Sciences and Techniques of Information Management
Volume 9, Issue 4, 2023
University of Qom

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

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

Sedigheh MohammadEsmaeil
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
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

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.

علوم و فنون مدیریت اطلاعات
دوره ۹، شماره ٤، ۱٤۰۲

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

محمدباقر رایین آبرومند
دانشجو دکتری، گروه علم اطلاعات و دانش‌شناسی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران.
ITmanager@tsfc.ir
صدیقه محمداسماعیل
دانشیار، گروه علم اطلاعات و دانش‌شناسی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران (نویسنده مسئول). Sm.esmaili2@gmail.com
داریوش مطلبی
دانشیار، گروه علوم تربیتی، واحد یادگار امام خمینی شهرری، 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 خطرها را آموزش می‌دهند، دنیای اطلاعات با وجود هکرها[1] 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 مواجه با تهدیدات سایبری انجام شده است.

روش: در این پژوهش با هدف و رویکرد کاربردی- توسعه‌ای، به کمک روش فراترکیب و کیفی- کمّی (متوالی- اکتشافی)، ابتدا به روش کتابخانه‌ای، از ۲۷۰ 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

نوع مقاله: پژوهشی **ناشر:** دانشگاه قم

۱. نفوذگرها

شناسایی مؤلفه‌های امنیت سیستم‌های اطلاعاتی، از تکنیک هفت مرحله‌ای باروسو[1] و ساندلوسکی[2] (۲۰۰۷) استفاده شده است. ۱۴۲ شاخص از اسناد غربال شده احصاء گردید و پس از خوشه‌بندی شاخص‌ها به کمک نرم‌افزار رپید ماینر، ابعاد و مولفه‌های 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 کمّی 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.[3] و متلب[4] 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 مولفه‌های 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 مولفه‌های «رمزنگاری» و «تجهیزات» با امتیاز ۰٫۹۷۸ به خود اختصاص داده و پایین‌ترین امتیاز را مولفه‌های «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 مولفه‌ها 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.

1. Barroso
2. Sandlowski
3. SPSS
4. MATLAB

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، به‌گونه‌ای درگیر فرهنگ دنیای دیجیتال هستیم. از بارزترین نمونه این درگیری، انواع کلاهبرداری‌های اینترنتی ازجمله فیشینگ[1] 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 بیش‌ازپیش احساس می‌شود (Pathari & Sonar, 2012).

به گزارش شرکت پی.سی.اچ. تکنولوژی[2] 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 صورتی‌که 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 خط‌مشیء و تصحیح ساختار سازمانی احساس می‌شود. از سوی دیگر، تصمیم‌گیری فرایندی بسیار مهم و پایه‌ای در فعالیت‌های

1. Phishing
2. PCHtechnologies

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

استدلال می‌شود که توسعه فرهنگ امنیت اطلاعات متعاقباً به یک سازمان امن منجر خواهد شد. بااین‌حال، مطالعات محدودی برای درک فرهنگ امنیت اطلاعات انجام شده است. فرهنگ ایده‌آل یا قوی امنیت اطلاعات می‌تواند در به‌حداقل رساندن تهدید انسان‌ها به حفاظت از اطلاعات و در نتیجه کمک در کاهش نقض داده‌ها یا حوادث در سازمان‌ها کمک کند. تقریباً همه سازمان‌ها اطلاعات حساس را به شکلی جمع‌آوری و نگهداری می‌کنند. برخی از سازمان‌های دولتی کنترل‌های نظارتی بر استفاده و توزیع انواع خاصی از اطلاعات حساس ایجاد کرده‌اند. برخی از سازمان‌های جنایی با مهارت‌های فنی پیشرفته سازمان‌دهی می‌شوند و مصمم هستند که به‌طور 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 سازمان‌های امروزی است. اگر اشتباهی در الگوی رفتاری یا استانداردهای اخلاقی یک کارشناس امنیت اطلاعات وجود داشته باشد، ممکن است منجربه 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 ریسک‌ها، در دسترسی کاربران به اطلاعات امن، مطمئن و محرمانه است و برای اطمینان از امنیت آن، سازمان باید سیاست‌ها و خط‌مشی‌های امنیت اطلاعات را شناسایی و تبیین کند. شکست‌های مداوم امنیت اطلاعات در سازمان‌ها باعث تمرکز بیشتر بر فرهنگ سازمانی شده است. همچنین، یکی دیگر از نگرانی‌های بزرگ برای امنیت اطلاعات یک سازمان، رفتار کارکنان است؛ زمانی که برای سیاست امنیت اطلاعات ارزش قائل نیستند و از آن مهم‌تر رفتار کارشناسان امنیت اطلاعات می‌باشد. عدم رعایت سیاست‌های امنیتی سیستم‌های اطلاعاتی کارشناسان امنیت اطلاعات یک نگرانی عمده برای مدیران امنیت فناوری اطلاعات است. سازمان‌ها به سیاست‌ها و شیوه‌های امنیت اطلاعات برای ایجاد مدیریت مناسب و استفاده از اطلاعات حساس به‌منظور کاهش خطرات مرتبط نیاز دارند. سیاست‌های امنیت اطلاعات فقط به‌اندازه افرادی که باید آنها را اعمال کنند، مؤثر هستند (Niekerk & Solms, 2005). فرهنگ یک سازمان تأثیر زیادی بر ارزش‌ها، اسطوره‌ها، قهرمانان و نمادهای کارمندان دارد که برای کارمند معنا می‌بخشد (Deal & Kennedy, 1999). این امکان وجود دارد که سیستم‌ها و نمادهای ارزش فرهنگی بتوانند بر نگرش کارکنان نسبت به

سیاست‌های امنیت اطلاعات سازمان تأثیر بگذارند. در بسیاری از سازمان‌ها، خط‌مشی‌ءها 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، موردنیاز 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

باتوجه‌به گسترش استفاده از اینترنت، تبادلات اطلاعاتی و هزینه‌های صرف شده به‌منظور یکپارچگی اطلاعاتی، امروزه مبحث و مدیریت جابه‌جایی‌های اطلاعاتی و برخورداری از سامانهٔ جامعی برای مدیریت امنیت اطلاعات، بیش‌ازپیش احساس می‌شود (شهریاری و همکاران، ۱۳۹۸). اکثر قریب به‌اتفاق 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. علاوه‌بر 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 آهنگر 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. بااین‌حال، 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، ۱۲٤ 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). بااین‌حال 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 شفیعی نیک‌آبادی و همکاران (۱٤۰۱)، به‌کارگیری سامانه مدیریت امنیت اطلاعات، موجب افزایش یکپارچگی فرایندهای سازمانی در زنجیره تأمین و از آن‌رو، موجب افزایش یکپارچه‌سازی زنجیره تأمین می‌شود و درنتیجه، 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 صحّت 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[1] 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

1. Bhattacharya

بودن و یکپارچگی سیستم‌های اطلاعاتی با جلوگیری یا کاهش تلفات دارایی ناشی از تهدیدات امنیت سایبری کمک می‌کند (Ragavendran, 2023). مارگیت شول[1] 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).

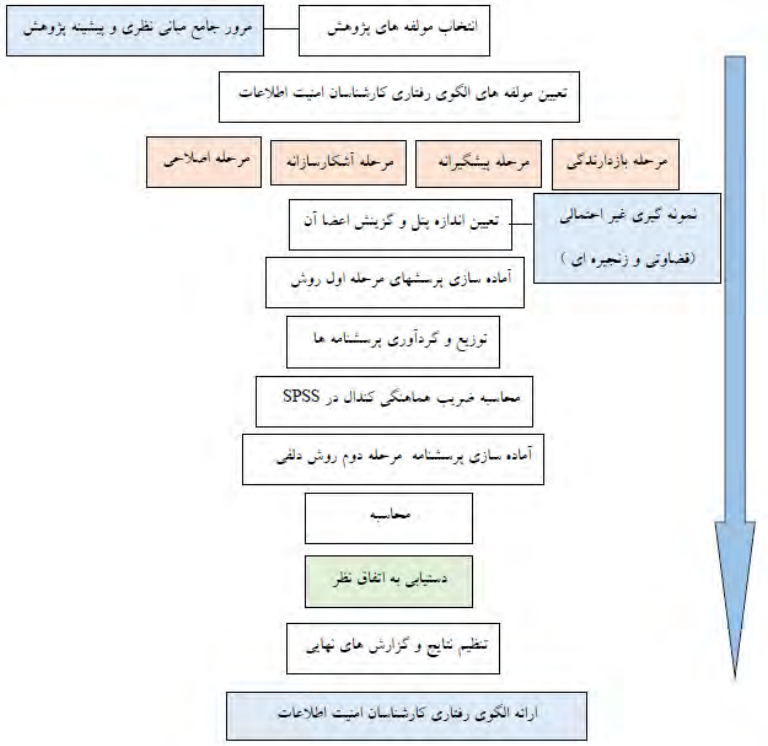
بررسی پیشینه پژوهش حاضر حاکی از آن است که برای ارتقای امنیت اطلاعات، با وجود اهمیت عامل انسانی، رجوع به راه‌حل‌های فنی، صرفاً پاک کردن صورت‌مسئله است و راه‌حل حقیقی کاهش خطای انسانی، و تبیین الگوی صحیح رفتاری می‌باشد. برای اثبات این موضوع در پژوهش حاضر به کمک روش دلفی و پیمایشی، نتایج مورد تحلیل و ارزیابی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

1. M Scholl



شکل ۱- مراحل روش دلفی

۴-۱. جامعه آماری

۴-۱-۱. جامعه آماری کیفی (دلفی)

بنابر کیفی- کمّی بودن ماهیت پژوهش حاضر، برای انتخاب نمونه آماری کیفی و تعیین حجم نمونه تعداد خبرگان مشارکت‌کننده 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. در پژوهش حاضر 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. پس از تعیین انواع مشارکت‌کنندگان، به‌منظور تعیین تعداد مشارکت‌کنندگان و اطمینان از دسترسی به داده‌های موردنیاز 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. از میان افراد معرفی شده، ۵۸ نفر واجد شرایط تشخیص داده شدند. انتخاب افراد برای فرایند دلفی در این پژوهش، وابسته به تجربه‌ها و تخصص‌های موردنیاز 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.

۴-۱-۲. جامعه آماری کمّی (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.

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

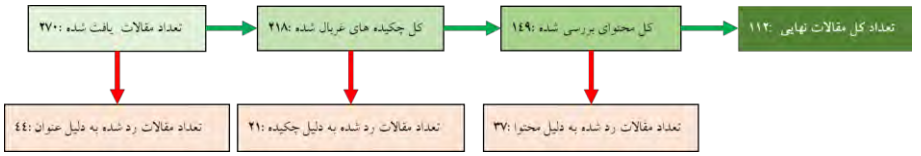
در این فرمول N حجم جامعه آماری و آماره p درصد توزیع صفت در جامعه، یعنی نسبت افرادی است که دارای صفت مورد مطالعه هستند و آماره q نیز درصد افرادی است که فاقد صفت مورد مطالعه هستند که اگر میزان p و q مشخص نباشد، از حداکثر مقدار آنها، یعنی ۰/۵ استفاده می‌شود. در سطح خطای ۵٪ مقدار z برابر ۱/۹۶ و Z^2 برابر 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 مواجه 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 چیستی 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 آنجایی‌که 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 مواجه 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[1]، ابعاد و مؤلفه‌ها از شاخص‌های تخصصی الگوی رفتاری در مواجه با تهدیدات سایبری و امنیتی، انتخاب و مورد تأیید اعضای خبرگان قرار گرفت. مؤلفه‌های «تهدیدات امنیتی» در ٦ بخش تهدیدات فیزیکی (عمدی/ غیرعمدی)، خسارت‌های غیرعمدی (مخدوش شدن منابع اطلاعاتی)، شکست و خرابی، انسداد خدمت، فعالیت مجرمانه /سوءاستفاده و تهدیدات قانونی تقسیم می‌شود. مولفه‌های «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 مولفه‌های 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 دسترس‌پذیری تقسیم می‌شود.

جدول ۱ - فراوانی عناوین شاخص‌ها در مراحل پژوهش

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

براساس فرایند فوق، ابتدا ۱٤۲ شاخص در ۵ بعد تهدیدات امنیتی شامل ۳٦ شاخص، آسیب‌پذیری‌های امنیتی و سایبری شامل ۳۱ شاخص، مولفه‌های انسانی شامل ۱۵ شاخص، مولفه‌های فنی شامل ٤۳ شاخص و مولفه‌های فرایندی شامل ۱۷ شاخص، جمع‌آوری گردید که شاخص‌های اصلی برای اجرای دلفی در نظر گرفته شد.

1. RapidMiner

۵. نتایج

۵-۱. روش دلفی

در پژوهش حاضر الگوی رفتاری کارشناسان امنیت اطلاعات در مواجه 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 شرکت‌کننده 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، پیشگیرانه، 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 قابل‌قبول 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 نظرگر فتن 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.

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

جدول ۳- نتایج دور اول دلفی

مؤلفه	کد	نام شاخص	تعداد پاسخ	میانگین	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	ازدست‌رفتن/ تخریب/ مخدوش‌شدن دارایی	۱۵	4.2	0.414	11.225	0	87%	73%	تأیید
شکست/ خرابی	q16	خرابی یا اختلال لینک‌ها/ شبکه‌های ارتباطی	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	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
انسداد خدمت فعالیت مجرمانه/ سو استفاده	q19	استراق سمع در مسیر انتقال داده‌ها/ سرقت نشست/ رهگیری اطلاعات محرمانه	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

مؤلفه	کد	نام شاخص	تعداد پاسخ	میانگین	انحراف معیار	آماره تی	سطح معناداری	CVR	CVI	تغییرات کیفی
	q27	دستکاری سخت‌افزار و نرم‌افزار	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 راه‌اندازی غیرمجاز نرم‌افزار	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
	q34	جستجوی جامع	۱۵	2.933	0.258	-1	0.334	60%	20%	حذف
تهدیدات قانونی	q35	استفاده غیرمجاز از منابع حفاظت شده	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q36	سوءاستفاده از داده‌های خصوصی	۱۵	4.333	0.488	10.583	0	100%	100%	تأیید
دسترسی فیزیکی غیرمجاز (عمدی/سهوی)	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 دستگاه‌های 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	پیکربندی ضعیف سامانه	۱۵	4.267	0.458	10.717	0	100%	100%	تأیید
	q44	ارزیابی امنیتی ناکارآمد فناوری‌ها	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
	q45	خط‌مشی‌ء و دستورالعمل‌های ناکارآمد	۱۵	4	0.378	10.247	0	93%	87%	تأیید
محیطی	q46	سازوکار نادرست در قفل‌گذاری منابع	۱۵	4	0.845	4.583	0	80%	60%	تأیید
	q47	مکان‌یابی 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 شکست / 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 برنامه‌ریزی 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 ناکافی در مقابل شنود/ رهگیری	q56	وجود شبکه ارتباطی بی‌سیم 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 مجرمانه /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 به‌کارگیری الگوریتم‌های معتبر رمزنگاری	۱۵	4.267	0.458	10.717	0	100%	100%	تأیید
	q62	امکان دستکاری در ورودی‌ها	۱۵	2.6	0.507	-3.055	0.009	53%	7%	حذف
	q63	ضعف در مواجهه با روش‌های مهندسی اجتماعی	۱۵	4.2	0.414	11.225	0	80%	60%	تأیید
	q64	ضعف در شناسایی شبکه‌های طعمه و فعالیت‌های مخرب	۱۵	4.2	0.414	11.225	0	93%	87%	تأیید
مسائل قانونی	q65	حفاظت ناکافی در مقابل چالش‌های 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 خط‌مشی‌های امنیت اطلاعات سازمان	۱۵	4.333	0.488	10.583	0	87%	73%	تأیید
	q69	حمایت مدیریت عالی از برنامه‌ها، پروژه‌ها و خط‌مشی‌های 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 محافظه‌کارانه کاربران در زمینه امنیت سیستم‌های اطلاعاتی	۱۵	4.133	0.352	12.475	0	100%	100%	تأیید
	q73	پیروی از استانداردها و دستورالعمل‌های امنیتی	۱۵	4.067	0.458	9.025	0	93%	87%	تأیید
	q74	حس پاسخگویی، خودارزیابی و خودگزارش‌دهی	۱۵	4.2	0.414	11.225	0	100%	100%	تأیید
	q75	تدوین و اجرای برنامه‌های 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 مسئولیت‌های 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	آماره تی	سطح معناداری	CVR	CVI	تغییرات کیفی
	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
عوامل فنی	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 مجور 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
	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	کابل‌کشی امن مابین سیستم ها/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	تعداد پاسخ	میانگین	انحراف معیار	آماره تی	سطح معناداری	CVR	CVI	تغییرات کیفی
	q104	استفاده از پویشگرها 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 صحّت و یکپارچگی داده‌ها	۱۵	4.6	0.507	12.22	0	93%	87%	تأیید
	q108	امضاءهای دیجیتالی	۱۵	4.467	0.516	11	0	100%	100%	تأیید
	q109	فناوری‌های نهان‌نگاری	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 فرایندی	q126	استفاده از چک‌لیست‌های امنیتی	۱۵	4.6	0.507	12.22	0	100%	100%	تأیید
	q127	تدوین قوانین، خط‌مشی‌ءها، 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 خط‌مشی‌ءهای 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	تغییرات 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 دسترس‌پذیری	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 شاخص روایی (مقدار سی وی آی بالای ۴۹%

و مقدار سی وی آر بالای ۶۰%) و معنادار از منظر آزمون تی تک نمونه‌ای (در تمامی شاخص‌ها مقدار میانگین بالاتر از ۳ و مقدار سطح معناداری کمتر از ۵%) هستند.

جدول ٤- نتایج دور دوم دلفی

ابعاد	مؤلفه	شاخص	مرحله بازدارندگی						مرحله پیشگیرانه						مرحله آشکارسازی						مرحله اصلاحی						نتیجه
			میانگین	انحراف معیار	آماره تی	سطح معناداری	cvr	cvi	میانگین	انحراف معیار	آماره تی	سطح معناداری	cvr	cvi	میانگین	انحراف معیار	آماره تی	سطح معناداری	cvr	cvi	میانگین	انحراف معیار	آماره تی	سطح معناداری	cvr	cvi	
تهدیدات امنیتی	تهدیدات فیزیکی	a11	3.9333	0.88372	4.09	0.001	87%	73%	4.1333	0.5164	8.5	0	87%	73%	4.0667	0.59362	6.959	0	93%	87%	3.867	0.516	6.5	0	100%	100%	تأیید
		a12	3.9333	0.70373	5.137	0	93%	87%	3.8667	0.83381	4.026	0.001	93%	87%	3.9333	0.70373	5.137	0	87%	73%	3.933	0.704	5.137	0	87%	73%	تأیید
		a13	3.8	0.86189	3.595	0.003	93%	87%	3.8	0.94112	3.292	0.005	93%	87%	4.0667	0.70373	5.87	0	93%	87%	4.267	0.704	6.971	0	93%	87%	تأیید
	خسارت‌های غیرعمدی	a21	3.9333	0.59362	6.089	0	93%	87%	3.6667	0.9759	2.646	0.019	87%	73%	4.2	0.86189	5.392	0	87%	73%	4.067	0.799	5.172	0	93%	87%	تأیید
		a22	4.2	0.7746	6	0	100%	100%	4.2	0.86189	5.392	0	93%	87%	4.4	0.63246	8.573	0	87%	73%	4.133	0.743	5.906	0	87%	73%	تأیید
		a23	3.7333	0.59362	4.785	0	93%	87%	3.8667	0.83381	4.026	0.001	87%	73%	4.1333	0.83381	5.264	0	87%	73%	4.333	0.724	7.135	0	87%	73%	تأیید
		a24	3.7333	0.79881	3.556	0.003	93%	87%	3.8667	0.91548	3.666	0.003	87%	73%	4.0667	0.88372	4.675	0	100%	100%	4.333	0.816	6.325	0	87%	73%	تأیید
		a25	3.8667	0.74322	4.516	0	80%	60%	3.8667	0.91548	3.666	0.003	87%	73%	4.3333	0.72375	7.135	0	100%	100%	4.333	0.617	8.367	0	80%	60%	تأیید
		a26	3.8667	0.5164	6.5	0	87%	73%	4	0.65465	5.916	0	100%	100%	4	0.75593	5.123	0	87%	73%	4.267	0.704	6.971	0	80%	60%	تأیید
		a27	3.8667	0.63994	5.245	0	93%	87%	3.9333	0.79881	4.525	0	100%	100%	4	0.75593	5.123	0	93%	87%	4.133	0.743	5.906	0	80%	60%	تأیید
		a28	4.2667	0.59362	8.264	0	100%	100%	4	0.84515	4.583	0	87%	73%	4.2667	0.70373	6.971	0	93%	87%	4.467	0.64	8.876	0	93%	87%	تأیید
		a29	4.3333	0.61721	8.367	0	100%	100%	4.0667	0.79881	5.172	0	93%	87%	4.3333	0.61721	8.367	0	87%	73%	4.2	0.775	6	0	80%	60%	تأیید
	انسداد خدمت فعالیت مجرمانه	a31	4.0667	0.70373	5.87	0	93%	87%	3.8	0.94112	3.292	0.005	93%	87%	4.2	0.7746	6	0	87%	73%	4.267	0.799	6.141	0	87%	73%	تأیید
		a32	4	0.92582	4.183	0.001	93%	87%	4.2	0.56061	8.29	0	87%	73%	4.2667	0.70373	6.971	0	87%	73%	4.267	0.704	6.971	0	73%	47%	تأیید
		a33	4.2	0.7746	6	0	93%	87%	3.9333	0.96115	3.761	0.002	87%	73%	4.3333	0.72375	7.135	0	80%	60%	4.2	0.775	6	0	93%	87%	تأیید

	نتیجه	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید
مرحله اصلاحی	cvi	73%	73%	73%	73%	87%	87%	87%	87%	73%	73%	73%	60%	60%	60%	73%	73%	87%	73%	73%	87%
	cvr	87%	87%	87%	87%	93%	93%	93%	93%	87%	87%	87%	80%	80%	80%	87%	87%	93%	87%	87%	93%
	سطح معناداری	0	0.002	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	آماره تی	5.264	3.761	5.264	5.906	5.87	7.359	5.392	5.264	4.583	5.906	11	11	5.916	5.906	5.264	3.761	5.264	6.959	5.906	4.525	6.971	5.551
	انحراف معیار	0.834	0.961	0.834	0.743	0.704	0.737	0.862	0.834	0.845	0.743	0.516	0.516	0.655	0.743	0.834	0.961	0.834	0.594	0.743	0.799	0.704	0.884
	میانگین	4.133	3.933	4.133	4.133	4.067	4.4	4.2	4.133	4	4.267	4.467	4.467	4	4.133	4.133	3.933	4.133	4.067	4.133	3.933	4.267	4.267
مرحله آشکارسازی	cvi	60%	60%	87%	60%	87%	73%	60%	73%	60%	73%	87%	47%	73%	60%	87%	60%	60%	73%	73%	87%	87%	87%
	cvr	80%	80%	93%	80%	87%	87%	80%	87%	80%	87%	93%	73%	87%	80%	93%	80%	80%	87%	87%	93%	93%	93%
	سطح معناداری	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.001	0	0
	آماره تی	6	4.795	5.906	5.264	5.87	8.876	5.392	6.141	5.172	6.971	11	8.573	5.87	5.264	5.906	4.795	6	8.5	6.874	4	8.876	6.548
	انحراف معیار	0.7746	0.91548	0.74322	0.83381	0.70373	0.63994	0.86189	0.79881	0.79881	0.70373	0.5164	0.63246	0.70373	0.83381	0.74322	0.91548	0.7746	0.5164	0.67612	0.7746	0.63994	0.82808
	میانگین	4.2	4.1333	4.1333	4.1333	4.2667	4.4667	4.2	4.2667	4.0667	4.2667	4.4667	4.4	4.0667	4.1333	4.1333	4.1333	4.2	4.1333	4.2	3.8	4.4667	4.4
مرحله پیشگیرانه	cvi	73%	60%	60%	60%	87%	47%	73%	60%	60%	73%	73%	73%	87%	60%	60%	60%	73%	87%	87%	87%	60%	60%
	cvr	87%	80%	80%	80%	93%	73%	87%	80%	80%	87%	87%	87%	93%	80%	80%	80%	87%	93%	93%	93%	80%	80%
	سطح معناداری	0	0.002	0	0.003	0	0.016	0	0	0.003	0.001	0.001	0	0	0.003	0	0.002	0	0	0	0.015	0.003	0.036
	آماره تی	4.675	3.761	6.141	3.666	10.693	2.75	6.325	11	3.556	4.09	4.298	5.551	6.859	3.666	6.141	3.761	4.675	11.225	5.123	2.779	3.666	2.32
	انحراف معیار	0.88372	0.96115	0.79881	0.91548	0.50709	1.0328	0.8165	0.5164	0.79881	0.88372	0.96115	0.88372	0.63994	0.91548	0.79881	0.96115	0.88372	0.41404	0.75593	0.74322	0.91548	1.1127
	میانگین	4.0667	3.9333	4.2667	3.8667	4.4	3.7333	4.3333	4.4667	4.1333	3.8667	4.2667	3.9333	4.1333	3.8667	4.2667	3.9333	4.0667	4.2	4	3.5333	3.8667	3.6667
مرحله بازدارندگی	cvi	73%	73%	73%	73%	87%	100%	60%	87%	60%	73%	87%	87%	73%	100%	73%	73%	73%	73%	73%	73%	73%	60%
	cvr	87%	87%	87%	87%	93%	100%	80%	93%	80%	87%	93%	93%	87%	100%	87%	87%	87%	87%	87%	87%	87%	80%
	سطح معناداری	0	0	0	0	0.022	0.003	0	0.001	0.001	0.002	0	0	0.003	0.001	0	0	0	0	0.01	0	0.012	0.004
	آماره تی	5.172	5.137	6.874	4.036	2.567	3.595	6.325	4.432	4.183	3.761	5.392	5.264	3.595	4.036	6.874	5.137	5.172	12.475	2.955	4.785	2.87	3.389
	انحراف معیار	0.79881	0.70373	0.67612	0.70373	1.20712	0.86189	0.8165	0.99043	0.61721	0.96115	0.86189	0.83381	0.86189	0.70373	0.67612	0.70373	0.79881	0.35187	0.96115	0.59362	0.89974	0.99043
	میانگین	4.0667	3.9333	4.2	3.7333	3.8	3.8	4.3333	4.1333	3.6667	3.9333	4.2	4.1333	3.8	3.7333	4.2	3.9333	4.0667	4.1333	3.7333	3.7333	3.6667	3.8667
	شاخص	a34	a35	a36	a37	a38	a41	a42	a43	a44	a45	a46	a47	a48	b11	b12	b13	b14	b15				
	مؤلفه						سوءاستفاده								ضعف در نگهداری منابع اطلاعاتی								
	ابعاد														آسیب‌پذیری‌های امنیتی								

نتیجه		تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید
مرحله اصلاحی	cvi	73%	87%	73%	87%	87%	73%	73%	87%	73%	73%	73%	87%	87%	73%	60%	73%	87%
	cvr	87%	93%	87%	93%	93%	87%	87%	93%	87%	87%	87%	93%	93%	87%	80%	87%	93%
	سطح معناداری	0	0	0	0	0.001	0	0	0	0	0	0	0	0	0.003	0	0	0
	آماره تی	7.135	6.089	4.516	6.141	5.123	4.785	4.183	8.367	5.172	8.367	4.583	3.674	5.906	13.229	14.666	8.367	4.583
	انحراف معیار	0.724	0.594	0.743	0.799	0.756	0.594	0.617	0.617	0.799	0.617	0.845	0.632	0.743	0.488	0.458	0.617	0.845
	میانگین	4.333	3.933	3.867	4.267	4	3.733	3.667	4.333	4.067	4.333	4	3.6	4.133	4.667	4.733	4.333	4
مرحله آشکارسازی	cvi	73%	73%	87%	73%	73%	87%	73%	73%	87%	73%	73%	73%	73%	73%	87%	87%	73%
	cvr	87%	87%	93%	87%	87%	93%	87%	87%	93%	87%	87%	87%	87%	87%	93%	93%	87%
	سطح معناداری	0	0	0	0	0	0	0	0	0	0	0	0.001	0	0	0	0	0
	آماره تی	6	5.916	5.245	5.172	5.87	5.137	5.527	8.876	8.876	8.876	5.906	4.036	5.906	14.666	16.837	8.876	5.906
	انحراف معیار	0.7746	0.65465	0.63994	0.79881	0.70373	0.70373	0.56061	0.63994	0.63994	0.63994	0.74322	0.70373	0.74322	0.45774	0.41404	0.63994	0.74322
	میانگین	4.2	4	3.8667	4.0667	4.0667	3.9333	3.8	4.4667	4.4667	4.4667	4.1333	3.7333	4.1333	4.7333	4.8	4.4667	4.1333
مرحله پیشگیرانه	cvi	73%	73%	73%	73%	87%	73%	73%	87%	73%	73%	73%	73%	87%	87%	73%	87%	73%
	cvr	87%	87%	87%	87%	93%	87%	87%	93%	87%	87%	87%	87%	93%	93%	87%	93%	87%
	سطح معناداری	0	0	0	0.068	0.003	0	0	0	0	0	0.001	0	0	0	0	0	0
	آماره تی	5.264	5.245	5.137	1.974	3.666	6.859	4.583	9.28	8.367	4.026	5.392	4.583	6.971	7.122	5.137	5.392	4.026
	انحراف معیار	0.83381	0.63994	0.70373	0.91548	0.91548	0.63994	0.67612	0.63994	0.61721	0.83381	0.86189	0.50709	0.70373	0.83381	1.0556	0.86189	0.83381
	میانگین	4.1333	3.8667	3.9333	3.4667	3.8667	4.1333	3.8	4.5333	4.3333	3.8667	4.2	3.6	4.2667	4.5333	4.4	4.2	3.8667
مرحله بازدارندگی	cvi	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	87%	73%	100%	87%	100%
	cvr	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	93%	87%	100%	93%	100%
	سطح معناداری	0	0	0	0.001	0.001	0.002	0.005	0	0	0.033	0.001	0	0.002	0.001	0.001	0.001	0.033
	آماره تی	4.525	10.247	6.5	4.036	4.026	3.761	3.292	4.75	4.583	2.358	4.294	6.5	3.756	4.183	4.012	4.294	2.358
	انحراف معیار	0.79881	0.37796	0.5164	0.70373	0.83381	0.96115	0.94112	1.0328	1.01419	0.98561	1.08233	0.5164	1.09978	1.23443	1.2228	1.08233	0.98561
	میانگین	3.9333	4	3.8667	3.7333	3.8667	3.9333	3.8	4.2667	4.2	3.6	4.2	3.8667	4.0667	4.3333	4.2667	4.2	3.6
شاخص		b16	b17	b21	b22	b23	b31	b32	b33	b34	b35	b36	b37	b42	b41	b45	b44	b43
مؤلفه				دسترسی فیزیکی غیرمجاز			نقص در زیرساخت‌های اطلاعاتی							حفاظت ناکافی در مقابل شنود/ره‌گیری و بروز فعالیت مجرمانه				
ابعاد																		

نتیجه		تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید
مرحله اصلاحی	cvi	73%	73%	87%	60%	60%	87%	60%	87%	60%	73%	60%	73%	73%	87%	87%	60%	87%	87%
	cvr	87%	87%	93%	80%	80%	93%	80%	93%	73%	87%	80%	87%	87%	93%	93%	80%	93%	93%
	سطح معناداری	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	آماره تی	8.29	6.859	5.392	8.411	5.87	8.367	6	4.583	7.135	6.859	6.874	6.874	8.573	8.573	6.859	4.583	8.367	8.573
	انحراف معیار	0.561	0.64	0.862	0.737	0.704	0.617	0.775	0.845	0.724	0.64	0.676	0.676	0.632	0.632	0.64	0.845	0.617	0.632
	میانگین	4.2	4.133	4.2	4.6	4.067	4.333	4.2	4	4.333	4.133	4.2	4.2	4.4	4.4	4.133	4	4.333	4.4
مرحله آشکارسازی	cvi	73%	47%	60%	73%	87%	87%	87%	73%	73%	87%	60%	60%	73%	87%	47%	73%	60%	87%
	cvr	87%	73%	80%	87%	93%	93%	93%	87%	87%	93%	80%	80%	87%	93%	73%	87%	80%	93%
	سطح معناداری	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.001	0	0
	آماره تی	8.5	6.959	6.325	11.309	5.916	8.367	5.123	5.123	8.876	8.264	5.87	5.87	10.693	10.693	8.29	4.026	8.264	6.971
	انحراف معیار	0.5164	0.59362	0.8165	0.59362	0.65465	0.61721	0.75593	0.75593	0.63994	0.59362	0.70373	0.70373	0.50709	0.50709	0.56061	0.83381	0.59362	0.70373
	میانگین	4.1333	4.0667	4.3333	4.7333	4	4.3333	4	4	4.4667	4.2667	4.0667	4.0667	4.4	4.4	4.2	3.8667	4.2667	4.2667
مرحله پیشگیرانه	cvi	87%	73%	73%	47%	60%	87%	87%	87%	87%	73%	73%	73%	47%	73%	60%	87%	60%	60%
	cvr	93%	87%	87%	73%	80%	93%	93%	93%	93%	87%	87%	87%	73%	87%	80%	93%	80%	80%
	سطح معناداری	0	0	0.001	0	0	0	0.001	0.002	0	0	0	0	0	0	0	0	0	0
	آماره تی	5.137	8.5	4.298	5.137	8.29	5.392	4.026	3.761	5.392	8.29	4.583	4.675	5.87	5.87	8.5	5.906	5.392	6
	انحراف معیار	0.70373	0.5164	0.96115	0556Y1.	0.56061	0.86189	0.83381	0.96115	0.86189	0.56061	0.74322	0.88372	0.70373	0.70373	0.5164	0.74322	0.86189	0.7746
	میانگین	3.9333	4.1333	4.0667	4.4	4.2	4.2	3.8667	3.9333	4.2	4.2	4.1333	4.0667	4.0667	4.0667	4.1333	4.1333	4.2	4.2
مرحله بازدارندگی	cvi	87%	87%	60%	73%	87%	87%	100%	100%	87%	87%	87%	73%	60%	100%	87%	73%	100%	73%
	cvr	93%	93%	80%	87%	93%	93%	100%	100%	93%	93%	93%	87%	80%	100%	93%	87%	100%	87%
	سطح معناداری	0	0	0	0.008	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	آماره تی	5.137	11.225	4.583	3.096	9.025	6	9.025	5.906	6	9.025	6.874	6.874	12.475	12.475	10.717	8.5	10.717	8.5
	انحراف معیار	0.70373	0.41404	0.84515	1.33452	0.45774	0.7746	0.45774	0.74322	0.7746	0.45774	0.67612	0.45774	0.35187	0.35187	0.45774	0.5164	0.45774	0.5164
	میانگین	3.9333	4.2	4	4.0667	4.0667	4.2	4.0667	4.1333	4.2	4.0667	4.2	4.0667	4.1333	4.1333	4.2667	4.1333	4.2667	4.1333
شاخص		b46	b47	b48	c11	c12	c13	c14	c15	c16	c17	c18	c21	c22	c23	c24	c25	c26	c27
مؤلفه					کاربردی								مدیریتی						
ابعاد					عوامل انسانی														

نتیجه		تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید
مرحله اصلاحی	cvi	60%	87%	87%	100%	87%	73%	73%	73%	73%	100%	87%	87%	87%	73%	73%	73%	87%	60%
	cvr	80%	93%	93%	100%	93%	87%	87%	87%	87%	100%	93%	93%	93%	87%	87%	87%	93%	80%
	سطح معناداری	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	آماره تی	7.359	7.135	5.906	8.876	8.876	8.876	8.876	7.135	5.906	5.916	8.264	8.876	8.876	8.876	6.971	5.906	6.971	6.859
	انحراف معیار	0.737	0.724	0.743	0.64	0.64	0.64	0.64	0.756	0.724	0.743	0.655	0.594	0.64	0.64	0.64	0.743	0.704	0.64
	میانگین	4.4	4.333	4.133	4.467	4.467	4.467	4.467	4	4.333	4.133	4	4.267	4.467	4.467	4.467	4.133	4.267	4.133
مرحله آشکارسازی	cvi	73%	73%	60%	87%	87%	87%	60%	87%	73%	87%	60%	87%	60%	87%	87%	87%	73%	73%
	cvr	87%	87%	80%	93%	93%	93%	80%	93%	87%	93%	80%	93%	80%	93%	93%	93%	87%	87%
	سطح معناداری	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	آماره تی	7.135	9.28	5.87	6.971	6.971	8.876	10.693	8.264	6.971	11.5	4.525	14.666	8.264	11	12.22	8.367	6	5.916
	انحراف معیار	0.72375	0.63994	0.70373	0.70373	0.63994	0.70373	0.50709	0.59362	0.70373	0.5164	0.79881	0.45774	0.59362	0.5164	0.50709	0.61721	0.7746	0.65465
	میانگین	4.3333	4.5333	4.0667	4.2667	4.2667	4.2667	4.4	4.2667	4.5333	4.3333	3.9333	4.7333	4.2667	4.6	4.3333	4.2	4.2	4
مرحله پیشگیرانه	cvi	87%	73%	73%	73%	60%	87%	87%	60%	87%	87%	60%	87%	87%	87%	87%	87%	87%	100%
	cvr	93%	87%	87%	87%	80%	93%	93%	80%	93%	93%	80%	93%	93%	93%	93%	93%	93%	100%
	سطح معناداری	0	0	0	0	0	0	0.001	0	0	0	0	0	0	0	0	0	0	0
	آماره تی	6.859	8.876	5.172	5.264	6.971	6.325	4.09	11.225	6.859	11	5.245	14.666	5.123	4.09	11.5	8.264	6	8.29
	انحراف معیار	0.63994	0.63994	0.79881	0.83381	0.70373	0.8165	0.88372	0.41404	0.63994	0.5164	0.63994	0.45774	0.75593	0.88372	0.5164	0.59362	0.7746	0.56061
	میانگین	4.1333	4.4667	4.0667	4.1333	4.2667	4.3333	3.9333	4.2	4.1333	4.4667	3.8667	4.7333	4	3.9333	4.5333	4.2667	4.2	4.2
مرحله بازدارندگی	cvi	87%	87%	87%	73%	73%	60%	60%	73%	73%	73%	87%	87%	87%	87%	87%	87%	87%	87%
	cvr	93%	93%	93%	87%	87%	80%	80%	87%	87%	87%	93%	93%	93%	93%	93%	93%	93%	93%
	سطح معناداری	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	آماره تی	12.475	10.693	10.717	10.583	8.5	8.367	12.475	11.225	10.583	8.5	6.959	12.22	7.246	9.025	11	10.717	10.717	8.5
	انحراف معیار	0.35187	0.50709	0.45774	0.48795	0.5164	0.61721	0.35187	0.41404	0.48795	0.5164	0.59362	0.50709	0.53452	0.45774	0.5164	0.45774	0.45774	0.5164
	میانگین	4.1333	4.4	4.2667	4.3333	4.1333	4.3333	4.1333	4.2	4.1333	4.3333	4.0667	4.6	4	4.0667	4.4667	4.2667	4.2667	4.1333
شاخص		d11	d12	d13	d14	d15	d16	d17	d18	d21	d22	d23	d24	d25	d26	d27	d28	d31	d32
مؤلفه		کنترل دسترسی								رمز نگاری								تجهیزات	
ابعاد		عوامل فنی																	

	نتیجه	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید	تأیید
مرحله اصلاحی	cvi	73%	87%	100%	100%	100%	100%	87%	87%	73%	73%	100%	87%	100%	100%	100%	87%	87%	87%
	cvr	87%	93%	100%	100%	100%	100%	93%	93%	87%	87%	100%	93%	100%	100%	100%	93%	93%	93%
	سطح معناداری	0	0.014	0.003	0	0	0	0	0	0	0	0	0	0	0	0.001	0	0	0
	آماره تی	4.525	2.806	3.556	5.906	5.123	5.123	6.874	11.225	8.264	7.246	5.87	5.123	5.906	6.205	4.183	5.137	5.137	6.874
	انحراف معیار	0.799	0.828	0.799	0.743	0.756	0.704	0.676	0.414	0.594	0.535	0.704	0.756	0.743	0.458	0.617	0.704	0.704	0.676
	میانگین	3.933	3.6	3.733	4.133	4	4.067	4.2	4.2	4.267	4	4.067	4	4.133	3.733	3.667	3.933	3.933	4.2
مرحله آشکارسازی	cvi	73%	73%	87%	100%	87%	87%	100%	100%	87%	73%	60%	87%	87%	100%	87%	73%	100%	73%
	cvr	87%	87%	93%	100%	93%	93%	100%	100%	93%	87%	80%	93%	93%	100%	93%	87%	100%	87%
	سطح معناداری	0	0.003	0	0	0	0.001	0	0	0	0	0	0	0	0	0.001	0	0	0
	آماره تی	5.172	3.556	5.123	4.525	5.123	4.036	5.906	5.137	11	8.5	8.29	7.246	5.123	5.123	4.036	5.906	5.137	11
	انحراف معیار	0.79881	0.79881	0.75593	0.79881	0.75593	0.70373	0.74322	0.70373	0.5164	0.5164	0.56061	0.53452	0.75593	0.75593	0.79881	0.75593	0.79881	0.79881
	میانگین	4.0667	3.7333	4	3.9333	4	3.7333	4.1333	3.9333	4.4667	4.1333	4.2	4	4	4	3.9333	3.7333	4.1333	3.9333
مرحله پیشگیرانه	cvi	73%	73%	73%	73%	87%	100%	100%	87%	73%	60%	87%	87%	100%	87%	73%	73%	73%	100%
	cvr	87%	87%	87%	87%	93%	100%	100%	93%	87%	80%	93%	93%	100%	93%	87%	87%	87%	100%
	سطح معناداری	0	0	0	0	0	0	0.001	0.001	0	0	0	0	0	0	0	0	0	0.001
	آماره تی	5.87	6.959	6.874	4.525	6.089	6.089	4	4.026	5.906	6.959	5.916	7.897	5.123	4.525	6.874	4.525	6.959	5.87
	انحراف معیار	0.70373	0.59362	0.67612	0.79881	0.79881	0.59362	0.7746	0.83381	0.74322	0.59362	0.65465	0.45774	0.75593	0.79881	0.67612	0.79881	0.59362	0.70373
	میانگین	4.0667	4.0667	4.2	3.9333	4	3.9333	3.8	3.8667	4.1333	4.0667	4	3.9333	4	3.9333	4.2	3.9333	4.0667	4.0667
مرحله بازدارندگی	cvi	87%	100%	87%	100%	100%	87%	73%	60%	87%	87%	100%	87%	100%	100%	100%	87%	100%	87%
	cvr	93%	100%	93%	100%	100%	93%	87%	80%	93%	93%	100%	93%	100%	100%	100%	93%	100%	93%
	سطح معناداری	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	آماره تی	8.29	8.5	7.246	8.29	8.5	9.539	7.897	5.123	10.717	9.025	12.475	14	12.475	8.5	8.29	7.246	8.5	8.29
	انحراف معیار	0.56061	0.5164	0.53452	0.56061	0.5164	0.35187	0.45774	0.75593	0.45774	0.45774	0.35187	0.2582	0.35187	0.5164	0.56061	0.53452	0.5164	0.56061
	میانگین	4.2	4.1333	4	4.2	4.1333	3.8667	3.9333	4	4.2667	4.0667	4.1333	3.9333	4.1333	4.1333	4.2	4	4.1333	4.2
	شاخص	d33	d34	d35	d36	d37	d38	d39	d41	d42	d43	d44	d45	d46	d47	d48	d51	d52	d53
	مؤلفه								برنامه‌ریزی								پایش		
	ابعاد																		

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

ابعاد	مؤلفه	شاخص	مرحله بازدارندگی					مرحله پیشگیرانه					مرحله آشکارسازی					مرحله اصلاحی					نتیجه
			میانگین	انحراف معیار	آماره تی	سطح معناداری	CVR	میانگین	انحراف معیار	آماره تی	سطح معناداری	CVR	میانگین	انحراف معیار	آماره تی	سطح معناداری	CVR	میانگین	انحراف معیار	آماره تی	سطح معناداری	CVR	
		e26	4.4667	0.5164	11	0	93%	4.2667	0.59362	8.264	0	100%	4	0.65465	5.916	0	100%	4.133	0.743	5.906	0	100%	تأیید
		e27	4.3333	0.48795	10.583	0	93%	4.0667	0.79881	5.172	0	93%	4	0.65465	5.916	0	100%	4	0.655	5.916	0	100%	تأیید
		e28	4.1333	0.5164	8.5	0	93%	4	0.75593	5.123	0	93%	4.2667	0.59362	8.264	0	93%	4.067	0.704	5.87	0	100%	تأیید

برای تعیین اتفاق‌نظر میان اعضای پانل، علاوه‌بر شاخص‌های مرکزی شامل میانگین و انحراف استاندارد و... آزمون تی تک‌نمونه‌ای، CVI و CVR، از ضریب هماهنگی کندال نیز استفاده شده است. مطابق جدول (۵)، ضریب همبستگی کندال که با نماد w نشان داده می‌شود، یک آزمون ناپارامتریک است و برای تعیین میزان هماهنگی میان نظرات استفاده می‌شود. ضریب کندال بین ۰ و ۱ متغیر است. مقدار صفر، عدم توافق کامل و ۱، توافق کامل را نشان می‌دهد. نتایج دلفی نشان می‌دهد که اتفاق‌نظر اعضای پانل حاصل شده است و می‌توان به تکرار دورها پایان داد. با توجه به کمتر بودن مقدار سطح معنی‌داری از ۰/۰۵، می‌توان گفت که ضریب توافقی کندال معنادار بوده و در سطح اطمینان ۹۵% اتفاق‌نظر بین خبرگان در هر سه مرحله وجود داشته است. افزایش مقدار ضریب کندال در هر مرحله نسبت به مرحله قبل نیز گواه این مطلب می‌باشد.

جدول ۵- جمع‌بندی نهایی دلفی

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

در نهایت، مطابق جدول (۶) مدل اندازه‌گیری (بارهای عاملی) و شاخص هم‌خطی بررسی گردید.

جدول ٦ - (بارهای عاملی) و شاخص هم‌خطی

بعد	مؤلفه	شاخص	تحلیل عاملی تاییدی مرتبه اول				هم خطی
			بارعاملی	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

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

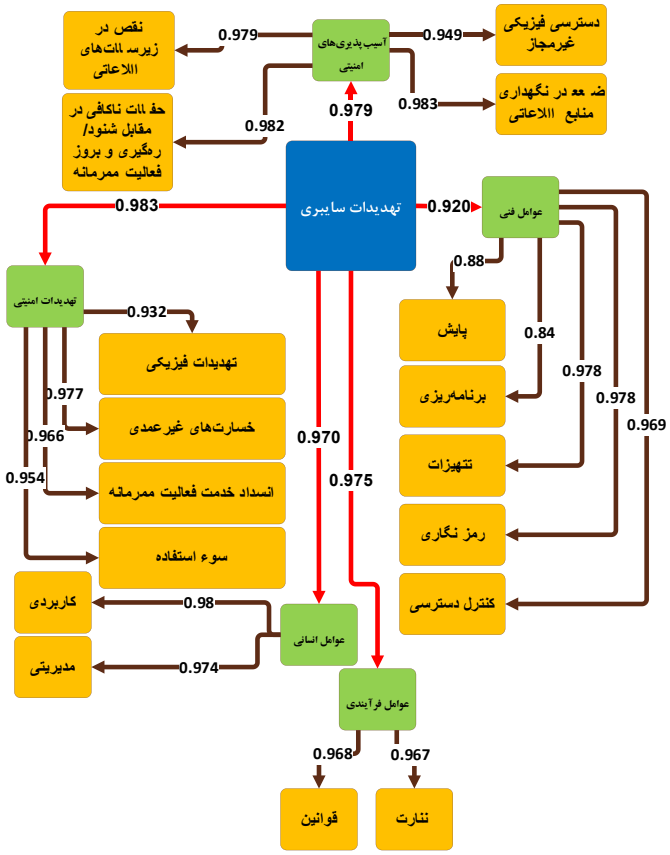
بعد	مؤلفه	شاخص	تحلیل عاملی تاییدی مرتبه اول				هم خطی
			بارعاملی	خطا	آماره تی	سطح معناداری	VIF
	نقص در زیرساخت‌های اطلاعاتی	b31	0.896	0.023	38.209	0.001	2.077
		b32	0.887	0.027	33.15	0.001	2.8455
		b33	0.908	0.021	43.041	0.001	3.3495
		b34	0.906	0.022	41.101	0.001	2.197
		b35	0.915	0.019	47.167	0.001	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

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

بعد	مؤلفه	شاخص	تحلیل عاملی تاییدی مرتبه اول				هم خطی
			بارعاملی	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. نتیجه‌گیری

برای هر مؤلفه، بار عاملی مرتبه دوم و سوم مطابق شکل (۳) محاسبه و ترسیم گردید. همان‌گونه که در پیشینه پژوهش حاضر به این موضوع اذعان شد که تصحیح الگوی رفتاری ارجح‌تر از راه‌حل‌های 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 مولفه‌های آن، بالاترین وزن را مؤلفه «خسارت‌های غیرعمدی» دارد و بیانگر آن است که منشأ بسیاری از حملات سایبری عامل انسانی است که عموماً به‌صورت ناخواسته، زمینه را جهت نفوذ فراهم می‌کند. بنابراین، تبیین یک الگوی رفتاری صحیح می‌تواند 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 (۱٤۰۰) مورد مقایسه قرار گرفته و همخوانی رتبه‌بندی‌های دو پژوهش حاکی از صحّت و اعتبار بالای نتایج می‌باشد.

جدول ۷ - مقایسه نتایج این پژوهش از نظر رتبه‌بندی مؤلفه‌ها با نتایج مطالعات شعبانی (۱٤۰۰)

شعبانی (۱٤۰۰)		پژوهش حاضر	
رتبه میانگین	مؤلفه	مؤلفه	وزن مؤلفه عاملی
۱۶,۲۶	فرهنگ سازمانی	تهدیدات امنیتی	۰,۹۸۳
۱۳	ساختار سازمانی	آسیب‌پذیری‌های امنیتی	۰,۹۷۹
۱۲,۱۱	منابع انسانی	عوامل فرایندی (ساختار سازمانی)	۰,۹۷۵
۱۱,۶۳	زیرساخت فناوری اطلاعات	عوامل انسانی	۰,۹۷۰
۱۰,۹۸	آموزش و بازآموزی	عوامل فنی	۰,۹۲۰
۹,۴۸	جنبه راهبردی و رهبری		

۷. پیشنهادات

پیرو 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 به‌منظور 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 خط‌مشیء 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، خط‌مشی‌ءها، 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 خط‌مشی‌ءهای 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 صحّت، محرمانگی و دسترس‌پذیری اطلاعات سازمان،

۱۱. تدوین اصول پایش و کنترل کاربران،

۱۲. تعیین راهبردها در صورت عدم پیروی از خط‌مشی‌ءهای 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 پویشگرها 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 قابل‌حمل 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 صحّت 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 دسترس‌پذیری و ظرفیت حافظه پشتیبان.

منـابـع

آهنگر، ع.، باب‌الحوائجی، 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.، فرج پهلو، ع.، خادمی‌زاده، ش.، نادران طحان، م. (۱۴۰۱). ارائه معماری پیشنهادی به‌کارگیری اینترنت اشیاء در کتابخانه‌های 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). امکان‌سنجی استقرار مدیریت دانش در سازمان دانش محور. *فناوری اطلاعات انتظامی*، ۴(۸): ۶۷-۸۴. https://doi.org/10.22034/pitc.2022.1266565.1114

شفیعی نیک‌آبادی، 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 چالش‌های امنیتی شبکه LTE، و موانع و فرصت‌های بومی‌سازی شبکه در بستر استاندارد. *پدافند 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 Pahlo, 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.