5.906	5.906	5.906	5.906	5.906
تایید	0.743	0.655	0.743	0.743	0.743	0.743	0.743	0.743	0.743	0.743	0.743	0.743	0.743	0.743
تایید	4.133	4	4.133	4.133	4.133	4.133	4.133	4.133	4.133	4.133	4.133	4.133	4.133	4.133
تایید	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%
تایید	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%
تایید	0	0	0	0	0	0	0	0	0	0	0	0	0	0
تایید	8.264	5.916	8.264	8.264	8.264	8.264	8.264	8.264	8.264	8.264	8.264	8.264	8.264	8.264
تایید	0.59362	0.65465	0.59362	0.59362	0.59362	0.59362	0.59362	0.59362	0.59362	0.59362	0.59362	0.59362	0.59362	0.59362
تایید	4.2667	4	4.2667	4.2667	4.2667	4.2667	4.2667	4.2667	4.2667	4.2667	4.2667	4.2667	4.2667	4.2667
تایید	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%
تایید	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%
تایید	0	0	0	0	0	0	0	0	0	0	0	0	0	0
تایید	5.123	5.172	5.123	5.123	5.123	5.123	5.123	5.123	5.123	5.123	5.123	5.123	5.123	5.123
تایید	0.75593	0.79881	0.75593	0.75593	0.75593	0.75593	0.75593	0.75593	0.75593	0.75593	0.75593	0.75593	0.75593	0.75593
تایید	4	4.0667	4	4	4	4	4	4	4	4	4	4	4	4
تایید	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%
تایید	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%
تایید	0	0	0	0	0	0	0	0	0	0	0	0	0	0
تایید	8.5	10.583	8.5	8.5	8.5	8.5	8.5	8.5	8.5	8.5	8.5	8.5	8.5	8.5
تایید	0.5164	0.48795	0.5164	0.5164	0.5164	0.5164	0.5164	0.5164	0.5164	0.5164	0.5164	0.5164	0.5164	0.5164
تایید	4.1333	4.3333	4.1333	4.1333	4.1333	4.1333	4.1333	4.1333	4.1333	4.1333	4.1333	4.1333	4.1333	4.1333
تایید	e26	e27	e26	e26	e26	e26	e26	e26	e26	e26	e26	e26	e26	e26

برای تعیین اتفاق نظر میان اعضای پانل، علاوه بر شاخص های مرکزی شامل میانگین و انحراف استاندارد و... آزمون تی تک نمونه ای، CVI و CVR، از ضریب همبستگی کندال نیز استفاده شده است. مطابق جدول (۵)، ضریب همبستگی کندال که با نماد w نشان داده می شود، یک آزمون ناپارامتریک است و برای تعیین میزان همبستگی میان نظرات استفاده می شود. ضریب کندال بین ۰ و ۱ متغیر است. مقدار صفر، عدم توافق کامل و ۱، توافق کامل را نشان می دهد. نتایج دلفی نشان می دهد که اتفاق نظر اعضای پانل حاصل شده است و می توان به تکرار دورها پایان داد. با توجه به کمتر بودن مقدار سطح معنی داری از ۰/۰۵، می توان گفت که ضریب توافقی کندال معنادار بوده و در سطح اطمینان ۹۵٪ اتفاق نظر بین خبرگان در هر سه مرحله وجود داشته است. افزایش مقدار ضریب کندال در هر مرحله نسبت به مرحله قبل نیز گواه این مطلب می باشد.

جدول ۵- جمع بندی نهایی دلفی

دور اول دلفی	دور دوم دلفی
Kendall's W=0/319	Kendall's W=0/422
Chi-square=177/482	Chi-square=218/411
Sig=0/001	Sig=0/001

در نهایت، مطابق جدول (۶) مدل اندازه گیری (بارهای عاملی) و شاخص هم خطی بررسی گردید.

جدول ۶- (بارهای عاملی) و شاخص هم خطی

بعد	مؤلفه	شاخص	تحلیل عاملی تاییدی مرتبه اول				هم خطی
			بار عاملی	خطا	آماره تی	سطح معناداری	VIF
تهدیدات فیزیکی		a11	0.949	0.012	77.35	0.001	2.4995
		a12	0.972	0.007	149.104	0.001	2.096
		a13	0.953	0.011	89.624	0.001	2.8055

هم خطی	تحلیل عاملی تاییدی مرتبه اول				شاخص	مؤلفه	بعد			
	سطح معناداری	آماره تی	خطا	بار عاملی						
VIF										
3.849	0.001	54.803	0.017	0.937	a21	خسارت‌های غیر عمدی	تهدیدات امنیتی			
3.978	0.001	61.461	0.015	0.942	a22					
3.941	0.001	89.433	0.011	0.953	a23					
2.508	0.001	91.399	0.01	0.953	a24					
2.837	0.001	34.044	0.027	0.905	a25					
2.771	0.001	46.634	0.02	0.918	a26					
2.917	0.001	41.135	0.022	0.922	a27					
1.9885	0.001	27.45	0.032	0.886	a28					
2.637	0.001	29.774	0.03	0.901	a29					
3.657	0.001	54.753	0.017	0.934	a31	انسداد خدمت فعالیت مجرمانه		تهدیدات امنیتی		
3.5765	0.001	52.75	0.018	0.932	a32					
3.844	0.001	53.6	0.017	0.933	a33					
3.0805	0.001	53.37	0.017	0.929	a34					
3.9155	0.001	78.94	0.012	0.948	a35					
2.1165	0.001	71.865	0.013	0.949	a36					
2.3535	0.001	74.592	0.013	0.951	a37					
2.289	0.001	56.447	0.017	0.932	a38					
2.747	0.001	47.679	0.019	0.915	a41				سوءاستفاده	تهدیدات امنیتی
3.367	0.001	55.326	0.017	0.931	a42					
2.756	0.001	48.607	0.019	0.922	a43					
2.938	0.001	41.497	0.022	0.907	a44					
3.265	0.001	57.259	0.016	0.93	a45					
3.2785	0.001	65.797	0.014	0.935	a46					
3.1015	0.001	55.109	0.017	0.917	a47					
2.996	0.001	43.876	0.021	0.906	a48					
3.878	0.001	49.712	0.019	0.926	b11	ضعف در نگهداری منابع اطلاعاتی	سبب‌پذیری‌های امنیتی			
2.456	0.001	56.018	0.017	0.931	b12					
3.193	0.001	50.066	0.019	0.933	b13					
2.3275	0.001	62.27	0.015	0.946	b14					
3.5335	0.001	51.029	0.018	0.936	b15					
3.3245	0.001	54.453	0.017	0.936	b16					
2.4455	0.001	38.756	0.023	0.904	b17					
3.262	0.001	108.994	0.009	0.96	b21	دسترسی فیزیکی غیرمجاز			سبب‌پذیری‌های امنیتی	
1.4375	0.001	15.009	0.06	0.905	b22					
3.3245	0.001	88.657	0.011	0.961	b23					

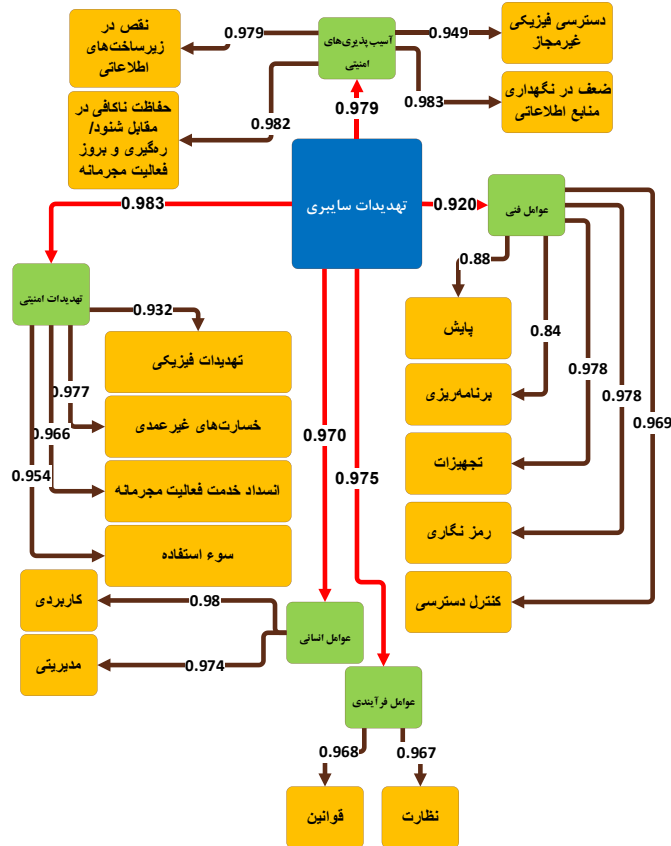
بهد	مؤلفه	شاخص	تحلیل عاملی تاییدی مرتبه اول				هم خطی
			بار عاملی	خطا	آماره تی	سطح معناداری	VIF
بعد	نقص در زیرساخت‌های اطلاعاتی	b31	0.896	0.023	38.209	0.001	2.077
		b32	0.887	0.027	33.15	0.001	2.8455
		b33	0.908	0.021	43.041	0.001	3.3495
		b34	0.906	0.022	41.101	0.001	2.197
		b35	0.915	0.019	47.167	0.001	2.9775
		b36	0.914	0.021	43.471	0.001	2.7145
		b37	0.915	0.021	43.051	0.001	2.8835
	حفاظت ناکافی در مقابل شنود/رهگیری و بروز فعالیت مجرمانه	b41	0.87	0.031	27.655	0.001	1.9805
		b42	0.933	0.021	45.297	0.001	3.35
		b43	0.923	0.019	48.065	0.001	2.9075
		b44	0.921	0.021	44.886	0.001	3.054
		b45	0.943	0.013	74.586	0.001	2.586
		b46	0.944	0.013	72.567	0.001	3.2615
		b47	0.952	0.012	78.898	0.001	3.5845
		b48	0.948	0.013	73.765	0.001	3.219
عوامل انسانی	کاربردی	c11	0.928	0.018	52.682	0.001	3.2995
		c12	0.924	0.017	53.973	0.001	3.237
		c13	0.891	0.031	29.001	0.001	2.813
		c14	0.903	0.024	37.665	0.001	3.1995
		c15	0.932	0.018	51.735	0.001	3.4625
		c16	0.922	0.017	55.624	0.001	3.2535
		c17	0.928	0.018	52.848	0.001	3.139
		c18	0.877	0.028	31.507	0.001	1.883
	مدیریتی	c21	0.889	0.026	34.3	0.001	1.862
		c22	0.911	0.022	41.896	0.001	2.325
		c23	0.924	0.022	42.405	0.001	3.1625
		c24	0.933	0.015	60.763	0.001	3.5815
		c25	0.94	0.014	67.502	0.001	3.4275
		c26	0.896	0.029	31.366	0.001	2.148
		c27	0.906	0.019	46.789	0.001	2.581
عوامل فنی	کنترل دسترسی	d11	0.95	0.014	69.31	0.001	3.996
		d12	0.952	0.011	82.91	0.001	3.481
		d13	0.968	0.007	131.943	0.001	2.636
		d14	0.962	0.008	117.493	0.001	3.221
		d15	0.925	0.019	47.673	0.001	3.212
		d16	0.939	0.014	67.861	0.001	3.877

هم خطی	تحلیل عاملی تاییدی مرتبه اول				شاخص	مؤلفه	بعد
	سطح معناداری	آماره تی	خطا	بار عاملی			
VIF							
3.357	0.001	57.263	0.016	0.935	d17	رمز نگاری	
1.9355	0.001	30.717	0.029	0.883	d18		
3.4045	0.001	49.869	0.019	0.936	d21		
3.583	0.001	67.712	0.014	0.942	d22		
3.8575	0.001	52.446	0.018	0.929	d23		
2.2495	0.001	69.385	0.014	0.949	d24		
2.6385	0.001	80.417	0.012	0.961	d25		
2.3165	0.001	60.274	0.016	0.936	d26		
3.267	0.001	75.901	0.013	0.949	d27		
3.2255	0.001	67.806	0.014	0.944	d28		
2.6915	0.001	35.742	0.025	0.906	d31	تجهیزات	
2.4375	0.001	33.637	0.027	0.894	d32		
3.3905	0.001	53.346	0.018	0.934	d33		
3.283	0.001	63.291	0.015	0.94	d34		
3.1465	0.001	43.679	0.021	0.926	d35		
3.2185	0.001	73.081	0.013	0.944	d36		
3.744	0.001	58.596	0.016	0.937	d37		
3.8025	0.001	58.001	0.016	0.934	d38		
3.191	0.001	78.516	0.012	0.953	d39		
0.978	0.001	9.196	0.08	0.734	d41		
1.484	0.001	9.857	0.078	0.765	d42		
1.0105	0.001	9.101	0.091	0.828	d43		
0.9365	0.001	9.506	0.08	0.757	d44		
0.9055	0.001	9.351	0.077	0.723	d45		
1.1885	0.001	9.008	0.085	0.763	d46		
1.187	0.001	9.997	0.046	0.459	d47		
1.263	0.001	9.05	0.053	0.48	d48		
0.778	0.001	9.89	0.067	0.663	d51	پایش	
0.883	0.001	9.958	0.071	0.709	d52		
1.1785	0.001	9.427	0.083	0.782	d53		
1.227	0.001	9.704	0.064	0.62	d54		
1.2685	0.001	9.001	0.078	0.698	d55		
1.0795	0.001	9.518	0.08	0.757	d56		
1.2565	0.001	9.259	0.091	0.845	d57		
1.361	0.001	9.397	0.082	0.768	d58		

بُعد	مؤلفه	شاخص	تحلیل عاملی تاییدی مرتبه اول				هم خطی
			بار عاملی	خطا	آماره تی	سطح معناداری	VIF
عوامل فرایندی	قوانین	e11	0.943	0.014	69.501	0.001	3.5555
		e12	0.91	0.023	39.323	0.001	2.9945
		e13	0.913	0.021	42.51	0.001	3.4655
		e14	0.931	0.017	55.499	0.001	3.399
		e15	0.892	0.025	35.087	0.001	2.2795
		e16	0.881	0.03	29.453	0.001	1.9735
		e17	0.913	0.021	44.015	0.001	2.8925
		e18	0.922	0.02	45.739	0.001	2.777
	نظارت	e21	0.939	0.017	56.498	0.001	3.772
		e22	0.915	0.021	43.152	0.001	3.116
		e23	0.849	0.033	25.821	0.001	1.773
		e24	0.936	0.018	53.403	0.001	3.542
		e25	0.911	0.022	41.869	0.001	2.5055
		e26	0.915	0.021	43.329	0.001	3.1175
		e27	0.863	0.039	22.185	0.001	1.649
		e28	0.918	0.019	47.105	0.001	3.347

۶. نتیجه گیری

برای هر مؤلفه، بار عاملی مرتبه دوم و سوم مطابق شکل (۳) محاسبه و ترسیم گردید. همان گونه که در پیشینه پژوهش حاضر به این موضوع اذعان شد که تصحیح الگوی رفتاری ارجح تر از راه حل های فنی است، در نتایج حاصل نیز کاملاً مشهود است که در تهدیدات سایبری، بُعد «عوامل فنی» کمترین وزن را داشته و بُعد «تهدیدات امنیتی» بالاترین وزن را دارد که در مؤلفه های آن، بالاترین وزن را مؤلفه «خسارت های غیر عمدی» دارد و بیانگر آن است که منشأ بسیاری از حملات سایبری عامل انسانی است که عموماً به صورت ناخواسته، زمینه را جهت نفوذ فراهم می کند. بنابراین، تبیین یک الگوی رفتاری صحیح می تواند از بسیاری خسارات آینده جلوگیری کند.



شکل ۳- بار عاملی مرتبه دوم و سوم برای هر مؤلفه

همان‌گونه که در بُعد «عوامل فرایندی» مشهود است، وزن مؤلفه «قوانین» از مؤلفه «نظارت» بیشتر است؛ به این معنی که نظارت دقیق بر اجرای قوانین نادرست، کمکی به بهبود شرایط نمی‌کند و از این رویکرد، تبیین قوانین برای اصلاح الگوی رفتاری کارشناسان امنیت اطلاعات بسیار حائز اهمیت است.

همچنین، در بُعد «عوامل فنی» مشهود است که «تجهیزات» و «رمزنگاری» وزن بالاتری نسبت به «پایش» دارد و این موضوع اثبات‌کننده این موضوع است که «بستر امن» یک محیط امن ایجاد می‌کند و نمی‌توان در بستر ناامن انتظار محیطی امن داشت. در واقع، بستر امن را فرهنگ و عوامل انسانی ایجاد می‌کنند و تجهیزات به‌تنهایی نمی‌توانند بستر امن ایجاد کنند. بنابراین، با فرهنگ‌سازی و ایجاد الگوی رفتاری صحیح که در ادامه پیشنهادهای آن آمده است، می‌توان به بستری امن رسید، تا سازمانی امن شکل گیرد.

مطابق جدول (۷)، نتایج این پژوهش با نتایج مطالعات شعبانی و همکاران (۱۴۰۰) مورد مقایسه قرار گرفته و همخوانی رتبه‌بندی‌های دو پژوهش حاکی از صحت و اعتبار بالای نتایج می‌باشد.

جدول ۷ - مقایسه نتایج این پژوهش از نظر رتبه‌بندی مؤلفه‌ها با نتایج مطالعات شعبانی (۱۴۰۰)

پژوهش حاضر		شعبانی (۱۴۰۰)	
مؤلفه	وزن مؤلفه عاملی	رتبه میانگین	مؤلفه
تهدیدات امنیتی	۰,۹۸۳	۱۶,۲۶	فرهنگ سازمانی
آسیب‌پذیری‌های امنیتی	۰,۹۷۹	۱۳	ساختار سازمانی
عوامل فرایندی (ساختار سازمانی)	۰,۹۷۵	۱۲,۱۱	منابع انسانی
عوامل انسانی	۰,۹۷۰	۱۱,۶۳	زیرساخت فناوری اطلاعات
عوامل فنی	۰,۹۲۰	۱۰,۹۸	آموزش و بازآموزی
		۹,۴۸	جنبه راهبردی و رهبری

۷. پیشنهادات

پیر و مشورت با خبرگان و با در نظر گرفتن منابع معتبر خوانده شده، برای رسیدن به الگوی رفتاری صحیح کارشناسان امنیت اطلاعات در مواجهه با تهدیدات سایبری، سرفصل‌های ذیل پیشنهاد می‌گردد.

کارشناسان می‌بایست در خصوص سرفصل‌ها و بُعدهای ذیل که به ترتیب وزن مرتب شده‌اند، در ۴ مرحله بازدارندگی، پیشگیرانه، آشکارسازی و اصلاحی، موارد پیشنهادی ذیل هر بُعد که آنها نیز به ترتیب وزن مرتب شده‌اند، را تبیین نمایند:

۱) تهدیدات امنیتی

۱. هوشیاری در مقابل خسارت‌های غیرعمدی ناشی از خطای انسانی (بیشترین وزن در تهدیدات امنیتی را دارد)،

۲. انسداد خدمت در صورت مشاهده فعالیت مجرمانه (رتبه دوم در تهدیدات امنیتی را دارد)،

۳. ایجاد حساسیت در ارکان سازمانی به منظور خنثی‌سازی سوءاستفاده‌های احتمالی مانند مهندسی اجتماعی،

۴. شناسایی و پایش مداوم تهدیدات فیزیکی و دسترسی‌های غیرمجاز سازمان (کمترین وزن در تهدیدات امنیتی را دارد).

۲) آسیب‌پذیری‌های امنیتی

۱. تدوین خط‌مشی و دستورالعمل نگهداری کارآمد از منابع اطلاعاتی (ضعف در نگهداری

منابع اطلاعاتی بیشترین وزن در آسیب‌پذیری‌های امنیتی را دارد)،

۲. تمهیدات لازم در حفاظت کافی در مقابل شنود اطلاعات و رهگیری در صورت بروز فعالیت مجرمانه (حفاظت ناکافی در مقابل شنود اطلاعات، دومین رتبه در آسیب‌پذیری‌های امنیتی را دارد)،
۳. طراحی و برنامه‌ریزی کارآمد در خصوص حفاظت از زیرساخت‌های اطلاعاتی،
۴. جلوگیری از دسترسی فیزیکی غیرمجاز با استفاده از ابزارهای احراز هویت و آموزش‌های لازم کارکنان (کمترین وزن در آسیب‌پذیری‌های امنیتی را دارد).

۳) عوامل فرایندی

۱. تدوین قوانین، خط‌مشی‌ها، دستورالعمل‌ها و استانداردهای امنیتی (در عوامل فرایندی قوانین نسبت به نظارت از وزن بالاتری برخوردار است)،
۲. عضویت و تعامل با انجمن‌های حرفه‌ای امنیت،
۳. ارزیابی و به‌روزرسانی منظم قوانین و خط‌مشی‌های سازمان،
۴. برنامه‌ریزی‌های آموزشی و آگاهی‌رسانی امنیتی،
۵. ایجاد رویه‌های تشخیص، گزارش‌دهی و پاسخ به رخداد و استفاده از چک‌لیست‌های امنیتی،
۶. طراحی معماری امن،
۷. رعایت اصول طبقه‌بندی داده‌ها و منابع اطلاعاتی،
۸. استفاده از روش‌های کارآمد در شناسایی و طبقه‌بندی دارایی‌ها،
۹. رعایت اصول جمع‌آوری، نظارت و تحلیل اطلاعات،
۱۰. بررسی مداوم صحت، محرمانگی و دسترسی‌پذیری اطلاعات سازمان،
۱۱. تدوین اصول پایش و کنترل کاربران،
۱۲. تعیین راهبردها در صورت عدم پیروی از خط‌مشی‌های امنیتی توسط کاربران،
۱۳. برنامه‌ریزی و بودجه‌بندی امنیتی سازمان و ارائه گزارش به مدیریت عالی،
۱۴. سازمان‌دهی قواعد استفاده از اینترنت توسط کاربران.

۴) عوامل انسانی

- ♦ بالاتر بودن وزن کاربردی از مدیریتی، نشان‌دهنده آن است که مدیریت صحیح به‌تنهایی کافی نبوده و بازوی اجرایی و کاربردی آن از وزن بالاتری برخوردار است.
۱. تدوین و اجرای برنامه‌های آموزشی در حوزه امنیت اطلاعات (تکنیک‌های نفوذ، هک، اخلاقیات، قوانین و مقررات، ممیزی و...)،
 ۲. فرهنگ‌سازی سازمانی در خصوص برنامه‌های امنیتی سازمان،

۳. ترغیب کارمندان سازمان به گزارش مخاطرات و مشکلات امنیتی،
۴. پذیرش مسئولیت‌های امنیتی سازمان،
۵. ایجاد روحیه تعهد و وفاداری کارمندان سازمان به رعایت ملاحظات امنیتی رایج،
۶. غربالگری و ارزیابی دوره‌ای کارمندان از منظر ملاحظات امنیت اطلاعات،
۷. همسو کردن کارکنان با خط‌مشی‌های امنیت اطلاعات سازمان،
۸. تلاش برای افزایش آگاهی کارکنان در زمینه امنیت اطلاعات،
۹. درک نیازهای امنیتی در سطوح مختلف سازمان،
۱۰. رفتار محافظه‌کارانه در زمینه امنیت سیستم‌های اطلاعاتی،
۱۱. پیروی از استانداردها و دستورالعمل‌های امنیتی،
۱۲. تعریف و پایش مداوم کاربری‌های مجاز سیستم و بررسی سطوح دسترسی،
۱۳. نظارت و پایش مستمر فعالیت‌های طرف ثالث در حوزه امنیت اطلاعات،
۱۴. همسو کردن مدیریت عالی به‌منظور حمایت از برنامه‌ها، پروژه‌ها و خط‌مشی‌های امنیتی سازمان.

۵) عوامل فنی

- ✦ در عوامل فنی، تجهیزات و رمزنگاری از بالاترین وزن برخوردار هستند:
- ۱. استفاده از پوششگرها و سیستم‌های بروز تشخیص نفوذ،
- ۲. ایمن‌سازی و مقاوم‌سازی فیزیکی و محیطی اماکن و فضاهای حساس،
- ۳. استفاده از امضاءهای دیجیتالی در سامانه‌های سازمانی و به‌کارگیری فناوری‌های نهان‌نگاری،
- ۴. استفاده از الگوریتم‌های رمزنگاری در زیرساخت اطلاعاتی،
- ۵. به‌کارگیری پروتکل‌های امنیت اطلاعات به‌منظور ایجاد ارتباط امن،
- ۶. استفاده دیواره آتش و سازوکار یکپارچه مدیریت تهدید،
- ۷. کنترل و کدگذاری رسانه‌های قابل حمل سازمانی و سامانه‌ها،
- ۸. استفاده مؤثر و کارا از سازوکار کنترل دسترسی و صدور مجوز،
- ۹. محدود کردن دسترسی کاربران در طرح سطح‌بندی اطلاعات،
- ۱۰. مدیریت ارتباطات در برون‌سپاری خدمات امنیتی،
- ۱۱. گمنام‌سازی داده‌ها و لینک‌های ارتباطی،
- ۱۲. مدیریت و تعیین خط‌مشی‌های حقوق دسترسی کاربران،
- ۱۳. حفاظت از منابع در مقابل دسترسی و نفوذ فیزیکی،

۱۴. حفظ محرمانگی و صیانت از صحت و یکپارچگی داده‌های سازمانی (امنیت اطلاعات سازمانی)،

۱۵. مدیریت، انتقال و نگهداری امن داده‌های سازمانی،

۱۶. تدوین سازوکار و بازرسی امنیت ارتباطات و تجهیزات ارتباطی،

۱۷. نظارت بر دسترسی افراد بیرونی به اطلاعات سیستم،

۱۸. نظارت و کنترل دسترسی طرف ثالث و پیمانکاران،

۱۹. استفاده از سیستم‌های پایش و سامانه‌های جامع نظارت اطلاعات سازمانی،

۲۰. سازوکار پالایش محتوا و پایش عملیات،

۲۱. ممیزی ادواری امنیت اطلاعات سازمانی،

۲۲. مدیریت انرژی (پشتیبان برق و مدیریت شرایط اضطرار و سامانه‌های اطفای حریق و اعلام هشدار حرارتی)،

۲۳. رعایت استانداردها و سازوکارهای کنترل دما و رطوبت دستگاه‌های الکترونیکی،

۲۴. پشتیبان‌گیری منظم از سیستم‌ها و بررسی دسترسی پذیری و ظرفیت حافظه پشتیبان.

منابع

- آهنگر، ع.، باب الحوائجی، ف.، حسینی بهشتی، م.س.، حریری، ن.، خادمی، م. (۱۴۰۱). ترسیم و تحلیل ساختار شبکه مفاهیم حوزه امنیت اطلاعات. *پژوهشنامه پردازش و مدیریت اطلاعات*، ۳۷(۲): ۴۷۳-۴۹۵.
<https://doi.org/10.52547/jipm.37.2.473>
- شاهینی، ش.، فرح پهلوی، ع.، خادمی زاده، ش.، نادران طحان، م. (۱۴۰۱). ارائه معماری پیشنهادی به کارگیری اینترنت اشیاء در کتابخانه های دانشگاهی ایران. *پژوهشنامه پردازش و مدیریت اطلاعات*، ۳۸(۱۱۴).
<https://doi.org/10.22034/JIPM.2023.701680>
- شعبانی، م.م.، رفعتی اصل، س.م.، سهرابی، ش. (۱۴۰۰). امکان سنجی استقرار مدیریت دانش در سازمان دانش محور. *فناوری اطلاعات/انتظامی*، ۴(۸): ۶۷-۸۴. ۱۱۴.۱۲۶۶۵۶۵.
<https://doi.org/10.22034/pitc.2022.1266565.1114.84-67>
- شفیعی نیک آبادی، م.، جعفریان، ا.، جلیلی بوالحسنی، ا. (۱۴۰۱). تأثیر مدیریت امنیت اطلاعات بر یکپارچگی فرآیندهای سازمانی در زنجیره تأمین. *پژوهشنامه پردازش و مدیریت اطلاعات*، ۲۷(۲): ۵۶۰-۶۰۴.
- شهریاری، م.، مددی، ب.، صابری، م. (۱۳۹۸). تحلیل چالش های امنیتی شبکه LTE، و موانع و فرصت های بومی سازی شبکه در بستر استاندارد. *پایفند الکترونیک و سایبری*، ۷(۲۶): ۱۲۱-۱۳۲.

References

- Ahangar, A., Babal-Hawaeji, F., Hosseini Beheshti, M.S., Hariri, N. & Khademi, M. (2022). Drawing and analyzing the network structure of information security concepts. *Journal of Information Processing and Management*, 37(2): 473-495. <https://doi.org/10.52547/jipm.37.2.473>[in persian]
- Alhogail, A. (2015). Design and validation of information security culture framework. *Computers in human behavior*, 49: 567-575.
- Bhattacharya, C.B., Sen, S. & Korschun, D. (2011). *Leveraging corporate responsibility: the stakeholder route to maximizing business and social value*. Cambridge University Press.
- 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.
- Deal, T. & Kennedy, A. (1999). *The new corporate cultures: revitalizing the workplace after downsizing, mergers, and reengineering*. Cambridge: Basic books.
- Dhillon, G. & Backhouse, J. (2000). Technical opinion: information system security management in the new millennium. *Communications of the acm*, 43(7): 125-128.
- merete Hagen, J., Albrechtsen, E. & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information management & computer security*, 16(4): 377-397.
- 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.
- Pathari, V. & Sonar, R. (2012). Identifying linkages between statements in information security policy, procedures and controls. *Information management & computer security*, 20(4): 264-280.
- ragavendran, V.A. (2023). An analysis of the literature on society's concerns on india's cybersecurity in the twenty-first century. *International journal of social sciences and management review*, Vol. 6.
- Scholl, M. (2023). Sustainable information security sensitization in smes: designing measures with

- long-term effect. *Proceedings of the 56th Hawaii International Conference on System Sciences*.
- Shabani, M.M., Rafati Asl, S.M. & Sohrabi, S. (2021). Feasibility of establishing knowledge management in a knowledge-oriented organization. *Law enforcement information technology magazine*, 4(8): 67-84. <https://doi.org/10.22034/pitc.2022.1266565.1114> [in persian]
- Shafii Nikabadi, M., Jafarian, A. & Jalili Boalhasani, A. (2022). The effect of information security management on the integration of organizational processes in the supply chain. *Journal of Information Processing and Management*, 27(2): 560-604. [in persian]
- Shahini, Sh., Faraj Pahló, A., Khademizadeh, Sh. & Nadran Tahan, M. (2022). Presenting a proposed architecture for using the Internet of Things in Iranian academic libraries. *Journal of information processing and management*, 37(2): 473-495. <https://doi.org/10.22034/JIPM.2023.701680> [in persian]
- Shahriari, M., Maddi, B. & Saberi, M. (2018). Analysis of security challenges of LTE network, and barriers and opportunities of network localization in the standard platform. *Electronic and Cyber Defense*, 7(26): 121-132. [in persian]
- Thomson, K. & Van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security*, 20(1): 39-46.