-- Special Issuance of Tax Research --
Conference on Tax and Financial Policies in Iran,
May 10, 2025, 71-98
taxjournal.ir
DOI:/10.61882/taxjournal.0.71

Iranian National Tax Administration

Presenting the Conceptual Model of Maturity of Cyber Security in the Cloud Space of the Taxpayers System of the Country's Tax Affairs Organization

Marzieh Davoodi*

Department of Information Technology Management, Ha.C, Islamic Azad University, Hamedan, Iran.

Mohammad Mehdi Shirmohammadi

Department of Computer, Ha.C, Islamic Azad University, Hamedan, Iran.

Abstract

The security of the digital space depicts a new facet of the national security of each country; therefore, it is necessary to parallel the rapid development of information technology applications by recognizing the country's key infrastructures that are vitally dependent on information, and by planning to protect these infrastructures, the development of the country in achieving the goal of becoming a knowledge-based society. The country's tax affairs organization, which deals with sensitive data and information, benefits from the cloud. Presenting the conceptual model of cyber security maturity in the cloud space of the taxpayer system of the country's tax affairs organization is the main goal of this research. In this research, based on high-quality documents in the cyber field and using mixed research methods (quantitative and qualitative), an integrated interpretation of the findings obtained from qualitative studies was conducted, to achieve a perceptual level and present a conceptual model. Experts were selected using the Delphi technique. The validity and reliability of the research have been confirmed by the professors. To identify the dimensions, components, and indicators, using the theoretical literature and studying the previous research, first, 139 studies were evaluated using the CASP tool, and finally, 19 studies were selected. Selected studies were coded using MAXQDA software, and finally, 51

* Corresponding Author: Mardav7959@gmail.com

How to Cite: Davoodi, M., & Shirmomammadi, M. M. (2025). Presenting the Conceptual Model of Maturity of Cyber Security in the Cloud Space of the Taxpayers System of the Country's Tax Affairs Organization. *Conference on Tax and Financial Policies in Iran, Special Issuance of Tax Research,* 71-98.

Original Research
Accepted: 01/09/2025
Received: 11/08/2025
p-ISSN: 2251-64-84
e-ISSN: 2717-1817

[DOI: 10.61882/taxjournal.0.71]

indicators were calculated. These indicators were shared with 16 experts through a questionnaire, and the final indicators were extracted for model design. The obtained model includes 3 dimensions, 11 components, and 51 indicators.

Introduction

In this research, the solutions and strategies of security risk management in the cloud space of the Taxpayers' system of the Tax Affairs Organization of the country are discussed. One of the challenges ahead is that some organizations may have concerns about online access and security in the Cloud. However, with the benefit of cloud space, the country's tax affairs organization can improve its performance and efficiency and fight related challenges. Meanwhile, the lack of preparation for crisis management and recovery after attacks or technical problems can also become a risk. To deal with these risks, the tax affairs organization needs to carefully implement security strategies and policies and use modern security technologies and solutions. Also, personnel training and continuous updating of security technology are of particular importance. It should be noted that in addition to the mentioned cases, performance management and optimal operations in the cloud space require special skills and capabilities, and it is necessary to transfer things to the cloud space that can reduce costs from another point of view, legal questions related to data protection, information Confidentiality, and the possibility of changes in policy settings may lead to security issues in the cloud. To deal with these risks, organizations need risk management strategies, implementation of security standards, increasing awareness of threats, and continuous updating of technology security (Tabatabai and KarimkhaniZandi, 2015).

In addition, it is essential that organizations choose the most reliable and high-security providers for cloud services. Because the use of cloud space in the tax affairs organizations of the countries, as an effective approach in data management and information systems, has been highly effective in increasing the efficiency and organizational facilities, this will entail significant risks.

Therefore, to reduce these risks, the tax organization needs to have continuous updates in the field of information security, use advanced security technologies, promote training and awareness processes, and also comply with national and international security standards.

For this purpose, this research seeks to provide a conceptual model of cyber security maturity for the cloud space of the taxpayer system of the Tax Administration of Iran by focusing on cyber security management standards, analyzing cyber security maturity models, and using the opinions of experts, specifying the components of the cyber security maturity model. In general, people related to this system and direct and indirect supervisors need to know things such as insufficient protection against unauthorized access to servers and physical facilities, which may be a risk, increasing the volume of information

[DOI: 10.61882/taxjournal.0.71]

and transactions, which requires a scalable and scalable tax system trust is, Failure to comply with security and technology standards that may lead to security vulnerabilities, lack of assurance of data trust that information in the cloud may be compromised and out of trust due to management mistakes or Cyber Attacks, and in this regard Have the necessary knowledge.

The need to make changes in tax laws and the legal system, on one hand, and the need to optimize tax technology on the other hand, may create challenges in the tax system. In this regard, non-compliance with security and technology standards may lead to security vulnerabilities, and the increase in the volume of information and transactions requires a scalable and reliable tax system.

Scalability and capability in managing system changes and updates are important so that the organization can quickly adapt to technological developments and new needs.

In order to implement and protect this system, we need to define different departments with various responsibilities and collect the necessary information in this field, along with daily, weekly, and annual monitoring, and prepare and compile the necessary reports.

The implementation of this monitoring will improve the functioning of the system, establish more security, and prevent intrusion, sabotage, and manipulation in this field. The obtained model can result in increasing the security of critical infrastructures in the cyber field, and the decision of national managers to implement the maturity model of cyber security at the national level, and in line with the review and assessment of the state of cyber security in the cloud space of the country's tax system.

In the following, it can be mentioned that conducting this research is important from the following aspects: due to the sensitivity of tax information, it will be vital to provide strong and effective solutions to strengthen the security of the cloud space in the tax affairs organization.

For example, regarding the violation of personal privacy and internal intrusion into the system, and before that, preserving the privacy of citizens' tax information is one of the main challenges, and any violation can lead to legal and credit problems, as well as unauthorized access or destructive activities by internal people. Organization personnel are one of the significant risks.

Also, regarding Cyber Attacks, cyber threats may target tax systems and manipulate confidential information. In general, migration to the cloud requires changes in the configuration of systems and software, which may lead to challenges.

Meanwhile, dealing with security threats in the cloud is very important because sensitive tax information may be at risk.

Finally, it can be said that carrying out this research led to things such as: identifying and analyzing security risks and threats related to the use of cloud space in the taxpayer system of the country's tax affairs organization and

[DOI: 10.61882/taxjournal.0.71]

providing a cyber security maturity model for this system, providing risk identification methods and the security threats in the cloud space, the risks in the Taxpayer system and their effects on the operation of this system will be identified.

Methods and Materials

The research method used in this study is mixed (quantitative and qualitative). To better understand the effective factors in securing and to examine the various dimensions of cyber security maturity models and their indicators, and to design a conceptual model of cyber security maturity for the taxpayer system of the country's tax affairs organization, a metasynthesis approach is used.

Compared to early qualitative studies, this approach is far more suitable for generating theory. This approach can be used to support the existing theories, interpret and explain them more precisely, and also to complete the theories (Abadi Jafari, 2018).

Quantitative methods are used to validate and test the model obtained by the metacombination method. In this research, the Delphi technique is used to evaluate and validate the model and confirm the relevant components and elements. The Delphi method is one of the data collection methods.

Keywords: Cloud Space, Cyber Security, Cyber Security Maturity Model, Security Risk Management, Taxpayers' System.

[DOI: 10.61882/taxjournal.0.71]

-- مجله علمی، ویژه‌نامه --
همایش سیاست‌های مالی و مالیاتی ایران،
اردیبهشت ۱۴۰۴، ۹۸-۷۱
taxjournal.ir
DOI:/10.61882/taxjournal.0.39

مقاله پژوهشی
تاریخ دریافت: ۱۴۰۴/۰۵/۲۰
تاریخ پذیرش: ۱۴۰۴/۰۶/۱۰
e-ISSN: ۲۷۱۷-۱۸۱۷ p-ISSN: ۲۲۵۱-۶۴-۸۴

ارائه مدل مفهومی بلوغ امنیت سایبری در فضای ابری سامانه مؤدیان سازمان امور مالیاتی کشور

مرضیه داودی* گروه مدیریت فناوری اطلاعات، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران.

محمدمهدی شیرمحمدی گروه کامپیوتر، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران.

چکیده

امنیت فضای دیجیتال وجه تازه‌ای از امنیت ملی هر کشور را به تصویر می‌کشد، لذا لازم است به موازات توسعه سریع کاربری‌های فناوری اطلاعات با شناخت زیرساخت‌های کلیدی کشور که وابستگی حیاتی به اطلاعات دارند و با برنامه‌ریزی جهت حفاظت از این زیرساخت‌ها، سیر توسعه کشور در دستیابی به جامعه دانایی‌محور هموار گردد. سازمان امور مالیاتی کشور که با داده‌ها و اطلاعات حساس سروکار دارد، از فضای ابری بهره‌مند می‌شود. ارائه مدل مفهومی بلوغ امنیت سایبری در فضای ابری سامانه مؤدیان سازمان امور مالیاتی کشور، هدف اصلی این پژوهش به شمار می‌آید. در این پژوهش، با استناد به اسناد بالادستی در حوزه سایبری و با استفاده از روش تحقیق آمیخته (کمّی و کیفی)، جهت تفسیر یکپارچه یافته‌های بدست آمده از مطالعات کیفی و با هدف دستیابی به سطح ادراکی، مدلی مفهومی ارائه شده است. خبرگان تحقیق، با استفاده از تکنیک دلفی انتخاب شدند. روایی و اعتبار پژوهش نیز توسط اساتید تأیید شده است. برای شناسایی ابعاد، مؤلفه‌ها و شاخص‌ها، با استفاده از ادبیات نظری و مطالعه تحقیق‌های پیشین، ابتدا ۱۳۹ پژوهش با ابزار CASP ارزیابی، و در نهایت ۱۹ پژوهش انتخاب شدند. پژوهش‌های منتخب با استفاده از نرم‌افزار MAXQDA کدگذاری و در نهایت، ۵۱ شاخص احصاء گردید. این شاخص‌ها از طریق پرسشنامه با ۱۶ نفر از خبرگان به اشتراک گذاشته شد و شاخص‌های نهایی برای طراحی مدل استخراج گردید. مدل بدست آمده شامل ۳ بعد، ۱۱ مؤلفه و ۵۱ شاخص است.

کلید واژه‌ها: امنیت سایبری، سامانه مؤدیان، فضای ابری، مدل بلوغ امنیت سایبری، مدیریت ریسک‌های امنیتی.

*نویسنده مسئول: Mardav7959@gmail.com

[DOI: 10.61882/taxjournal.0.71]

مقدمه

این پژوهش به راهکارها و استراتژی‌های مدیریت ریسک امنیتی در فضای ابری سامانه مؤدیان سازمان امور مالیاتی کشور می‌پردازد. یکی از چالش‌های پیش رو، این است که برخی از سازمان‌ها ممکن است نگرانی‌هایی مربوط بدسترسی آنلاین و اطمینان در فضای ابری داشته باشند.

با این همه، سازمان امور مالیاتی کشور با بهره‌مندی از فضای ابری، می‌تواند عملکرد و کارایی خود را بهبود داده و با چالش‌های مرتبط بجنگد. این در حالی است که عدم آمادگی برای مدیریت بحران و بازیابی پس از حملات یا مشکلات فنی نیز می‌تواند به ریسک تبدیل شود.

برای مقابله با این ریسک‌ها، سازمان امور مالیاتی نیاز دارد تا به دقت، استراتژی‌ها و سیاست‌های امنیتی را اجرا کرده و از تکنولوژی‌ها و راهکارهای امنیتی مدرن بهره ببرد. آموزش پرسنل و به‌روزرسانی مداوم فناوری امنیتی نیز از اهمیت ویژه‌ای برخوردار است. لازم به ذکر است علاوه بر موارد گفته شده، مدیریت عملکرد و عملیات بهینه در فضای ابری، نیازمند مهارت‌ها و توانمندی‌های خاصی است؛ مانند انتقال به فضای ابری. اگر این امر می‌تواند باعث کاهش هزینه‌ها شود و از نگاهی دیگر، سبب ایجاد سوألات قانونی مرتبط با حفاظت از داده‌ها و اطلاعات محرمانه گردد و نیز احتمال تغییرات در تنظیم قوانین، ممکن است به مشکلات امنیتی در فضای ابری منجر شود. برای مقابله با این ریسک‌ها، سازمان‌ها نیاز به استراتژی‌های مدیریت ریسک، اجرای استانداردهای امنیتی، افزایش آگاهی از تهدیدات و به‌روزرسانی مداوم امنیت فناوری دارند (طباطبائی و کریمخانی زندی، ۱۳۹۵).

همچنین ضروری است که سازمان‌ها در اخذ خدمات ابری، از میان اعتمادپذیرترین ارائه‌دهندگان که امنیت بالا دارند، انتخاب کنند. به دلیل اینکه استفاده از فضای ابری در سازمان‌های امور مالیاتی کشورها، به عنوان رویکردی مؤثر در مدیریت داده و سیستم‌های اطلاعاتی، به شدت در افزایش کارایی و امکانات سازمانی تأثیرگذار بوده است و این مهم ریسک‌هایی در پی خواهد داشت. لذا برای کاهش این ریسک‌ها، سازمان مالیاتی نیاز دارد که در زمینه امنیت اطلاعات، به روزرسانی‌های مداوم داشته باشد، از تکنولوژی‌های امنیتی پیشرفته استفاده کند، فرایندهای آموزش و آگاهی‌دهی را ترویج کند و همچنین استانداردهای امنیتی ملی و بین‌المللی را رعایت کند.

[DOI: 10.61882/taxjournal.0.71]

بدین منظور این پژوهش، به دنبال ارائه مدل مفهومی بلوغ امنیت سایبری، برای فضای ابری سامانه مؤدیان سازمان امور مالیاتی کشور و با تمرکز بر استانداردهای مدیریت امنیت سایبری، واکاوی مدل‌های بلوغ امنیت سایبری، و بهره‌گیری از نظرات خبرگان، با مشخص ساختن مؤلفه‌های مدل بلوغ امنیت سایبری است.

اصلی‌ترین تفاوت امنیت سایبری و امنیت اطلاعات این است که در امنیت طلاعات، حفاظت از اطلاعات حساس، هدف اصلی است، اما در امنیت سایبری، هدف اصلی، محافظت از فناوری مورد استفاده در سازمان است. این دو حوزه در سازمان‌ها به صورت متفاوتی مدیریت می‌شوند اگرچه این امکان وجود دارد که از ملاحظات ایمنی یکسان استفاده کنند.

در حالت کلی، افراد مرتبط به این سامانه و ناظران مستقیم و غیر مستقیم لازم است بدانند که مواردی چون عدم حفاظت کافی در مقابل دسترسی‌های غیرمجاز به سرورها و امکانات فیزیکی که ممکن است یک ریسک باشد، افزایش حجم اطلاعات و تراکنش‌ها نیازمند یک سیستم مالیاتی مقیاس‌پذیر و قابل اعتماد است، عدم پیروی از استانداردهای امنیتی و فناوری که ممکن است به آسیب‌پذیری‌های امنیتی منجر شود، عدم اطمینان از امانت داده‌ها که ممکن است اطلاعات در فضای ابری به دلیل اشتباهات مدیریتی یا حملات سایبری در معرض خطر قرار گیرند و از امانت خارج شوند، و در این خصوص آگاهی لازم را داشته باشند.لزوم انجام تغییرات در قوانین مالیاتی و نظام حقوقی از یک سو و نیاز به بهینه‌سازی فناوری مالیاتی از سوی دیگر ممکن است در سامانه مالیاتی چالش‌هایی ایجاد کند. در همین راستا، عدم پیروی از استانداردهای امنیتی و فناوری ممکن است به آسیب‌پذیری‌های امنیتی منجر شود و افزایش حجم اطلاعات و تراکنش‌ها نیازمند به یک سیستم مالیاتی مقیاس‌پذیر و قابل اعتماد است. مقیاس‌پذیری و توانمندی در مدیریت تغییرات و به‌روزرسانی‌های سامانه مهم است تا سازمان بتواند با تحولات فناوری و نیازهای جدید سریعاً سازگار شود .

جهت پیاده‌سازی و اجرای این سامانه و حفاظت از آن لازم است که بخش‌های مختلف با شرح مسئولیت‌های متفاوت تعریف شود و ضمن پایش روزانه، هفتگی و سالانه، اطلاعات لازم را در این زمینه، جمع‌آوری و گزارشات لازم تهیه و تدوین گردد. اجرای این پایش موجب هر چه بهتر شدن کارکرد سامانه و برقراری هر چه بیشتر امنیت، و جلوگیری از نفوذ و هرگونه خرابکاری و دستکاری در این زمینه خواهد شد. مدل بدست آمده می‌تواند منتج به افزایش ایمن‌سازی

[DOI: 10.61882/taxjournal.0.71]

زیرساخت‌های حیاتی در حوزه سایبری و تصمیم‌گیری مدیران کشوری برای پیاده‌سازی مدل بلوغ امنیت سایبری در سطح ملی و در راستای بازنگری و ارزیابی وضعیت امنیت سایبری در فضای ابری سامانه مؤدیان کشور گردد.

در ادامه، می‌توان اشاره کرد که انجام این پژوهش از جنبه‌های ذیل دارای اهمیت است: با توجه به حساسیت اطلاعات مالیاتی، ارائه راهکارهای قوی و مؤثر برای تقویت امنیت فضای ابری در سازمان امور مالیاتی، امری حیاتی و ضروری خواهد بود. به طور مثال، در خصوص نقض حریم شخصی و نفوذ داخلی در سامانه، و پیش از آن، حفظ حریم شخصی اطلاعات مالیاتی شهروندان، یکی از چالش‌های اصلی است و هر نقضی می‌تواند منجر به مشکلات قانونی و اعتباری شود. دسترسی غیرمجاز یا فعالیت‌های تخریبی از سوی افراد داخلی (پرسنل سازمان)، یکی دیگر از ریسک‌های مهم و قابل توجه است. همچنین تهدیدات سایبری ممکن است سامانه‌های مالیاتی را هدف قرار دهند و اطلاعات محرمانه را دستکاری کنند. به طور کلی می‌توان گفت، مهاجرت به فضای ابری نیاز به تغییرات در پیکربندی سیستم‌ها و نرم‌افزارها دارد که ممکن است چالش‌هایی را به دنبال داشته باشد. در این میان، مقابله با تهدیدات امنیتی در فضای ابری از اهمیت بالایی برخوردار است، زیرا اطلاعات حساس مالیاتی ممکن است در معرض خطر قرار بگیرند.

در نهایت می‌توان گفت انجام این تحقیق منجر به مواردی از جمله: شناسایی و تحلیل ریسک‌ها و تهدیدات امنیتی مرتبط با استفاده از فضای ابری در سامانه مؤدیان سازمان امور مالیاتی کشور و ارائه مدل بلوغ امنیت سایبری برای این سامانه، ارائه روش‌های شناسایی ریسک‌ها و تهدیدات امنیتی در فضای ابری، شناسایی ریسک‌ها در سامانه مؤدیان و اثرات آن‌ها بر کارکرد این سامانه، خواهد شد.

پیشینه پژوهش

بررسی تحقیقات پیشین نشان می‌دهد کـه مدل بلوغ امنیت اطلاعات و مدل بلوغ امنیت سایبری از برخی جوانب مورد بررسی قرار گرفته است ولی تحقیقات صورت گرفته در راستای احصای شاخص‌های ایمن‌سازی و ارائه مدل بلوغ امنیت سایبری زیرساخت‌های حیاتی کشور نبوده که پژوهش حاضر با ارائه مدل بلوغ امنیت سایبری برای زیرساخت‌های‌حیاتی کشور نسبت به احصای این شاخص‌ها اقدام کرده اسـت.

[DOI: 10.61882/taxjournal.0.71]

طباطبائی و همکاران (۱۳۹۵)، با بررسی تأثیر پدیده نوین رایانش ابری در مراکز دانش بنیانی نظیر کتابخانه‌ها و بیان فوایدش، و کاربردها و چگونگی عملکرد آن در کتابخانه‌های دیجیتال، به اختصار چالش‌های پیش روی به‌کارگیری این فناوری در کتابخانه‌ها را مورد مداقه قرار دادند. در این پژوهش، با برجسته کردن چالش مربوط به امنیت اطلاعات و حفظ حریم خصوصی کاربران، تهدیداتی را که در محیط ابری برای محرمانگی به وجود می‌آید، در هفت گروه طبقه‌بندی نمودند. در انتها، برای کاهش اثرات چالش‌های موجود در هر طبقه، راهکارها و استراتژی‌های تدافعی را تشریح کردند. طبق این بررسی، چالش‌های رایانش ابری را می‌توان در گروه‌های مختلف مانند: امنیت و حفاظت، مدیریت هویت، جداسازی داده‌ها، مدیریت منابع، مدیریت انرژی و برق، در دسترس بودن منابع و عدم تجانس منابع، دسته‌بندی کرد و مورد بحث قرار داد. در این پژوهش، تأکید روی چالش رایانش ابری، پیرامون مسائل امنیتی و حفظ حریم خصوصی است، لذا از پرداختن به سایر چالش‌ها صرف‌نظر شده است.

بیگیت اوزکان و اسپرویت (۲۰۱۸) با استفاده از پرسشنامه و بررسی انواع مدل‌های بلوغ امنیت سایبری، مدلی برای ارزیابی و بهبود امنیت سایبری برای ارائه‌دهندگان خدمات و مدیران زیرساخت‌های‌حیاتی ارائه کردند.

کاراباک و همکاران (۲۰۱۶) یک مدل بلوغ امنیت سایبری مبتنی برآسیب‌پذیری برای اندازه‌گیری زیرساخت‌های حیاتی در کشور ترکیه را با استفاده از نظرات خبرگان ارائه کرده‌اند.

ریا-گوامن و همکاران (۲۰۱۷)، مطالعه‌ای تطبیقی درباره مدل‌های بلوغ قابلیت امنیت سایبری انجام دادند و پرکاربردترین مدل‌های بلوغ قابلیت امنیت سایبری را در نتیجه یک بررسی سیستماتیک (SR) از مطالعات منتشرشده در بازه زمانی از ۲۰۱۲ تا ۲۰۱۷ توصیف و مقایسه کردند.

اخوان و رادفر (۱۳۹۹) مدل های بلوغ امنیت اطلاعات مورد بررسی قرار داد و با توجه به نظر خبرگان و یافته‌های پژوهش مدلی متشکل از ۵ مرحله برای پایش امنیت اطلاعات ارائه کرده‌اند. این پژوهش در یکی از شرکت‌های زیرمجموعه صنعت نفت انجام شده است و پایه آن بر اساس الزامات استانداردISO ۲۷۰۰۱ است.

میریوسفی و غفاری (۱۴۰۰)، به بررسی راهبردهای نوین حفاظت از زیرساخت های حیاتی پرداخته است. در این پژوهش، برخی شیوه‌ها و راهبردهای ملی برای حفاظت از زیرساخت‌های حیاتی بیان شده و چالش‌ها و الزامات پیش رو حفاظت از زیرساخت ها تبیین شده است.

ایده (۲۰۱۹) در پژوهشی که در قالب یک رساله دکتری انجام شده است، مدل بلوغ قابلیت

[DOI: 10.61882/taxjournal.0.71]

امنیت سایبری را برای سازمان‌های مالی نیجریه بررسی کرده است. این مدل، به عنوان مدلی توسعه‌ای و امنیتی برای تعیین سطح قدرت امنیت سایبری برگزیده شده و پنج سطح بلوغ را ارائه کرده است.

آقایی و همکاران (۲۰۱۹)، به مدلی مفهومی منطقی برای طبقه‌بندی تهدیدات سایبری پرداخته‌اند. این پژوهش، ادبیات موضوعی را بررسی کرده و به شناسایی تهدیدات سایبری پر تکرار، اعتبارسنجی آن‌ها از منابع معتبر و استخراج مفاهیم معتبر مربوط به شناسایی تهدیدات سایبری پرداخته است. همچنین ابعاد، مؤلفه‌ها و شاخص‌های طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی کشور نیز استخراج شده است.

بیگیت اوزکان و همکاران (۲۰۲۱) با اتکا به نظر خبرگان تهیه پرسشنامه، یک مدل بلوغ منطقه کانونی امنیت سایبری برای ارزیابی قابلیت‌های امنیت سایبری پیشنهاد شده است، همچنین در این تحقیق یک مؤسسه مالی مورد ارزیابی قرار گرفته است.

بریجت (۲۰۲۱) در پژوهشی در قالب رساله دکتری، با بررسی ادبیات موضوعی و مدل‌های مرجع نسبت به تبیین شاخص‌ها و مؤلفه‌های ارزیابی سازمان‌های بهداشتی ایالات متحده پرداخته و در نهایت با معرفی یک مدل قابل تعمیم و سیستم اندازه‌گیری عملکرد امنیت اطلاعات در سازمان‌های بهداشتی درمانی، کار خود را خاتمه داده است.

افشار و همکاران (۱۳۹۷)، دفاع در عمق را یکی از مهم‌ترین و پرکاربردترین راهبرد در ایمن‌سازی سیستم‌های کنترل صنعتی برشمرده‌اند.

سعادتمند و همکاران (۱۴۰۰) به روش مطالعه تطبیقی نسبت به تعیین شاخص‌های ارزیابی امنیت سایبری پرداخته شده‌اند. در این پژوهش با استناد به منابع کتابخانه‌ای و بررسی گزارش‌های ارائه شده از سوی مراجع معتبر در حوزه امنیت سایبری، هفت الگوی ارزیابی معتبر انتخاب و با رویکرد تطبیقی نسبت به بررسی ابعاد، اهداف و رویکرد آن‌ها اقدام شده است.

روش‌شناسی پژوهش

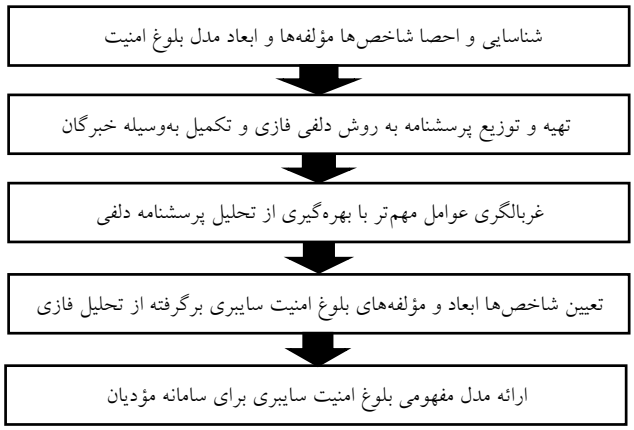
روش تحقیق مورد استفاده در این پژوهش، روش آمیخته (کمّی و کیفی) است. برای درک بهتر عوامل مؤثر در ایمن‌سازی و بررسی ابعاد مختلف مدل‌های بلوغ امنیت سایبری و شاخص‌های آن و طراحی یک مدل مفهومی بلوغ امنیت سایبری برای سامانه مؤدیان سازمان امور مالیاتی کشور از رویکرد فراترکیب (متاسنتز) استفاده می‌شود.

[DOI: 10.61882/taxjournal.0.71]

این رویکرد در مقایسه با مطالعات کیفی اولیه، به مراتب برای تولید نظریه مناسب‌تر است. این رویکرد می‌تواند در حمایت از نظریه‌های موجود، تفسیر و تشریح دقیق‌تر آن‌ها و نیز در تکمیل نظریه‌ها به‌کار گرفته شود (عابدی جعفری، ۱۳۹۸).

برای اعتبارسنجی و آزمون مدل بدست آمده به روش فراترکیب، از روش‌های کمّی استفاده می‌شود که در این پژوهش از تکنیک دلفی برای ارزیابی و اعتبارسنجی مدل و تأیید مؤلفه‌ها و عناصر مربوطه استفاده می‌شود. روش دلفی یکی از متدهای جمع‌آوری اطلاعات است.

نمودار ۱. فرایند انجام پژوهش



منبع: یافته‌های پژوهش.

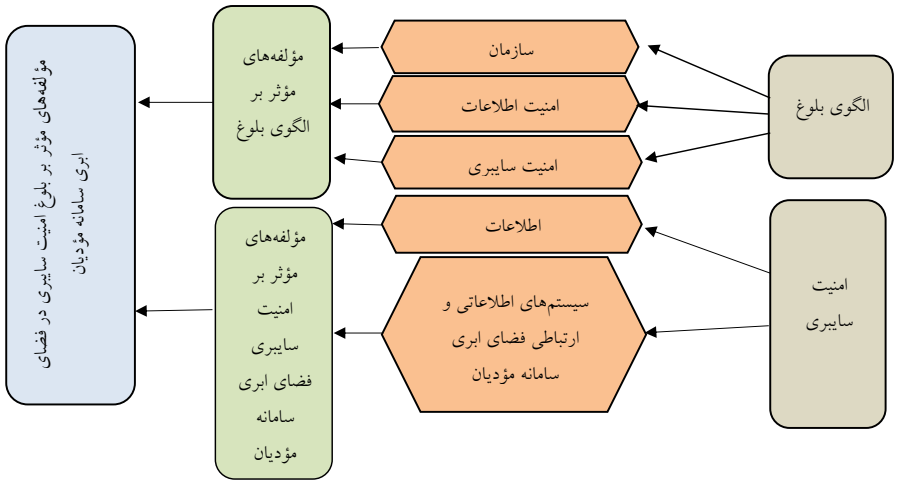
فرایند انجام پژوهش با رویکرد فراترکیب یک فرایند است که شامل مراحل گسسته‌ای است که پژوهشگر را قادر می‌سازد تا یک پرسش تحقیق مشخص را شناسایی کرده و سپس به جستجو، انتخاب، ارزیابی، خلاصه کردن و ترکیب شواهد برای پاسخگویی به سوأل تحقیق بپردازد. این فرایند با استفاده از روش‌های کیفی دقیق برای ترکیب مطالعات کیفی موجود برای ایجاد معنای بیشتر از طریق یک فرایند تفسیری انجام می‌شود (Erwin, 2011).

[DOI: 10.61882/taxjournal.0.71]

یافته‌ها

این پژوهش در پی ارائه مدل مفهومی بلوغ امنیت سایبری برای فضای ابری سامانه مؤدیان سازمان امور مالیاتی کشور می‌باشد. به همین منظور بر اساس نقشه راه (نمودار ۲)، ابتدا در دوشاخه به طور موازی به مرور ادبیات تحقیقات پیشین پرداخته و نهایتاً تقسیم‌بندی ذیل حاصل گردید.

نمودار۲. نقشه راه پژوهش



منبع: یافته‌های پژوهش.

الگوی بلوغ امنیت سایبری

در یک شاخه موضوع الگوی بلوغ در سه حوزه: الف) سازمان، ب) امنیت اطلاعات، ج) امنیت سایبری، قرارگرفته و نهایتاً مؤلفه‌های مؤثر بر بلوغ، شناسایی و استخراج می‌گردند. در شاخه دیگر موضوع امنیت سایبری در فضای ابری سامانه مؤدیان برای زیرساخت‌های حساس و حیاتی مربوطه در دو حوزه الف) اطلاعات، ب) سیستم‌های اطلاعاتی و ارتباطی و زیرساخت‌های حساس و حیاتی، قرارگرفته و نهایتاً مؤلفه‌های مؤثر بر امنیت سایبری سامانه مؤدیان استخراج می‌شوند. در پایان با تجمیع فاکتورهای استخراج شده از دوشاخه یاد شده بالا می‌توان مؤلفه‌های مؤثر بر بلوغ امنیت سایبری سامانه مؤدیان را احصاء و در گام آخر نسبت به ارائه مدل مفهومی

[DOI: 10.61882/taxjournal.0.71]

بلوغ امنیت سایبری این سامانه اقدام نمود. در پژوهش پیشرو، در گام نخست تمام پژوهش‌های منتخب را با استفاده از نرم‌افزار MAXQDA۲۰۲۲ تحلیل و نسبت به شناسایی کدها اقدام شده است. سپس با در نظر گرفتن مفهوم هر یک از کدها، آن‌ها را در یک مفهوم متشابه، دسته‌بندی شده است. هدف از این مرحله ارائه تفسیری جدید و یکپارچه از یافته‌هایی است که در طول بررسی و تحلیل از میان مطالعه‌های موجود بدست آمده است.

پایش کیفیت (پایایی و اعتبار)

آن چنان که در گام‌های قبل نیز مطرح شد، کوشش شده است که همه مقالات منتخب ازمجلات و پایگاه‌های معتبر انتخاب شوند، بنابراین مقالاتی که از درجه اعتبارکافی برخوردار نبودند، از فرایند پژوهش حذف شدند، همچنین از ابزارCASP برای بررسی روایی بخش کیفی پژوهش استفاده گردید که کمترین امتیاز مورد نیاز برای هر مقاله ۳۹ در نظرگرفته شد. برای این منظور تمام پژوهش‌های منتخب به کمک ۱۹معیارCASP ارزشیابی و مشاهده شد که ۱۹ کار پژوهشی ارزش بالاتر از ۳۱ داشتند. همچنین شیوه کدگذاری و طبقه‌بندی اطلاعات نیز چند بار مورد بررسی قرارگرفت. تمام این اقدامات برای تضمین کیفیت دستاوردهای پژوهش انجام شده است. در نهایت ۱۹ مقاله انتخاب شد که کمترین میانگین امتیاز داده شده به مقالات ۳۱ و بیشترین آن ۵۹ بوده است که ۱۴ مقاله در دسته امتیازی عالی (۴۹-۵۹) و ۸ مقاله در دسته خیلی خوب (۳۱-۴۹) هستند، در این خصوص می‌توان اظهارکرد مقالات منتخب برای تجزیه و تحلیل اطلاعات در این پژوهش در سطح قابل قبولی قرار دارند و در نتیجه، روایی پژوهش است.

[DOI: 10.61882/taxjournal.0.71]

جدول ۱. نتایج امتیازدهی منابع پس از ارزیابی کیفیت مطالعات اولیه تحقیق کیفی به استفاده از ابزارCASP

محدوده	تعداد مقالات
ضعیف(۱۰-۰)	۱۶
متوسط(۲۱-۱۱)	۷۰
خوب(۳۰-۲۱)	۳۱
خیلی خوب(۴۰-۳۱)	۸
عالی(۵۰-۴۰)	۱۴
جمع	۱۳۹

منبع: یافته‌های پژوهش.

به علاوه برای حفظ کیفیت یافته‌ها از شاخص کاپا استفاده شده است. از آنجا که در مراحل استخراج کدها، مفاهیم مطالعات گذشته به عنوان کد در نظرگرفته شدند و با در نظرگرفتن شباهت‌های مفهومی، شاخص‌های جدید شناسایی شدند، جهت کنترل شاخص‌های استخراج شده، از مقایسه نظر پژوهشگر با یک خبره استفاده شده است.

دامنه شاخص کاپا بین صفرتا یک است که هر چه این مقدار به عدد یک، نزدیک‌تر باشد، نشان‌دهنده توافق بیشتر بین رتبه‌دهندگان است. مقدار شاخص کاپا با استفاده از نرم‌افزارSPSS در سطح معناداری ۹۹۹. ۹، عدد۱۴۰ .۹ محاسبه گردید که در جدول (۱) نشان داده شده است. با توجه به کوچک‌تر بودن عدد معناداری از ۹۵ .۹ فرض استقلال شاخص‌های استخراج شده رد می‌شود و استخراج کدها از پایایی مناسبی برخوردار است.

جدول ۲. مقادیر اندازه توافق

	مقدار	انحراف استاندارد	عدد معناداری
ضعیف(۰ تا ۱۰)	۰.۷۴۶	۰.۰۶۲	۰.۰۰۰
تعداد موارد معتبر	۳۷		

منبع: یافته‌های پژوهش.

استخراج دستاوردهای مقالات و ارائه یافته‌ها، در این مرحله از فراترکیب یافته‌های حاصل از مراحل قبل ارائه می‌شود که پس از بازبینی و حذف شاخص‌های تکراری مجموعاً ۵۱

[DOI: 10.61882/taxjournal.0.71]

شاخص احصاء گردید و در قالب ۱۳ مؤلفه و ۳ بعد دسته‌بندی شدند. جدول(۳)، قسمتی از این دسته‌بندی را نشان می‌دهد.

جدول ۳. برخی از ابعاد مؤلفه‌ها و شاخص‌های احصاء شده

ردیف	ابعاد	مؤلفه	کد شاخص	شاخص منطبق با کدها	فراوانی در ۱۹ پژوهش
۱	فردی	مدیریت رخداد	C1	آگاهی از وضعیت	۴
۲			C2	عملیات امنیت	۳
۳			C3	کنترل حملات	۶
۴		ریسک	C5	منابع سازمانی	۳
۵			C6	مقررات و الزامات	۱
۶	سازمانی	تحلیل پاسخ به حوادث	C11	مدیریت رخداد	۴
۷		سواد امنیت سایبری	C31	فرهنگ‌سازی امنیت	۵
۸	فنی	معماری فرایند	C21	فناوری محافظتی	۵
۹		مدیریت تهدید	C23	مدیریت و کنترل تهدید	۵

منبع: یافته‌های پژوهش.

روش اجرای بخش کمّی

این گام «کمّی پژوهش»، شامل دو مرحله است. ابتدا، برای اعتبارسنجی شاخص‌های بدست آمده از گام قبلی تحقیق (فاز کیفی) از «تکنیک دلفی فازی» استفاده شد. ابزار جمع‌آوری داده‌ها و اطلاعات در بخش کمّی پژوهش، به منظور دستیابی به اهداف پژوهش، پرسشنامه‌هایی در دو بخش طراحی گردید. نخست، سن، تحصیلات، جنسیت، وضعیت استخدام برای سنجش عوامل جمعیت‌شناختی (دموگرافیک) در نظر قرار گرفت. در بخش‌های دیگر پرسشنامه‌ها، سوألاتی برای تأیید عناصر ابعاد مختلف و مؤلفه‌ها تهیه و تنظیم گردید.

[DOI: 10.61882/taxjournal.0.71]

روش توزیع و جمع‌آوری اطلاعات در بخش کمّی پژوهش

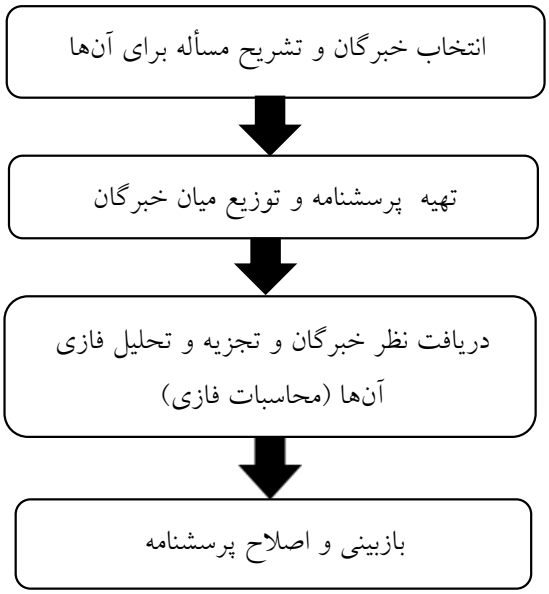
مرحله نخست- اعتبارسنجی مؤلفه‌هاو شاخص‌ها با تکنیک دلفی فازی:

پرسشنامه، از طریق ابزارپرس لاین، تهیه و تدوین گردید و لینک آن از طریق پیام‌رسان‌های مختلف به پاسخ‌دهندگان ارسال گردید. پس از جمع‌آوری پرسشنامه‌ها، برای اطمینان از کیفیت داده‌ها، پرسشنامه‌ها فیلتر شدند. برخی از پرسشنامه‌ها به علت وجود ایراد بی‌اعتباری حذف و مجدداً به پاسخ‌دهنده ارجاع داده شد و در نهایت پرسشنامه‌های معتبر مشخص گردید.

مرحله دوم- ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور:

بر اساس سوألات پژوهش و مطالعه ادبیات موضوع، مؤلفه‌ها و شاخص‌های مدل تدوین و پس از تأیید خبرگان مدل مربوطه ارائه گردید.

نمودار ۳. مراحل اجرای تکنیک دلفی فازی



منبع: یافته‌های پژوهش.

اعتبارسنجی شاخص‌های بلوغ امنیت سایبری و امنیت اطلاعات برای طراحی مدل بلوغ امنیت سایبری فضای ابری سامانه مؤدیان، نمونه‌ای از نتایج حاصل از بررسی پاسخ‌های پرسشنامه اول در جدول (۴) آمده است.

[DOI: 10.61882/taxjournal.0.71]

جدول ۴. نمونه‌ای از نتایج حاصل از شمارش پاسخ‌های پرسشنامه نخست

ردیف	شاخص‌های بلوغ امنیت سایبری و امنیت اطلاعات	درجه اهمیت				
		خیلی کم	کم	متوسط	زیاد	خیلی زیاد
۱	آگاهی از وضعیت	۰	۰	۳	۵	۱۱
۲	عملیات امنیت	۰	۰	۱	۱۰	۶
۳	کنترل حملات	۰	۰	۶	۴	۹

منبع: یافته‌های پژوهش.

ارزیابی اهمیت شاخص‌ها

بر اساس نتایج جدول (۴)، میانگین میزان اهمیت بند پیشنهادی، در خصوص هر یک از موارد پیشنهادی با توجه به میانگین میزان اهمیت برای این شاخص به صورت زیر بدست می‌آید.

$$\begin{aligned} A^{(i)} &= \frac{1}{16}(0 \times [0,0,2,4] + 0 \times [6,7,9,10] + 4 \times [9,10,12,13] \\ &\quad + 10 \times [12,14,16,16]) \\ &= \frac{1}{16}([0,0,0,0] + [0,0,0,0] + [12,14,18,20] \\ &\quad + [34,60,48,52] + [120,140,160,160]) \\ &= \frac{1}{16}[128,194,226,232] = [10,50,12,13,14,13,14,50] \end{aligned} \quad (۱)$$

اختلاف نظر هر یک از خبرگان از میانگین مطابق رابطه زیر محاسبه گردید:

$$\begin{aligned} &(a_{m1} - a_1{}^{(i)}, a_{m1} - a_2{}^{(i)}, a_{m3} - a_3{}^{(i)}, a_{m1} - a_4{}^{(i)}) \\ &= (\frac{1}{n} \sum a_1{}^{(i)}, \frac{1}{n} \sum a_2{}^{(i)}, \frac{1}{n} \sum a_3{}^{(i)}, \frac{1}{n} \sum a_4{}^{(i)}) \end{aligned} \quad (۲)$$

پرسشنامه دوم بر اساس نتایج حاصل از رابطه فوق تنظیم شده است که در آن اختلاف محاسبه شده مربوط به هر فرد خبره ثبت شده است. همچنین پیشنهادات خبرگان در خصوص اضافه شدن شاخص‌های جدید در دور اول دریافت و پس از بررسی و در صورت مناسب بودن، توسط پژوهشگران این پژوهش به شاخص‌ها اضافه و در دور دوم پرسشنامه به خبرگان جهت اعلام نظر ارائه گردید. در این صورت بر اساس ارزیابی مجدد هر خبره از نظر قبلی

[DOI: 10.61882/taxjournal.0.71]

خود، می‌توان نتایج جدیدی را بدست آورد. همچنین شاخص‌هایی که کمترین اهمیت را از دید خبرگان به خود تخصیص داده بوده‌اند پس از بررسی توسط پژوهشگران این پژوهش حذف گردید. در گام بعد اختلاف میانگین‌ها در دو پرسشنامه اول و دوم با استفاده از روابط فاصله میان اعداد فازی و بر اساس رابطه زیر محاسبه گردید. چنانچه این اختلاف میانگین از حد آستانه کم (مثال ۳. ۰) کمتر شود، فرایند متوقف می‌شود.

$$A^{(i)} = (a_1{}^{(i)}, a_2{}^{(i)}, a_3{}^{(i)}, a_4{}^{(i)}) \quad (۳)$$
$$i = 1, \ldots . n$$

$$A_m = (a_{m1,}\, a_{m2,}\, a_{m3,}\, a_{m4}\ )$$
$$= (\frac{1}{n}\ \sum\ a_1{}^{(i)}, \frac{1}{n}\ \sum\ a_2{}^{(i)}, \frac{1}{n}\ \sum\ a_3{}^{(i)}, \frac{1}{n} \sum\ a_4{}^{(i)}\ )$$

با توجه به اینکه در بعضی موارد اختلاف میانگین نظرات خبرگان در پرسشنامه‌های اول و دوم بزرگتر از ۳. ۰ است، برای سومین بار فرایند پرسشگری تکرار گردید این کار تا ثابت شدن نظرات خبرگان ادامه خواهد داشت. در گام بعد اختلاف میانگین‌ها در دو پرسشنامه دوم و سوم با استفاده از روابط فاصله میان اعداد فازی محاسبه گردید، با توجه به اینکه اختلاف میانگین نظرات خبرگان در پرسشنامه‌های دوم و سوم کوچک‌تر از ۳. ۰ است، فرایند پرسش‌گری متوقف می‌شود.

تجزیه و تحلیل داده‌ها

با استفاده از مرور ادبیات تحقیق و پیشینه پژوهش، ۶۱ شاخص اولیه برای مدل بلوغ امنیت سایبری زیرساخت‌های حیاتی شناسایی شد. بررسی این شاخص‌ها نشان می‌دهد که برخی از شاخص‌های احصاء شده، دارای همپوشانی و گاه تکراری هستند، بنابراین شاخص‌های تکراری، حذف و در نهایت، ۵۱ شاخص یکتا مشخص گردید. آنگاه مؤلفه‌های اصلی شناسایی شده (بر اساس محتوای شاخص‌ها)، در قالب سه بعد کلی دسته‌بندی شدند. این سه بعد، شامل عوامل فردی، عوامل سازمانی و عوامل فنی می‌باشند. برخی از شاخص‌های احصاء شده در این سه بعد در جداول زیر آمده است.

[DOI: 10.61882/taxjournal.0.71]

جدول ۵. مؤلفه‌های اصلی شناسایی شده و برخی از شاخص‌های احصاء شده

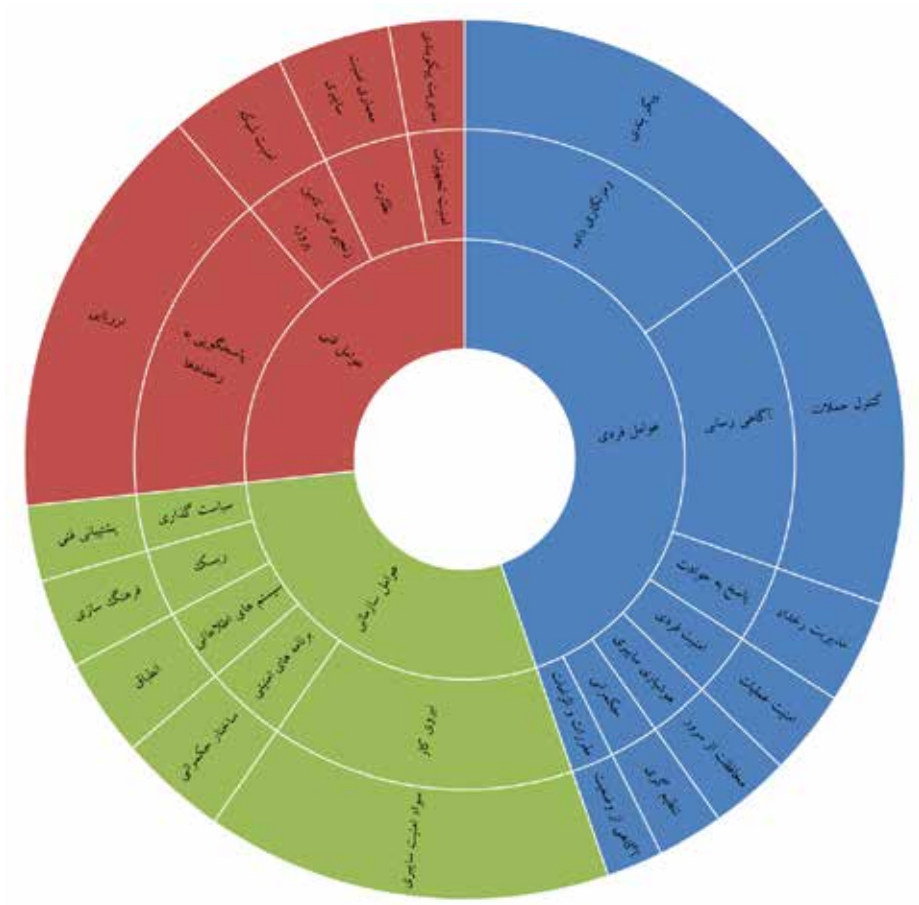
عوامل فردی	مدیریت رخداد	پاسخ به حوادث
	آگاهی از وضعیت	مقررات و الزامات
	امنیت عملیات	امنیت فردی
	کنترل حملات	آگاهی رسانی
	پیکربندی	رمزنگاری داده
	محافظت از سرور	هوشیاری سایبری
	تنظیم‌گری	حکمرانی
	پشتیبانی فنی	سیاست‌گذاری
	فرهنگ‌سازی	ریسک
عوامل سازمانی	سواد امنیت سایبری	نیروی کار
	ساختار حکمرانی	برنامه‌های امنیتی
	انطباق	سیستم‌های اطلاعاتی
	امنیت شبکه	زنجیره امن تأمین پروژه
عوامل فنی	مدیریت پیکربندی	امنیت تجهیزات
	معماری امنیت سایبری	نظارت
	ارزیابی	پاسخگویی به رخدادها

منبع: یافته‌های پژوهش.

شاخص‌های احصاء شده در این جداول منجر به ارائه مدل مفهومی گردید که در نمودار (۴) آمده است.

[DOI: 10.61882/taxjournal.0.71]

نمودار ۴. ارائه مدل مفهومی امنیت سایبری فضای ابری سامانه مؤدیان



منبع: یافته‌های پژوهش.

بحث و نتیجه‌گیری

در پژوهش صورت گرفته، برخی از شاخص‌های مدل و اهداف بدست آمده از آن‌ها، در جدول (۶) آمده است. بررسی این شاخص‌ها نشان می‌دهد برخی از شاخص‌های احصاء شده دارای همپوشانی با سایر شاخص‌ها می‌باشند. بنابراین در این پژوهش شاخص‌های دارای همپوشانی در ۱۳ گروه، دسته‌بندی شده و در جدول (۷) ارائه شده است.

[DOI: 10.61882/taxjournal.0.71]

جدول ۶. شاخص‌ها و اهداف مدل

شاخص	اهداف
معماری امنیت سایبری (Architecture)	ایجاد و حفظ ساختار معماری امنیت سایبری سازمان، شامل کنترل‌ها، فرایندها، فناوری‌ها و سایر عناصر، متناسب با اهمیت زیرساخت‌های حیاتی و اهداف سازمانی.
مدیریت دارایی، تغییر و پیکربندی (Asset)	مدیریت موجودی دارایی، مدیریت پیکربندی دارایی، مدیریت تغییرات در دارایی‌ها
مدیریت رخداد و تهدید (Treat)	رخدادها و تهدیدها شناسایی شده و به آن‌ها پاسخ داده می‌شود، کاهش آسیب‌پذیری امنیت سایبری
مدیریت نیروی کار (Workforce)	تعیین مسئولیت‌های امنیت سایبری، کنترل چرخه حیات نیروی کار، توسعه نیروی کار امنیت سایبری، افزایش آگاهی نیروی کار در حوزه امنیت سایبری
آگاهی از موقعیت (Situation)	ثبت وقایع (Logging)، نظارت
مدیریت برنامه‌های امنیت سایبری (Program)	ایجاد و حفظ یک برنامه امنیت سایبری سازمانی، تدوین برنامه‌ریزی راهبردی و حمایت مالی برای فعالیت‌های امنیت سایبری سازمان، به گونه‌ای که اهداف امنیت سایبری را هم با اهداف راهبردی سازمان و هم با اهمیت زیرساخت‌های حیاتی همسو می‌کند.

منبع: یافته‌های پژوهش.

نتایج این گروه‌بندی در جدول (۷) به لحاظ فراوانی و اهمیت شاخص‌ها بدست آمده است:
شاخص مدیریت رخداد با فراوانی ۱۱، توانسته است جایگاه اول را کسب کند. به همین جهت، این شاخص مورد توجه‌ترین شاخص در ایمن‌سازی زیرساخت‌های سامانه تلقی می‌گردد.
شاخص‌های کنترل دسترس ، نظارت و امنیت فیزیکی با فراوانی ۸ به طور مشترک در جایگاه بعدی قرار می گیرند.
شاخص‌های امنیت اطلاعات، سیاست های امنیتی، مدیریت ریسک و مدیریت نیروی کار با فراوانی ۷ در جایگاه بعدی قرار دارند.
شاخص مدیریت دارایی با فراوانی ۶ در جایگاه بعدی قرار دارد.
شاخص آگاهی و اطلاع رسانی با فراوانی ۵ در موضع بعدی قرار دارد.
شاخص رمز نگاری داده‌ها با فراوانی ۴ در جایگاه بعدی قرار دارد.
شاخص امنیت معماری با فراوانی ۳ در جایگاه بعدی قرار دارد.

[DOI: 10.61882/taxjournal.0.71]

شاخص حکمرانی با فراوانی ۲ در جایگاه آخر قرار دارد.

با توجه به نتایج بدست آمده و بر اساس جدول (۱۰)، در ادامه، نمودار گروه‌بندی شاخص‌ها بر اساس فراوانی و فراوانی نسبی ارائه می‌شود.

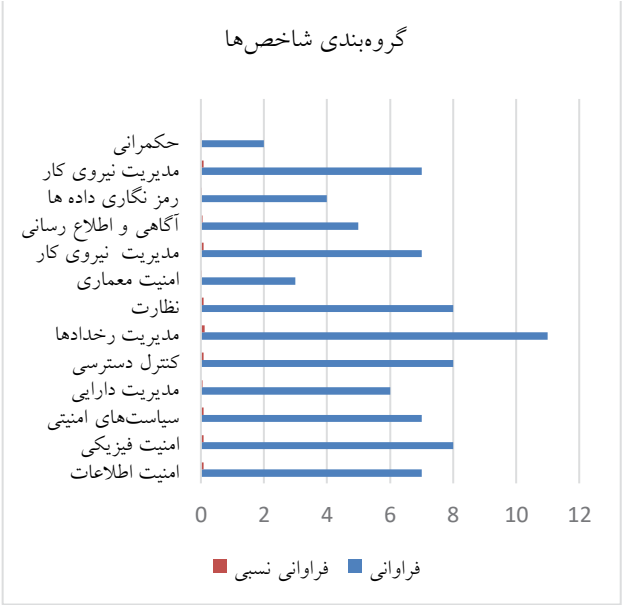
جدول۷. گروه‌بندی شاخص‌های دارای همپوشانی

ردیف	گروه‌بندی	فراوانی	فراوانی نسبی
۱	امنیت اطلاعات	۷	۰.۰۸
۲	امنیت فیزیکی	۸	۰.۰۹
۳	سیاست‌های امنیتی	۷	۰.۰۸
۴	مدیریت دارایی	۶	۰.۰۶
۵	کنترل دسترسی	۸	۰.۰۹
۶	مدیریت رخدادها	۱۱	۰.۱۲
۷	نظارت	۸	۰.۰۹
۸	امنیت معماری	۳	۰.۰۳
۹	مدیریت نیروی کار	۷	۰.۰۸
۱۰	آگاهی و اطلاع‌رسانی	۵	۰.۰۵
۱۱	رمزنگاری داده‌ها	۴	۰.۰۴
۱۲	مدیریت ریسک	۷	۰.۰۸
۱۳	حکمرانی	۲	۰.۰۲

منبع: یافته‌های پژوهش.

[DOI: 10.61882/taxjournal.0.71]

نمودار۵. گروه‌بندی شاخص‌ها بر اساس فراوانی و فراوانی نسبی



منبع: یافته‌های پژوهش.

در این مقاله، با احراز این مدل؛ نمودار (۴)، ابتدا مبانی نظری و اسناد بالادستی بین‌المللی در حوزه امنیت سایبری مورد مطالعه قرار گرفت. سپس با انتخاب پژوهش‌های منتخب به روش فراترکیب شاخص‌های بلوغ امنیت سایبری احصاء گردید، شاخص‌های مشابه حذف و در نهایت با توجه به حوزه عملکرد و با اتکا به مطالعات صورت گرفته در پیشینه پژوهش و مبانی نظری، ابعاد و مؤلفه‌ها تدوین و شاخص‌ها بر اساس ارتباط مفهومی در ابعاد و مؤلفه‌ها دسته‌بندی گردید و پس از آن این شاخص‌ها به روش دلفی فازی با خبرگان به اشتراک گذاشته شد، در نتیجه شاخص‌های کم اهمیت از نظر خبرگان حذف و شاخص‌های پیشنهادی مجدد در پرسشنامه دوم با خبرگان به اشتراک گذاشته شد و این مرحله تا توافق میان خبرگان ادامه پیدا کرد. در این پژوهش، ابعاد، مؤلفه‌هاو شاخص‌های مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور پس از مطالعه اسناد بین‌المللی و واکاوی مدل‌های مرجع بلوغ امنیت سایبری و امنیت اطلاعات با استفاده از روش فراترکیب احصاء و از مراجعه به آرای خبرگان حوزه امنیت سایبری استنباط گردید و با تجزیه و تحلیل مفاهیم و مضامین بدست آمده به صورت مدلی متشکل از ابعاد، مؤلفه‌ها و شاخص‌ها ارائه شد. بر اساس تحلیل‌های انجام گرفته و تحلیل

[DOI: 10.61882/taxjournal.0.71]

محتوای مقالات در مجموع۵۱ شاخص، ۱۱ مؤلفه و ۳ بعد جهت ارائه مدل مفهومی بلوغ امنیت سایبری فضای ابری سامانه مؤدیان سازمان امور مالیاتی کشور شناسایی گردید، در همین راستا مؤلفه‌های «اهمیت فردی نسبت به آگاهی از وضعیت» در بعد فردی، مؤلفه‌های «مدیریت ریسک، مقررات و الزامات، برنامه‌ریزی‌های امنیتی و مدیریت منابع انسانی» در بعد سازمانی و مؤلفه‌های «امنیت تجهیزات فیزیکی، سواد امنیت سایبری، نظارت، پاسخگویی به رخدادها، پشتیبانی فنی و سیستم‌های اطلاعاتی در بعد فنی قرار گرفتند. در جدول (۸) مقایسه برخی از مدل‌های دیگر قرار داده شده‌اند.

جدول ۸ مقایسه برخی شاخص‌ها و اهداف مدل بلوغ امنیت سایبری و امنیت اطلاعات

ردیف	نام مدل	شاخص‌های تدوین شده
۱	C2M2	مدیریت دارایی، تغییر و پیکربندی، مدیریت ریسک، مدیریت دسترسی، پاسخ به حوادث، مدیریت امنیت سایبری، مدیریت نیروی کار
۲	NICE	برنامه‌ریزی نیروی کار، فرایند کسب و کار، مدیریت ریسک، ساختارهای حکمرانی
۳	CYSFAM	محافظت از سرور، کنترل کاربر، امنیت شبکه، امنیت برنامه‌های کاربردی، رمزنگاری، امنیت تجهیزات قابل حمل، مدیریت حوادث امنیت سایبری

منبع: یافته‌های پژوهش.

مثال‌های کاربردی داخلی (ایران‌محور)

پنج هدف اصلی پدافند غیرعامل در سیاست ابلاغی از سوی مقام معظم رهبری، افزایش بازدارندگی، تداوم فعالیت ضروری، تسهیل مدیریت بحران، کاهش آسیب‌پذیری و ارتقای پایداری ملی است. در این پژوهش هدف دوم یعنی تداوم فعالیت ضروری موردبررسی قرار گرفته است؛ بنابراین، نظر به اینکه فضای سایبری هیچ گونه حد و مرزی ندارد و با کمترین هزینه و از هر نقطه جهان می‌توان هدف را موردحمله قرار داد، تهدیدات سایبری را می‌توان یکی از بزرگ‌ترین چالش‌های پیشروی حوزه امنیت زیرساخت‌های حیاتی قلمداد کرد. به همین جهت، فرایند طراحی سیاست‌های امنیت سایبری پایدار برای زیرساخت‌های حیاتی، در دستورکار بیشتر کشورهای جهان و همچنین سازمان پدافند غیرعامل کشور قرار گرفته است. ازاین رو، ضرورت دارد با توجه به اینکه در سال‌های اخیر حجم حملات سایبری به زیرساخت‌های حیاتی جمهوری اسلامی ایران، توسط دولت‌های متخاصم افزایش یافته است،

[DOI: 10.61882/taxjournal.0.71]

مدلی برای بالا بردن ضریب تاب‌آوری و امنیت سایبری زیرساخت‌های حیاتی ارائه شود. در گام اول برای رسیدن به این مدل، باید شاخص‌های ایمن‌سازی زیرساخت‌ها حاصل شود و سپس نسبت به تدوین مدل بلوغ امنیت سایبری برای این زیرساخت‌ها اقدام گردد.

در همین راستا پژوهش‌های متعددی انجام شده است که در پیشینه پژوهش به آن‌ها اشاره شده است.

تعارض منافع

این پژوهش تعارض منافع ندارد.

سپاسگزاری

از کلیه مشارکت‌کنندگان در تهیه و تدوین این مقاله تشکر و قدرانی می‌شود.

ORCID

Marzieh Davoodi https://orcid.org/0009-0003-2516-8037

Mohammad Mehdi Shirmohammadi https://orcid.org/0009-0004-8554-0838

[DOI: 10.61882/taxjournal.0.71]

منابع

۱. علیزاده سودمند، علیرضا، و فتحی هفشجانی، کیامرث، و شاه‌منصوری، اشرف، و عرب‌سرخی، ابوذر. (۱۴۰۳). تحلیل ساختارمند شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور. پدافند غیرعامل، ۱۵(۱)، ۸۷-۱۰۳.

۲. فرهادی مقدم، زینب. (۱۴۰۳). بررسی امنیت سایبری در دنیای اتصالات هوشمند: چالش‌ها و راهکارها. بیست و دومین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات، بابل، ایران.

۳. اختری، محمد، و کرامتی، محمدعلی، و موسوی، سید عبداله امین. (۱۴۰۱). مقایسه تطبیقی مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات و احصاء شاخص‌های امنیت سایبری مشترک. پدافند غیرعامل، ۱۳(۴)، ۲۱-۳۸.

۴. ولوی، محمد رضا، و نیک نفس، علی. (۱۴۰۰). مدل بلوغ نظام رصد و پایش و هشداردهی سایبری جمهوری اسلامی ایران. فصلنامه علمی امنیت ملی، ۴۰(۱۱)، ۱۵۵-۱۸۲.

۵. اخوان، فاطمه، و رادفر، رضا. (۱۳۹۹). ارائه مدلی برای پایش بلوغ امنیت اطلاعات. فصلنامه رشد فناوری، ۶۴(۲)، ۴۱-۵۱.

۶. میریوسفی، سید محسن، و غفاری، رضا. (۱۴۰۰). راهبردهای نوین حفاظت از زیرساخت‌های حیاتی. نشریه علمی پدافند غیر عامل، ۳(۴)، ۱-۱۴ .

۷. عابدی جعفری، عابد، و امیری، مجتبی. (۱۳۹۸). فراترکیب، روشی برای سنتز مطالعات کیفی. فصلنامه علمی پژوهشی روش‌شناسی علوم انسانی، ۲۵(۹۹)، ۷۳-۸۷.

[DOI: 10.61882/taxjournal.0.71]

References

1. Afshar, A., Termechi, A., Golshan, A., Aghaeian, A., Shahriari, H. R., Soleimani, S. (2018). Review of the Types of Strategies to Improve Security of Industrial Control Systems and Critical Infrastructure. *Journal of Passive Defence, 9*(2), 1-9. [In Persian]
2. Aghaei, M., Moeini, A., Arabsorkhi, A., Mohammadian, A., & Zareyi, A. A. (2019). A Logical Conceptual Model for Classifying Critical Infrastructure Cyber Threats. *Journal of National Security, 2,* 201-231. [In Persian]
3. Akhavan, F., & Radfar, R. (2021). A Model for Monitoring Information Security Maturity. *Journal of Technology Growth, 64*, 41-51. [In Persian]
4. Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. *Applied Sciences*, *10*(10), 1-15.
5. Bridget, J. (2021). *Information Security Maturity Model for Healthcare Organizations in the United States* (Doctoral Dissertation). University of Portland State, Portland.
6. British Standards Institution. (2013). *Moving from ISO 27001:2005 to ISO 27001:2013.* London: BSI. [In Persian]
7. Ide, M. (2019). *Cybersecurity Capability Maturity Model for Critical Information Technology Infrastructure among Nigerian Financial Organizations* (Doctoral Dissertation, Universiti Teknologi Malaysia).
8. Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). A Vulnerability-Driven Cyber Security Maturity Model for Measuring National Critical Infrastructure Protection Preparedness. *International Journal of Critical Infrastructure Protection*, *15*, 47-59.
9. Miryousefi, M., & Ghaffarpour, R. (2021). New Critical Infrastructure Protection Strategies. *Journal of Passive Defence, 3*, 1-14. [In Persian]
10. Rea-Guaman, A. M., San Feliu, T., Calvo-Manzano, J. A., & Sánchez-García, I. D. (2017). Comparative Study of Cybersecurity Capability Maturity Models. In *International Conference on Software Process Improvement and Capability Determination* (100-113). Cham: Springer International Publishing.
11. Saleh, M. (2021). Information Security Maturity Model. *International Journal of Computer Science and Security, 5*(3), 316-337.
12. U.S. Department of Energy. (2021). Office of Cybersecurity, Energy Security and Emergency Response. *CyberSecurity Capability Maturity Model (C2M2)*, *2.1*, 1-96.

[DOI: 10.61882/taxjournal.0.71]

13. Wong, W. N. Z. Z., & Shi, J. (2014). *Business Continuity Management System: A Complete Guide to Implementing ISO 22301*. London: Kogan Page Publishers.
14. Yigit Ozkan, B., Van Lingen, S., & Spruit, M. (2021). The Cybersecurity Focus Area Maturity (CYSFAM) Model. *Journal of Cybersecurity and Privacy*, *1*(1), 119-139.
15. Yigit Ozkan, B., & Spruit, M. (2018). A Questionnaire Model for Cybersecurity Maturity Assessment of Critical Infrastructures. In *International Workshop on Information and Operational Technology Security Systems* (49-60). Cham: Springer International Publishing.

استناد به این مقاله: داودی، مرضیه، و شیرمحمدی، محمدمهدی. (۱۴۰۴). ارائه مدل مفهومی بلوغ امنیت سایبری در فضای ابری سامانه مؤدیان سازمان امور مالیاتی کشور. پژوهشنامه مالیات، ویژه‌نامه همایش سیاست‌های مالی و مالیاتی ایران، ۷۱ - ۹۸ .