Scientific Journal of Electronic & Cyber Defense
Vol. 12, No. 2, Summer 2024, Serial No. 46
ISSN: 2322-4347 , E-ISSN: 2980-8979

Proposing framework for comparative evaluation of information security risk assessment methods (Case of study: Iranian Research Institute for Information Science and Technology (IranDoc))

H.R Khedmatgozar[1]* , H. Hassani [2]
Assistant Professor, Iran Information Science and Technology Research Institute (Irandak), Tehran, Iran

(Received: 2023/05/03, Revised: 2023/07/20, Accepted: 2024/07/30, Published: 2024/08/31)
DOR:

ABSTRACT

One of the key actions in information security management is information security risk management, the main stage of which is known as "information security risk assessment". So far, various methods, standards and frameworks have been formed for this purpose. The main question that has been considered in this study is that despite this range of information security risk assessment methods, how should an organization choose and implement the appropriate method for its goals and situation. To answer this question, in this research, first, an evaluation framework consisting of 13 evaluation criteria was designed in two categories: the nature of the method and the adaptation of the method to the organizational situation. Then, based on this framework, 18 well-known information security risk assessment methods were evaluated in the organizational case of Iranian Research Institute for Information Science and Technology (IranDoc). The results of this evaluation showed that the proposed framework has the required validity. Based on these results, the ISO 27005 standard was recognized as the most appropriate method of information security risk assessment in the investigated case. Finally, based on these results and in line with further development and validation of the presented framework, suggestions were presented .

Keywords: Information Security Risk Assessment (ISRA), ISRA methods, IranDoc.

*Corresponding Author Email: khedmatgozar@irandoc.ac.ir

"پدافند الکترونیکی و سایبری"
سال دوازدهم، شماره ۲، تابستان ۱۴۰۳، ص ۳۹-۲۷

علمی – پژوهشی

ارائه چارچوبی برای ارزیابی تطبیقی روش‌های ارزیابی مخاطره امنیت اطلاعات (موردمطالعه: پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک))

حمیدرضا خدمتگزار[۱*]، حمید حسنی[۲]

۱– استادیار،۲– دانشجوی دکتری، پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)، تهران، ایران.

(دریافت: ۱۴۰۳/۰۲/۱۴، بازنگری: ۱۴۰۳/۰۴/۳۰، پذیرش: ۱۴۰۳/۰۵/۲۳، انتشار: ۱۴۰۳/۰۶/۱۰)

DOR:

ناشر: دانشگاه جامع امام حسین (ع) نویسندگان

چکیده

یکی از اقدامات کلیدی در مدیریت امنیت اطلاعات، مدیریت مخاطره امنیت اطلاعات است که اصلی‌ترین مرحله آن با نام «ارزیابی مخاطره امنیت اطلاعات» شناخته می‌شود. تاکنون در سطح دنیا روش‌ها، استانداردها و چارچوب‌های مختلفی بدین منظور شکل‌گرفته است. پرسش اصلی که در این مطالعه مورد توجه قرار گرفته است آنست که باوجود این گستره از روش‌های ارزیابی مخاطره امنیت اطلاعات، یک سازمان چگونه باید روش منطبق با اهداف و وضعیت خود را انتخاب و اجرا کند. به‌منظور پاسخ به این پرسش، در این پژوهش ابتدا چارچوب ارزیابی متشکل از ۱۳ معیار ارزیابی در دودسته ماهیت روش و انطباق روش با وضعیت سازمانی طراحی شد. سپس مبتنی بر این چارچوب، ۱۸ روش شناخته شده ارزیابی مخاطره امنیت اطلاعات در بافت سازمانی پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) مورد ارزیابی قرار گرفتند. نتایج این ارزیابی نشان داد چارچوب پیشنهاد شده از اعتبار لازم برخوردار است. بر اساس این نتایج نیز استاندارد ایزو ۲۷۰۰۵ منطبق‌ترین روش ارزیای مخاطره امنیت اطلاعات در بافت مورد بررسی شناخته شد. در انتها نیز مبتنی بر این نتایج و در راستای توسعه و اعتباریابی بیشتر چارچوب ارائه شده پیشنهاداتی ارائه شد.

کلیدواژه‌ها: ارزیابی مخاطره امنیت اطلاعات، روش‌های ارزیابی، ایرانداک ،

۱- مقدمه

با پیشرفت سیستم‌های رایانه‌ای، رایانش ابری، خدمات شبکه‌های اجتماعی و همچنین وابستگی کسب‌وکارها به فناوری اطلاعات، خطرهای زیادی کسب‌وکارها را در معرض سرقت اطلاعات، ازبین‌رفتن اطلاعات و یا تخریب اطلاعات قرار می‌دهند. اطلاعات، از مهم‌ترین دارایی‌ها برای سازمان‌ها و افراد به شمار می‌آید. ازدست‌دادن حتی کوچک‌ترین بخش از این گنجینه، نیاز به‌صرف زمان، هزینه و نیروی کار غیرقابل‌تصوری برای جبران دارد و گاهاً می‌تواند اصول کاری و حتی موجودیت یک سازمان را تهدید کند. بیشتر سازمان‌ها برای بقا، پیشرفت و حفاظت از دارایی‌های اطلاعاتی‌شان، به سیستم‌های اطلاعاتی اعتماد می‌کنند [۱]. برای این منظور، مدیریت امنیت اطلاعات برای ایجاد امنیت در پیدایش و تبادل اطلاعات، به کمک نظام مدیریتی بر پایه استانداردها و راهنماهای فنی و تصمیم‌های صحیح مدیریتی، می‌تواند موجب بهبود عملکرد نظام اطلاعاتی و ارتباطی شود. در واقع، موضوع امنیت اطلاعات به‌عنوان مهم‌ترین عنصر فناوری اطلاعات در سازمان‌ها، استفاده از سیستم‌های امنیت اطلاعات را با چالش مخاطره مواجه کرده است. اگر فرآیند به‌کارگیری روش‌های مدیریت و ارزیابی مخاطره در این سیستم‌ها به‌درستی انجام شود، می‌تواند تأثیر چشمگیری بر سازماندهی فعالیت‌های امنیت اطلاعاتی سازمان‌ها داشته باشد [۲].

امنیت اطلاعات بر پایهٔ تعریف «انجمن سیستم‌های امنیت ملّی» [۲]، به معنای حفاظت از اطلاعات و مؤلفه‌های اصلی آن است که سیستم‌ها، سخت‌افزارها، انباره‌ها و انتقال اطلاعات را در برمی‌گیرد. در استاندارد ایزو ۲۷۰۰۱ [۳] امنیت اطلاعات این‌گونه تعریف شده است: «امنیت اطلاعات عبارت است از حفاظت از محرمانگی، صحت و درستی و دسترس‌پذیری اطلاعات. به علاوه، مشخصه‌های دیگری از قبیل تأیید صحت و سندیت[۴]، پاسخ‌گویی[۵]، عدم انکار[۶] و قابلیت اطمینان را نیز می‌توان مدنظر قرارداد». در امنیت اطلاعات از مجموعه‌ای از

[2] Committee on National Security Systems (CNSS)
[3] ISO 27001
[4] Authenticity
[5] Accountability
[6] Non-Repudiation

* رایانامه نویسنده مسئول: khedmatgozar@irandoc.ac.ir

تدابیر، روش‌ها و ابزارها برای محافظت از نظام‌های رایانه‌ای و ارتباطی در برابر دسترسی و تغییرات غیرمجاز استفاده می‌شود [۴]. باتوجه‌به انتشار گستردهٔ استفاده از اینترنت، تبادل اطلاعات و هزینه‌های مصرفی برای ایجاد یکپارچگی اطلاعات، امروزه ضرورت کنترل و مدیریت حرکت اطلاعات و استفاده از سامانه‌های جامع برای مدیریت امنیت اطلاعات بیشتر از پیش احساس می‌شود [۵].

با پررنگ‌تر شدن نقش اطلاعات و میزان اهمیت آن برای سازمان‌های گوناگون، رفته‌رفته موضوع امنیت اطلاعات و نیاز دستیابی به یک سیستم مدیریت امنیت اطلاعات اهمیت بیشتری یافته است. تا جایی که توسعه امنیت اطلاعات در طول ۵۰ سال گذشته، به شکل‌های گوناگونی نمود پیدا کرده است. یکی از این اشکال، بیانگر سیر تکامل و پیشرفت امنیت اطلاعات در چهار موج فنی، مدیریتی، نهادینه‌سازی و حاکمیت امنیت اطلاعات است [۶- ۸]. مدیریت امنیت اطلاعات جزء سیستم کلی و برجستهٔ مدیریت در هر سازمان است که بر اساس رویکرد مخاطرات کسب‌وکار قرار دارد، و هدف آن شامل بنیان‌گذاری، اجرا، بهره‌برداری، نظارت، بازبینی، نگه‌داری و بهبود امنیت اطلاعات است. با پیاده‌سازی دقیق این نوع مدیریت، می‌توان نقش مهمی در کاهش مخاطرات محیطی ایفا کرده و به تضمین سطح امنیت موردنیاز کمک کرد [۹]. مدیریت امنیت اطلاعات، بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف امنیت، بررسی موانع رسیدن به این اهداف و ارائه راهکارهای لازم را برعهده دارد [۱۰]. در نگاهی جامع به مدیریت امنیت اطلاعات، می‌توان آن را به‌صورت زیر تعریف کرد: یک چارچوب جامع، کامل و انطباق‌پذیر متشکل از برنامه‌های امنیتی و فرآیندها و رویه‌های مدیریتی که هدف نهایی آن تأمین و استمرار امنیت در محیط تبادل اطلاعات سازمانی می‌باشد. با پیدایش نخستین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵ میلادی، نگرش نظام‌مند به مقوله امن‌سازی فضای تبادل اطلاعات شکل گرفت [۵]. باتوجه‌به این دیدگاه، امنیت فضای تبادل اطلاعات در سازمان‌ها به تکرار تأمین نمی‌شود؛ بلکه این وظیفه باید به‌صورت مداوم و در چرخه‌ای از فرآیندها شامل مراحل طراحی، پیاده‌سازی، ارزیابی و بهبود انجام شود. برای این هدف، هر سازمان باید با رویکرد مشخص و برنامه‌ریزی دقیق، کنترل و نظارتی بر اطلاعات و تبادلات اطلاعات در داخل سازمان خود اعمال کند [۱۱].

مخاطره یا ریسک به‌احتمال اینکه یک تهدید بتواند از آسیب‌پذیری(های) یک یا گروهی از دارایی‌های اطلاعاتی استفاده کرده و سبب آسیب‌رساندن یا ازدست‌دادن آن دارایی(ها) گردد، گفته می‌شود [۱۲]. به‌عبارت‌دیگر، مخاطره احتمال یک اثر مشخص بر روی سیستم در یک دوره زمانی مشخص است که می‌تواند ترکیبی از احتمال وقوع تهدید، پیامد و آسیب‌پذیری باشد. در این تعریف با سه مفهوم دارایی اطلاعاتی، تهدید و آسیب‌پذیری مواجه هستیم که به شرح زیر تعریف می‌شوند:

-دارایی اطلاعاتی: هر چیزی مرتبط با اطلاعات که برای سازمان مهم است. به شکل کلی، خود اطلاعات، دارایی است که همانند دیگر دارایی‌های سازمان دارای ارزش بوده و در نتیجه باید به طور مناسبی مورد محافظت قرار گیرد. در یک دسته‌بندی کلی دارایی‌های اطلاعاتی را می‌توان در دسته‌های گوناگونی از جمله نرم‌افزارها، سخت‌افزارها، سرویس‌ها، منابع انسانی و اسناد اطلاعات جای داد.

-آسیب‌پذیری: به نقاط ضعف در توصیف، طراحی، پیاده‌سازی، پیکربندی و یا اجرای اطلاعات در دارایی‌های اطلاعاتی اشاره دارد که بتوان از آنها برای نقض امنیت اطلاعات استفاده کرد. یک آسیب‌پذیری تا زمانی که مورد سوءاستفاده یک تهدید قرار نگیرد، نمی‌تواند موجب آسیب شود.

-تهدید: یک عامل خطر است که به‌صورت بالقوه می‌تواند از یک یا چند آسیب‌پذیری سوءاستفاده کند. این تهدیدها می‌تواند منشأ طبیعی یا انسانی داشته باشد و به شکل تصادفی و یا عمدی باشند. یک تهدید می‌تواند بر یک یا چند دارایی تأثیر بگذارد [۱۳].

برای نمونه زمانی که در یک سامانه به‌عنوان یک دارایی اطلاعاتی، پیکربندی مناسب امنیتی وجود ندارد، این آسیب‌پذیری می‌تواند توسط تهدیدی با نام دسترسی غیرمجاز مورد سوءاستفاده قرار گرفته و یک رخداد امنیتی ایجاد کند. مجموع این ترکیب با عنوان یک مخاطره باید مورد توجه قرار گیرد. یک رخداد امنیتی می‌تواند موجب پیامدهایی شود که این پیامدها باید مورد توجه قرار گیرد. از مهم‌ترین این پیامدها می‌توان به کاهش سطح محرمانگی، صحت و دسترس‌پذیری اطلاعات اشاره کرد.

مدیریت مخاطرات امنیت اطلاعات که اساس سیستم مدیریت امنیت اطلاعات را تشکیل می‌دهد، فرآیندی برای شناخت مخاطرات پتانسیلی و برنامه‌ریزی جهت کاهش اثرات، ازبین‌بردن یا بهره‌برداری از آن‌ها است. این فرآیند می‌تواند شامل مراحل مختلفی باشد [۱۴]. از اصلی‌ترین گام‌های مدیریت مخاطره امنیت اطلاعات، ارزیابی مخاطره امنیت اطلاعات یا به‌اختصار «ایسرا» [1] است. با ارزیابی مخاطره امنیت اطلاعات می‌توان وضعیت امنیت اطلاعات را در سازمان مشخص و با اتخاذ تصمیمات صحیح و اقدامات پیش‌گیرانه، از هزینه‌های اضافی جلوگیری کرد [۱۵، ۱۶]. ارزیابی مخاطره امنیت اطلاعات به شکل کلی، یک روش نظام‌مند به‌منظور دستیابی به یک دید جامع در خصوص شناسایی (یافتن، تشخیص و تشریح)، تحلیل

[1] ISRA (Information Security Risk Assessment)

(درک ماهیت و تعیین سطح) و سنجش (مقایسه سطح با معیارها) مخاطره‌های امنیت اطلاعات است. بر پایهٔ بررسی‌های اولیه انجام شده، برای دستیابی به سطح مطلوبی از محافظت در برابر تهدیدها و فراهم‌کردن سازوکارهای لازم جهت محافظت از دارایی‌ها و دانش سازمان، تاکنون تعداد زیادی روش در قالب دستورالعمل‌ها/ راهنماها، استانداردها و چارچوب‌های ملّی و بین‌المللی از خاستگاه‌های گوناگون کاربردی و پژوهشی و به‌منظور ارزیابی مخاطره امنیت اطلاعات طراحی و به‌کارگرفته‌شده است. به همین دلیل، استفاده از روش‌های مدیریت و ارزیابی مخاطره می‌تواند تأثیر مهمی بر نحوه سازمان‌دهی فعالیت‌ها در زمینه امنیت اطلاعات داشته باشد [۲].

به شکل کلی، روش‌های متعددی برای ارزیابی مخاطره امنیت اطلاعات هستند [۱۲] و وظیفه اصلی هر سازمان تشخیص این مهم است که کدام روش را باید به کار گرفت. ازآنجاکه سازمان باید برای هر کدام از آن روش‌ها هزینه‌ای را صرف کند، لذا این امر ضروری است که روش انتخاب شده سازگار با الزامات سازمان و منطبق بر یکی از استانداردهای مدیریت مخاطره امنیت اطلاعات باشد. اگر پارامترهای مورداستفاده برای همه روش‌های ارزیابی مخاطره قابل‌اجرا باشند، سازمان‌ها می‌توانند تمامی پارامترهای ممکن را برای مشاهده عینی، و تصمیم به بهره‌برداری از بهترین روش، مورد ارزیابی قرار دهند.

پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) پژوهشگاهی است که باهدف اصلی توسعه و گسترش پژوهش در زمینه علوم و فناوری اطلاعات، مدیریت دانش و جامعه اطلاعاتی و همچنین تجاری‌سازی دستاوردهای پژوهشی پدیدآمده است. مأموریت‌های کلیدی تعریف شده برای این پژوهشگاه ۱- پژوهش،۲- آموزش، ۳- مدیریت اطلاعات علمی و فناورانه، ۴- توسعه منابع انسانی در زمینه علوم و فناوری اطلاعات، مدیریت اطلاعات، و اطلاع‌رسانی، و ۵- همکاری و هماهنگی است. در حوزه مأموریتی مشخص شده در پژوهشگاه، انواع سامانه‌ها، خدمات و تجهیزات فناوری اطلاعات در حال توسعه و فعالیت هستند. به تبع فعالیت و مأموریت این پژوهشگاه در حوزه فناوری اطلاعات، اهمیت مدیریت امنیت اطلاعات به شکل کلی و ارزیابی مخاطره امنیت اطلاعات را به شکل خاص در آن دوچندان کرده است. از این‌رو مسأله اصلی این مطالعه را می‌توان ارزیابی و انتخاب روش ارزیابی مخاطره امنیت اطلاعات به منظور بکارگیری در نظام مدیریت امنیت اطلاعات در پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) تعریف کرد.

در همین راستا، بخش دوم مقاله به‌مرور پیشینه، بخش سوم به روش پژوهش، بخش چهارم به تجزیه‌وتحلیل یافته‌ها، و بخش پنجم به بحث و نتیجه‌گیری می‌پردازد.

۲- مرور پیشینه

در این بخش به بررسی پژوهش‌های گذشته در حوزه بررسی و مقایسه روش‌های ارزیابی مخاطرات امنیت اطلاعات می‌پردازیم. در این پژوهش‌ها رویکردهای مختلفی به‌منظور بررسی و مقایسه این روش‌ها به‌کاررفته است. در برخی از پژوهش‌های گذشته در این حوزه، به بررسی مزایا و معایب روش‌های کیفی و کمی ارزیابی مخاطرات امنیت اطلاعات پرداخته شده است. به طور مثال در پژوهش «لی» [۱۷]، این دو نوع رویکرد مورد بررسی و مقایسه قرار گرفتند. وی پیشنهاد می‌کند که روش‌های کمی را می‌توان برای تجزیه و تحلیل هزینه- فایده و برای به دست آوردن نتایج دقیق‌تر مورد استفاده قرار داد، اما آنها بر مقیاس اندازه‌گیری متکی هستند. با این حال، روش‌های کیفی، ارائه تحلیل هزینه و فایده را دشوارتر می‌کنند. در این پژوهش به بررسی روش‌های ارزیابی مخاطرات امنیت اطلاعات از جنبه فنون مورد استفاده در توسعه روش‌ها پرداخته شده است و بیان می‌کند فرآیند تحلیل سلسله مراتبی «ای.اچ.پی»[1]، شبکه عصبی، منطق فازی در توسعه و فرآیند ارزیابی مخاطرات امنیت مورد استفاده قرار گرفته‌اند. همچنین «آیونیتا» [۱۸] در پژوهش خود به بررسی و مقایسه و ارائه مزایا و معایب ۱۴ روش ارزیابی مخاطره امنیت اطلاعات پرداخته است. در این پژوهش به منظور بررسی روش‌های ارزیابی مخاطره امنیت اطلاعات از معیارهایی نظیر قیمت، کاربران، و محدوده جغرافیایی استفاده شده است. همچنین در این پژوهش ۲۵ ابزار مورد استفاده در فرآیند ارزیابی مخاطره امنیت اطلاعات و ۷ مدل مفهومی نیز مورد بررسی و مقایسه قرار گرفته است. علاوه بر این، دستورالعمل‌هایی به منظور کمک به سازمان‌ها در فرآیند انتخاب روش ارزیابی مخاطره امنیت اطلاعات تدوین شده است.

در برخی دیگر از پژوهش‌های انجام شده در این حوزه، با استفاده و الهام‌گرفتن از یک استاندارد یا چارچوب بین‌المللی به مقایسه روش‌های مختلف ارزیابی مخاطره امنیت اطلاعات پرداخته شده است. به طور مثال «وانگن» و همکارانش [۱۹] در پژوهشی به توسعه «چارچوب مخاطره یکپارچه هسته‌ای» [2] به‌منظور مقایسه روش‌های ارزیابی مخاطره امنیت اطلاعات پرداختند. بر خلاف پژوهش‌های مختلفی که به بررسی و مقایسه روش‌های ارزیابی مخاطره امنیت اطلاعات بر اساس تعدادی معیار از پیش تعریف‌شده پرداخته‌اند، در این پژوهش با درنظرگرفتن ایزو ۲۷۰۰۵ به‌عنوان مدل مرجع و سه فرآیند اصلی شناسایی مخاطره، تحلیل مخاطره و سنجش مخاطره با رویکردی پایین‌به‌بالا به مقایسه روش‌های ارزیابی مخاطره امنیت اطلاعات

[1] Analytic Hierarchy Process (AHP)
[2] Core Unified Risk Framework (CURF)

پرداختند. در این پژوهش ۱۱ روش مختلف ارزیابی مخاطره امنیت اطلاعات مورد مقایسه قرار گرفت. همچنین در پژوهش «لَبسکگنی» [۲۰] وی یک چارچوب مقایسه‌ای مبتنی بر چارچوب بین‌المللی حاکمیت فناوری اطلاعات «کوبیت» [1] ارائه می‌دهد. ازآنجایی‌که چارچوب مقایسه‌ای مبتنی بر این چارچوب حاکمیتی فناوری اطلاعات است، یک روش عینی برای مقایسه ویژگی‌های گوناگون روش‌های ارزیابی مخاطره امنیت اطلاعات ارائه می‌دهد. این چارچوب مقایسه‌ای همچنین نشان می‌دهد که آیا یک روش ارزیابی مخاطره امنیت اطلاعات مطابق با توصیه‌های حاکمیت فناوری اطلاعات است یا خیر. روش‌های مورد ارزیابی در این پژوهش، روش‌های «کرام»، «اُکتاو» و «کُرا» [2] بودند. پس از ارزیابی، نقاط قوت و ضعف هر کدام از این روش‌ها و جنبه‌های مهم در مورد روش‌های ارزیابی مخاطره امنیت اطلاعات مشخص شد.

برخی از پژوهش‌های دیگر در حوزه مقایسه روش‌های ارزیابی مخاطره امنیت اطلاعات به‌مرور نظام‌مند از پژوهش‌های پیشین و روش‌های مورداستفاده در این حوزه و ارائه یک طبقه‌بندی از آنها پرداخته‌اند. به طور مثال «پَن» و همکاران [۲۱] در پژوهشی به مرور نظام‌مند پژوهش‌های صورت گرفته در حوزه ارزیابی مخاطره امنیت اطلاعات در سال‌های ۲۰۰۴ تا ۲۰۱۴ پرداخته‌اند و یک چارچوب طبقه‌بندی از آنها ارائه کرده‌اند. در مطالعه آنها، پژوهش‌های مورد بررسی قرار گرفته شده در هفت طبقه شامل شناسایی مخاطره، مقایسه تحلیل مخاطره، بهبود تحلیل مخاطره، مقایسه چارچوب‌ها، بهبود چارچوب‌ها، مطالعه موردی، و سایر دسته‌بندی شدند. این مرور نظام‌مند نشان می‌دهد که نظریه فازی به طور گسترده‌ای برای کاهش ذهنیت در محاسبه امتیازات مخاطره استفاده می‌شود. از جمله نتایجی که این پژوهش نشان داد این است که عمده رویکردهای کنونی تحلیل مخاطره، به جای تمرکز بر انواع خاصی از خطرات امنیت اطلاعات، مقابله با تهدیدات عمومی را پیشنهاد می‌کنند. در حالی که این رویکرد ممکن است از منظر آکادمیک مطلوب باشد، ولی از منظر عملی کار مخاطرات زیادی به دنبال داشته باشد. در برخی پژوهش‌های دیگر، ویژگی‌هایی دیگری در کنار ویژگی‌هایی مانند کمی یا کیفی بودن برای طبقه‌بندی روش‌های ارزیابی مخاطره امنیت اطلاعات ارائه شده است. به طور مثال در پژوهش «شاملی-سندی» و همکارانش [۲۲] یک طبقه‌بندی از روش‌های ارزیابی مخاطره امنیت اطلاعات بر اساس چهار ویژگی ارزیابی (کیفی، کمی، و ترکیبی)، منظر (دارایی، سرویس، و فرآیند کسب و کار،)، ارزش‌گذاری منابع (حیاتی یا غیرحیاتی بودن)، و اندازه‌گیری مخاطره (قابل انتشار بودن به منابع دیگر یا غیر قابل انتشار بودن) انجام شده است. در پژوهش آنها ۱۲۵ مقاله از سال‌های ۱۹۹۵ تا ۲۰۱۴ مورد بررسی و مقایسه قرار گرفت.

برخی از پژوهش‌های دیگر مقایسه روش‌های ارزیابی مخاطره امنیت اطلاعات را در طی فرآیندی چندمرحله‌ای و با استفاده از شاخص‌های مختلف در هر مرحله انجام داده‌اند. به طور مثال «مَسدو» و «داسیلوا» [۲۳] در پژوهشی به بررسی و مقایسه ۲۲ روش ارزیابی مخاطره امنیت اطلاعات در طی سه مرحله پرداختند. این روش‌ها در مرحله اول با چهار معیار عینی روش یا راهنما بودن، به‌صورت مشخص برای اندازه‌گیری مخاطرات امنیت اطلاعات به‌کاررفتن، قیمت و دسترس‌پذیری مستند مربوطه، و به‌روز بودن یا نبودن مورد مقایسه قرار گرفتند. خروجی مرحله اول حذف ۱۶ روش از ۲۲ روش اولیه بوده است؛ این مدل‌ها با یک یا چند معیار مطابقت نداشتند و به همین دلیل به طور عمیق‌تر موردمطالعه قرار نمی‌گیرند. شش روش باقیمانده در مرحله دوم با پنج معیار میزان پیچیدگی، رویکرد مدل، ابزار، خاستگاه روش، و گستره استفاده جغرافیایی مورد بررسی و مقایسه قرار گرفتند و سه روش از بهترین روش‌ها برای مرحله سوم انتخاب شدند. معیارهای مرحله سوم شامل تعریف مفهومی، رویکرد ارزیابی مخاطره امنیت اطلاعات، نتایج و خروجی‌ها، و میزان پیچیدگی است. نتایج ارزیابی عملی از سه روش باقیمانده بدین صورت است که بدون درنظرگرفتن نیازهای خاص یک سازمان، «آیرَم» [3] رویکردی است که قابلیت استفاده، پیچیدگی، انعطاف‌پذیری و نتایج نهایی را بهتر تطبیق می‌دهد. «اُکتاو» [4]، باوجود ساده و سریع بودن، فقط اطلاعات ضروری را بدون جزئیات زیاد در اختیار قرار می‌دهد. از طرف دیگر «آی. تی. گرانتشتز» [5] که سطح امنیت فناوری اطلاعات سازمان را محاسبه می‌کند و توصیه‌های فنی بسیار دقیق را، اما با هزینه بسیار بالا (زمان، تخصص و منابع) ارائه می‌دهد.

«بهینا» و همکاران [۲۴] در پژوهشی به بررسی و مقایسه روش‌های مختلف تحلیل مخاطره امنیت اطلاعات پرداختند. آنها برخی از روش‌های کیفی و برخی روش‌های کمی را برای انجام مقایسه خود انتخاب کردند. چارچوب ارائه شده در آن پژوهش، موجب تسریع و تسهیل در روند انتخاب روش‌های تحلیل مخاطره می‌شود. در پژوهش آنها پنج روش کیفی تحلیل مخاطره و چهار روش کمی تحلیل مخاطره بر اساس ویژگی‌هایی مانند "زبان"، "قیمت"، "کشور مبدأ"، مورد بررسی و مقایسه قرار گرفت. بااین‌حال در مورد مزایای خاص، عملکرد، ورودی، خروجی روش‌ها مطلبی ارائه نشده است. آگراوال [۲۵] در پژوهشی به ارائه تحلیلی از چهار روش

[1] COBIT (Control Objectives for Information and Related Technologies)
[2] CRAMM, OCTAVE, CORA

[3] IRAM (Information Risk Analysis Methodologies)
[4] OCTAVE (Operationally Critical Threat, Asset, And Vulnerability Evaluation)
[5] ITGrundschutz

تجزیه‌وتحلیل مخاطره با استفاده از طبقه‌بندی کمپبل و همکاران ارائه کرده است. در این پژوهش خلاصه‌ای از چهار روش تجزیه‌وتحلیل مخاطره امنیت اطلاعات با استفاده از هستی‌شناسی ارائه شده است و همچنین این روش‌ها بر اساس ویژگی‌های عمومی مانند ورودی، خروجی، هدف، تلاش، مقیاس‌پذیری، روش‌شناسی و غیره مورد بررسی و مقایسه قرار گرفته‌اند.

باید به این نکته اشاره شود در بخش مرور پیشینه داخلی، هر چند محدود پژوهش‌هایی در خصوص معرفی و تحلیل روش‌های ارزیابی مخاطره امنیت اطلاعات به شکل موردی و تکی انجام شده است، اما پژوهشی که به طور خاص بر ارزیابی تطبیقی روش‌های ارزیابی مخاطره امنیت اطلاعات تمرکز کرده باشد، یافت نشد.

۳- روش تحقیق

به‌منظور دستیابی به هدف پژوهش که ارزیابی تطبیقی روش‌های ارزیابی مخاطره امنیت اطلاعات است، از الگوی ارائه شده توسط «وارتیاینن» [۲۶] استفاده شد. بر اساس بیان وی، ارزیابی تطبیقی باید مبتنی بر چهار گام اصلی انجام شود:

- **گام نخست - انتخاب شئ برای ارزیابی:** ابتدا باید اشیاء مورد ارزیابی و روش انتخاب آنها مشخص شود. در این مطالعه اشیاء مورد بررسی روش‌های ارزیابی مخاطره امنیت اطلاعات در سطح جهان است. به‌منظور انتخاب این روش‌ها، در گام نخست، بر اساس مطالعه کتابخانه‌ای و جستجو در اسناد مرتبط، ۴۹ سند پایه که با نام مشخص یک روش ارزیابی مخاطره امنیت اطلاعات را معرفی کرده بودند، شناسایی شدند. در گام دوم، بر پایه بررسی اولیه اسناد، ارزیابی مجددی بر اساس معیارهای امکان دسترسی در زمان بررسی، وضعیت به‌روزرسانی یا جایگزینی با نسخه به‌روز، و امکان ادغام به‌عنوان یک سری روش انجام شد و مبتنی بر آن ۱۸ روش ارزیابی انتخاب شدند.
- **گام دوم- سطح مقایسه:** قلمرو، اصول حاکم و سطح تشابه یا تفاوت اشیاء مورد ارزیابی در این مرحله مشخص می‌شود. قلمرو ارزیابی در این پژوهش محدود به مقایسه روش‌های ارزیابی مخاطره امنیت اطلاعات بر پایه یک چارچوب ارزیابی است.

اصل نخست: در این پژوهش، اصطلاح **روش** در این مطالعه، به کلیه استانداردها، چارچوب‌ها، روش‌ها، راهنماها، اصول، رهنمودهایی اشاره دارد که به‌منظور مدیریت و ارزیابی مخاطره امنیت اطلاعات منتشر شده‌اند. باتوجه‌به اینکه همه این موارد در قالب یک یا چند سند پایه منتشر شده‌اند، از اصطلاح **سند پایه** به‌جای روش در فرآیند شناسایی، دسته‌بندی و ارزیابی استفاده شده است.

اصل دوم: باتوجه‌به هدف این مطالعه، روش ارزیابی مورد انتخاب در این پژوهش، روش ارزیابی روشنگرانه است. در این روش، واحدهای ارزیابی به‌صورت غیرمستقیم و با استفاده از چارچوب پیشنهادی مطالعه، مورد مقایسه قرار می‌گیرند. کاربرد اصلی این روش نیز در استانداردسازی و بیان تعمیم کاربرد چارچوب مورداستفاده در فرآیند ارزیابی می‌باشد. در این بخش طراحی چارچوب ارزیابی و استخراج پارامترها و معیارهای آن مبتنی بر مرور پیشینه استفاده شده است. به‌منظور اعتباریابی چارچوب ارزیابی نیز از روش **یک‌سویه‌سازی پژوهشگر** استفاده شده است. مبتنی بر این روش دو پژوهشگر به‌صورت جداگانه مبتنی بر مرور پیشینه معیارها را شناسایی کرده، سپس به اشتراک گذاشته و در انتها موارد در جلسه‌ای با مشارکت یک ناظر بیرونی نهایی شده است.

- **گام سوم- درک مفهومی:** در این گام باید به‌صورت شفاف مفاهیم و اشیاء معرفی شود. بدین منظور برای هر کدام از اسناد پایه مورد ارزیابی، شناسنامه‌ای مشتمل بر پارامترهای (نام اختصاری، نام کامل، ارائه‌دهنده، کشور ارائه‌دهنده، وضعیت نسخه، زبان، قیمت، دامنه کاربرد/ استفاده، هدف، اندازه سازمان هدف، چکیده، مراحل مدیریت مخاطره، متغیرها/ عملگرهای محاسبه مخاطره، فرمول محاسبه مخاطره، سازگاری با استانداردها، سطح کاربری، سطح مهارت موردنیاز، ابزارهای پشتیبان، مزایا/ نقاط قوت، معایب/ نقاط ضعف، و آدرس وب‌سایت رسمی) برای هر کدام از ۱۸ سند پایه تدوین شد. به‌منظور اعتباریابی شناسنامه‌ها نیز از روش **یک‌سویه‌سازی پژوهشگر** استفاده شده است.
- **گام چهارم- انجام و تحلیل یافته‌های ارزیابی:** روش ارزیابی و تحلیل یافته‌های حاصل از آن در این گام مشخص می‌شود. به‌منظور انجام این ارزیابی، ابتدا کلیه اسناد پایه شناسایی شده به همراه شناسنامه تدوین شده گام سوم در اختیار چهار نفر از تصمیم‌گیرندگان این حوزه در ایرانداک قرار گرفت. معیار انتخاب این افراد، سابقه و مسئولیت در حوزه فناوری اطلاعات، آشنایی نسبی با مفاهیم مدیریت و مخاطره امنیت اطلاعات، و آشنایی کامل با حوزه‌های فعالیت ایرانداک مشخص شد. به همراه این اسناد، جدول ارزیابی اسناد پایه بر پایه چارچوب ارزیابی طراحی شده در گام دوم در اختیار افراد قرار گرفت و از آنها خواسته شده مبتنی بر معیارهای ارزیابی، به هر یک اسناد پایه به‌منظور به‌کارگیری

در ایرانداک نظر خود را اعلام کنند. پس از دریافت نظرات همه مشارکت‌کنندگان، تحلیل با استفاده از روش‌ها و ابزارهای زیر در سه زیر گام انجام شد:

۱. روش «آنتروپی شانون» [1] بر پایه پیشنهاد «پومرول» و «باربارومرو» [۲۷] در نرم‌افزار اکسل به‌منظور محاسبه وزن معیارها؛ در مقایسه با دیگر روش‌ها، از دلایل انتخاب این روش در این پژوهش می‌توان به ۱- سادگی روش، ۲- عدم نیاز به ارزیابی جداگانه باتوجه‌به تعداد بالای معیارها و گزینه‌ها، و ۳- آشنایی تیم پژوهش به این روش اشاره کرد.

۲. استفاده از ابزار افزونه «سانا» [2] برای محاسبه فاصله‌ها از ایده‌آل و ضد ایده‌آل در روش «تاپسیس» [3] به‌عنوان یکی از روش‌های تصمیم‌گیری چندمعیاره؛ از دلایل اصلی انتخاب این روش برای ارزیابی در این بخش، در کنار آشنایی کامل پژوهشگران با این روش، می‌توان به مزایایی از جمله درنظرگرفتن هر دو حال جواب‌های ایده‌آل مثبت و منفی، آسانی استفاده و قابل‌درک بودن الگوریتم آن، امکان به‌کارگیری توأم معیارهای کمی و کیفی، ارائه خروجی با مشخص‌کردن ترتیب اولویت گزینه‌ها و بیان آن‌ها به‌صورت کمی، درنظرگرفتن تضاد و تطابق بین شاخص‌ها، روش کار ساده و سرعت بالا و منطبق بودن نتایج این روش با روش‌های تجربی اشاره کرد [۲۸]. در این روش m گزینه به‌وسیله n معیار ارزیابی می‌شود. ملاک انتخاب و اولویت‌بندی گزینه‌ها در این روش حداکثر فاصله از ایده‌آل منفی و حداکثر نزدیکی به راه‌حل ایده‌آل مثبت است. جهت پیاده‌سازی و انجام روش «تاپسیس» گام‌های زیر اجرا می‌شوند:

۱) تشکیل ماتریس تصمیم: گام اولیه این روش تشکیل ماتریس تصمیم است. ماتریس تصمیم در این روش شامل یکسری معیار و گزینه است. در این ماتریس معیارها در ستون‌ها قرار می‌گیرند و گزینه‌ها در سطر هستند. هر سلول ماتریس نیز ارزیابی هر گزینه نسبت به هر معیار است. بعد از اینکه ماتریس تصمیم تشکیل شد، باید آن را توسط نظرات خبرگان تکمیل شود که با توجه به کمی یا کیفی بودن معیارها انجام می‌شود. در معیارهای کیفی این کار از طریق تخصیص طیف لیکرت به معیارها انجام می‌شود.

۲) بی مقیاس کردن ماتریس تصمیم (نرمال‌سازی ماتریس تصمیم): بی مقیاس کردن در این روش تاپسیس با استفاده از روش نرم صورت میگیرد و به اینصورت انجام می‌شود که هر درایه بر جذر مجموع مربعات درایه های آن ستون معیار تقسیم می‌شود. در این گام در واقع ماتریس تصمیم تبدیل به یک ماتریس بی بعد می‌شود.

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{k=1}^{m} x_{kj}^2}}, \quad i = 1,2,\ldots,m, \quad j = 1,2,\ldots,n$$

۳) تعیین ماتریس بی‌مقیاس وزن‌دار: در این گام باید وزن معیارها که از روش‌های دیگر بدست آمده است، را در ماتریس نرمال ضرب کنیم تا ماتریس وزن دار حاصل شود.

$$t_{ij} = r_{ij} \cdot w_j, \quad i = 1,2,\ldots,m, \quad j = 1,2,\ldots,n$$

$$w_j = W_j \Big/ \sum_{k=1}^{n} W_k, j = 1,2,\ldots,n$$

$$\sum_{i=1}^{n} w_i = 1$$

۴) یافتن حل ایده ال مثبت و ایده آل منفی: در این جا باید نوع معیارها مشخص شود معیارها یا جنبه مثبت دارند یا منفی. معیارهای مثبت معیارهایی هستند که افزایش آن ها باعث بهبود در سیستم شود مثل کیفیت یک محصول این معیار از نوع مثبت است و حل ایده آل مثبت آن برابر با بزرگترین درایه ستون معیار و ایده آل منفی برابر با کوچکترین درایه سلول. برای معیارهای منفی بالعکس.

- برای معیارهایی که بار مثبت دارند، ایده‌آل مثبت بزرگ‌ترین مقدار آن معیار است.
- برای معیارهایی که بار مثبت دارند، ایده‌آل منفی کوچک‌ترین مقدار آن معیار است.
- برای معیارهایی که بار منفی دارند، ایده‌آل مثبت کوچک‌ترین مقدار آن معیار است.
- برای معیارهایی که بار منفی دارند، ایده‌آل منفی بزرگ‌ترین مقدار آن معیار است.

$$A_w = \{\langle \max(t_{ij} \mid i = 1,2,\ldots,m) \mid j \in J_- \rangle, \langle \min(t_{ij} \mid i = 1,2,\ldots,m) \mid j \in J_+ \rangle\} \equiv \{t_{wj} \mid j = 1,2,\ldots,n\},$$

$$A_b = \{\langle \min(t_{ij} \mid i = 1,2,\ldots,m) \mid j \in J_- \rangle, \langle \max(t_{ij} \mid i = 1,2,\ldots,m) \mid j \in J_+ \rangle\} \equiv \{t_{bj} \mid j = 1,2,\ldots,n\},$$

جایی که:

$$J_+ = \{j = 1,2,\ldots,n \mid j\}$$

$$J_- = \{j = 1,2,\ldots,n \mid j\}$$

۵) محاسبه فاصله از حل ایده ال مثبت و ایده آل منفی: در این گام بر اساس رابطه زیر فاصله هر گزینه را از ایده آل مثبت و منفی‌اش محاسبه می‌شود.

$$d_{iw} = \sqrt{\sum_{j=1}^{n} (t_{ij} - t_{wj})^2}, \quad i = 1,2,\ldots,m,$$

$$d_{ib} = \sqrt{\sum_{j=1}^{n} (t_{ij} - t_{bj})^2}, \quad i = 1,2,\ldots,m$$

[1] Shannon Entropy
[2] Sanna (https://nb.vse.cz/~jablon/sanna.htm)
[3] Topsis

۶) محاسبه شاخص شباهت و رتبه‌بندی گزینه‌ها: شاخص شباهت نشان دهنده امتیاز هر گزینه است و بر اساس رابطه زیر محاسبه می‌شود هرچقدر این شاخص به عدد یک نزدیکتر باشد نشان از برتری آن گزینه می دهد.

$$s_{iw} = d_{iw}/(d_{iw} + d_{ib}),$$

$$0 \le s_{iw} \le 1, \quad i = 1, 2, \ldots, m.$$

۷) رتبه بندی گزینه ها بر اساس شاخص شباهت: در این مرحله گزینه های مورد بررسی به ترتیب نزولی شاخص شباهت مرتب می‌شوند.

۳. استفاده از میانگین هندسی فاصله‌ها به‌منظور محاسبه شاخص شباهت در تصمیم‌گیری گروهی بر اساس روش «تاپسیس گروهی» ارائه شده توسط «شیه»، «شیور» و «لی» [۲۸]. از مزیت‌های این راهکار می‌توان به مبنای محاسباتی مستدل و دقیق، استفاده از راهکار کمی به‌جای کیفی در تصمیم‌گیری گروهی و امکان استقلال اعضای گروه در ارزیابی و جلوگیری از اثر هاله‌ای اشاره کرد.

۴- تجزیه و تحلیل یافته‌ها

در این بخش یافته‌های پژوهش بر اساس گام‌های اشاره شده در بخش قبل ارائه خواهد شد.

۴-۱. فهرست اسناد پایه

بر پایه گام نخست، فهرست ۱۸ سند پایه ارزیابی مخاطره امنیت اطلاعات به شرح جدول (۱) بدست آمد.

جدول (۱). فهرست اسناد پایه ارزیابی مخاطره امنیت اطلاعات

کد	نام کامل سند پایه		مخفف	گونه سند		
				استاندارد	راهنما/ دستورالعمل	روش/ مدل
D۱	ISO/IEC 27005	ISO/IEC 27000	ISO 27005	✓	✓	
D۲	ISO/IEC 31000	ISO/IEC 31000	ISO 31000	✓	✓	
	ISO/IEC 31010		ISO 31010			
D۳	NIST SP800-30	NIST SP 800	NIST SP800-30	✓	✓	
	NIST SP800-37		NIST SP800-37			
	NIST SP800-39		NIST SP800-39			
D۴	BSI STANDARD 200-3	BSI Series	BSI 200-3	✓		
	IT-GRUNDSCHUTZ		IT-GRUNDSCHUTZ			
D۵	The European Telecommunication Standards Institute Threat Vulnerability and Risk Analysis (TVRA) Method		ETSI TVRA	✓		✓
D۶	Austrian IT Security Handbook		Austrian IT Security Handbook		✓	
D۷	Risk Analysis and Management Methodology for Information Systems		MAGERIT		✓	✓
D۸	Microsoft's Security Risk Management Guide		Microsoft's Security Risk Management Guide		✓	
D۹	Control Objectives for Information and Related Technology for Risk		COBIT-5 for Risk		✓	
D۱۰	RISK IT		RISK IT		✓	✓
D۱۱	Consultative Objective Risk Analysis System		CORAS			✓
D۱۲	CCTA Risk Analysis and Management Method		CRAMM			✓
D۱۳	Expression des Besoins et Identification des Objectifs de Sécurité		EBIOS			✓
D۱۴	Factor Analysis of Information Risk		FAIR			✓
D۱۵	Facilitated Risk Analysis and Assessment Process		FRAAP			✓
D۱۶	Method for Harmonized Analysis of Risk		MEHARI			✓
D۱۷	Operationally Critical Threat, Asset, And Vulnerability Evaluation		OCTAVE			✓
D۱۸	Information Risk Analysis Methodologies		IRAM/ IRAM2			✓

همان‌طور که در این جدول مشخص است، هر یک از اسناد پایه مدیریت و ارزیابی مخاطره نشان‌دهنده یک یا ترکیبی از سه گونه به شرح زیر هستند:

- استاندارد: مجموعه‌ای از قوانین شناخته‌شده که چگونگی توسعه و مدیریت مواد، محصولات، خدمات، فناوری‌ها، وظایف، فرآیندها و سیستم‌ها توسط افراد را کنترل می‌کند.
- راهنما/ دستورالعمل: توصیه یا دستورالعمل داده شده به‌منظور هدایت یا راهنمایی یک عملیات است.
- روش/ مدل، به‌عنوان یک ترتیب منظم و نظام‌مند از مراحل انجام کار برای رسیدن به نقطه پایان تعریف می‌شود و الگوهایی هستند برای نمایش کنترل شده یک پدیده واقعی و با ساختار تعریف شده (شناسایی، تحلیل، ارزیابی) که در زیرمجموعه روش‌شناسی یک طرح قابل‌استفاده می‌باشند تا از طریق آنها نتایج نزدیک‌تر به واقعیت قابل‌استنباط باشند.

۴-۲. چارچوب ارزیابی

بر پایه گام دوم، چارچوب ارزیابی شامل ۱۳ معیار ارزیابی به شرح جدول (۲) حاصل شد. در تمامی این معیارها، جز معیار نخست، سنجش بر اساس طیف لیکرت پنج تایی شامل (۱- بسیارکم، ۲- کم، ۳- متوسط، ۴- زیاد، ۵- بسیار زیاد) انجام می‌شود.

جدول (۲). چارچوب ارزیابی اسناد پایه ارزیابی مخاطره امنیت اطلاعات

کد	عنوان معیار	تعریف/ نحوه اندازه‌گیری		منبع	طیف‌سنجش
A1	انطباق اندازه سازمان هدف	اندازه سازمان هدف در هر کدام از اسناد پایه در سه سطح ۱- سازمان بزرگ، ۲- سازمان متوسط، و ۳- سازمان کوچک، و یا ترکیبی از آنها دسته بندی شده‌اند. میزان انطباق اندازه سازمان مدنظر با اندازه سازمان هدف سند پایه مورد بررسی در این معیار سنجش می‌شود.	اندازه ایرانداک، به‌عنوان سازمان متوسط در نظر گرفته شده است.	[۱۷]، [۲۹]	(۰) انطباق ندارد، (۱) انطباق دارد.
A2	انطباق سطح کاربری	نوع کاربری روش بر پایهٔ یک یا ترکیبی از حالت‌های (مدیریتی، فنی، عملیاتی) است. میزان انطباق سطح کاربری مدنظر سازمان با سطح کاربری سند پایه مورد بررسی در این معیار سنجش می‌شود.	سطح کاربری مدنظر ایرانداک، ترکیبی از عملیاتی و فنی در نظر گرفته شده است.	[۱۷]، [۳۰- ۳۱]	(۱) بسیارکم، (۲) کم، (۳) متوسط، (۴) زیاد، (۵) بسیار زیاد
A3	انطباق سطح مهارت موردنیاز	سطح تخصص/ مهارت موردنیاز برای انجام هر یک از اسناد پایه در سه سطح تخصص بالا (متخصص)، تخصص متوسط (استاندارد)، تخصص کم (پایه) و یا ترکیبی از آنها دسته‌بندی شده است. میزان انطباق سطح مهارت موجود در سازمان با سطح مهارت موردنیاز در هر کدام از اسناد پایه در این معیار مشخص می‌شود.	سطوح مهارت در ایرانداک، متوسط و کم در نظر گرفته شده است.	[۱۷]، [۲۴ -۲۵]، [۳۰- ۳۲]	
A4	پشتیبانی از مراحل مدیریت مخاطره	مدیریت مخاطره شامل ۶ مرحله اصلی پایه‌گذاری محتوا، ارزیابی مخاطره، مقابله با مخاطره، پذیرش مخاطره، ارتباطات مخاطره، پایش و بازبینی مخاطره است. اینکه در یک سند پایه به چه میزان این شش مرحله پوشش داده شده است در این معیار مشخص می شود.		[۲۳]، [۲۵]، [۳۰]، [۳۲- ۳۵]	
A5	پشتیبانی از مراحل ارزیابی مخاطره	ارزیابی مخاطره به‌عنوان یکی از مراحل اصلی مدیریت مخاطره شامل سه مرحله شناسایی مخاطره، تحلیل مخاطره، سنجش مخاطره است. اینکه در یک سند پایه به چه میزان این سه مرحله پوشش داده شده است در این معیار مشخص می‌شود.		[۱۷]، [۲۳]، [۲۹]، [۳۱- ۳۲]، [۳۵- ۳۶]	
A6	تنوع شیوه ارزیابی مخاطره	تعیین‌کننده روش ارزیابی بر پایهٔ یک یا ترکیبی از حالت‌های (خودارزیابی، مصاحبه و یا کارگاه آموزشی) است.		[۲۳]، [۳۲]، [۳۷]	
A7	سطح پشتیبانی از زبان فارسی و زبان‌های رایج	تعیین‌کننده تنوع زبان‌هایی است که سند پایه از آنها پشتیبانی می‌کند. در این معیار سطح پشتیبانی از زبان فارسی در مرحله نخست و دیگر زبان‌های رایج در مرحله دوم مدنظر می‌باشد.		[۱۷]، [۲۴ -۲۵]، [۳۱]	
A8	میزان سازگاری با استانداردها و مستندات پایه	میزان تطابق با قوانین، مقررات، استانداردها، دستورالعمل‌ها و غیره را نشان می‌دهد.		[۱۷]، [۲۴]، [۳۱] ، [۳۸- ۴۰]	
A9	پوشش تعاریف و اصطلاحات	تعیین‌کننده میزان پوشش‌دهی تعاریف و اصطلاحات مورداستفاده در روش است به‌طوری‌که کاربر بدون نیاز به دانستن اصطلاحات خاص بتواند از آن استفاده کند.		[۲۳]، [۳۴]، [۳۹- ۴۰]	
A10	سرعت	زمان در نظر گرفته شده جهت انجام فرآیند تحلیل و ارزیابی مخاطره را نشان می‌دهد.		[۱۷]، [۲۳]، [۳۱- ۳۲]، [۳۴]، [۴۰- ۴۱]،	
A11	سهولت استفاده	میزان سادگی، آسانی و راحتی درک و استفاده را نشان می‌دهد.			
A12	فرآیند روشن و شفاف مراحل	میزان شفافیت مراحل و چگونگی اجرای هر مرحله را نشان می‌دهد.			
A13	تکرارپذیری	میزان قابلیت تکرارپذیری و مقایسه نتایج ارزیابی با دیگر روش‌ها (اسناد پایه) را نشان می‌دهد.			

همان‌طور که در این جدول مشخص است، معیارها به دودسته تقسیم شده‌اند. دسته نخست میزان انطباق سند پایه را با وضعیت موجود در سازمان موردنظر را بررسی می‌کند (معیارهای ۱ تا ۳)، و دسته دوم بر روی سند پایه و ویژگی‌های آن متمرکز است. در معیار۱ (انطباق اندازه سازمان هدف)، بر پایهٔ تعریف بانک مرکزی، واحدهایی که تعداد کارکنان آن کمتر از ۵۰ نفر باشد صنایع کوچک، با ۵۰ نفر تا ۲۵۰ نفر کارمند، صنایع متوسط و بیش از آن صنایع بزرگ نامیده می‌شوند [۴۲]. بر پایه معیار۲ (انطباق سطح کاربری)، هر یک از اسناد پایه ارزیابی مخاطره بر پایهٔ یک و یا ترکیبی از سطوح مدیریتی، عملیاتی و فنی تدوین شده است.

- سطح مدیریتی: دستورالعمل‌ها/ رهنمودهای عمومی را در اختیار قرار می‌دهد.
- سطح عملیاتی: دستورالعمل‌ها/ رهنمودهایی را برای برنامه‌ریزی و پیاده‌سازی با جزئیات کم ارائه می‌دهد.
- سطح فنی: دستورالعمل‌ها/ رهنمودهای خاص مربوط به جنبه‌های فنی، سازمانی، فیزیکی و انسانی امنیت فناوری اطلاعات را با جزئیات زیاد ارائه می‌دهد.

در معیار۳ (انطباق سطح مهارت موردنیاز) سه گونه مهارت در اسناد پایه مدیریت و ارزیابی مخاطره در نظر گرفته شده‌اند که عبارت‌اند از:

- معرفی: به مهارت‌های موردنیاز جهت درک وابستگی بین جزئیات خاص از محصول اشاره دارد. برای نمونه، مفاهیم گوناگون پشتیبانی شده، مراحل، فعالیت‌ها، و غیره.
- استفاده: به تخصص‌ها و مهارت‌های خاصی اشاره می‌کند که جهت انجام کارهای جاری نیاز است. برای نمونه، اسناد قابل‌فهم و کاربری آسان.
- نگهداری: به تخصص‌ها و مهارت‌های خاصی جهت حفظ و نگهداری چرخه عمر محصول اشاره می‌کند. برای نمونه، سفارشی‌سازی، متناسب‌سازی یا انجام منظم به‌روزرسانی‌ها.

در این معیار برای این‌گونه‌ها، سطح مهارت‌ها بر پایهٔ مقیاس زیر دسته‌بندی شده است:

- تخصص کم (پایه): بیانگر تجربه و حس مشترک است.
- تخصص متوسط (استاندارد): بیانگر این است که چند روز یا هفته برای آموزش کافی و مناسب است.
- تخصص بالا (متخصص): بیانگر تجربه و دانش کامل موردنیاز است.

۴-۳. نتایج ارزیابی

در گام سوم، ابتدا بر پایه روش «آنتروپی شانون» وزن هر کدام از معیارها توسط نفرات مشارکت‌کننده به شرح جدول (۳) بدست آمد.

جدول (۳): وزن معیارها بر اساس روش آنتروپی شانون توسط مشارکت‌کنندگان

کد معیار	وزن معیارها به تفکیک نفرات				میانگین حسابی
	۱	۲	۳	۴	
A1	۰/۰۲۰۵	۰/۰۵۴۶	۰/۰۴۵۳	۰/۰۲۱۹	۰/۰۳۵۶
A2	۰/۰۲۳۱	۰/۰۲۹۸	۰/۰۳۴۹	۰/۰۳۶۵	۰/۰۳۱۱
A3	۰/۰۳۹۱	۰/۰۵۷۴	۰/۰۵۶۰	۰/۰۴۶۷	۰/۰۴۹۸
A4	۰/۱۴۰۷	۰/۰۷۶۰	۰/۱۲۴۳	۰/۰۹۸۱	۰/۱۰۹۸
A5	۰/۰۱۱۸	۰/۰۳۹۹	۰/۰۰۹۵	۰/۰۱۲۶	۰/۰۱۸۵
A6	۰/۱۱۰۵	۰/۱۲۶	۰/۱۱۰۶	۰/۱۴۵۱	۰/۱۲۳۱
A7	۰/۲۲۹۷	۰/۱۹۷۰	۰/۲۰۰۳	۰/۲۱۶۶	۰/۲۱۰۹
A8	۰/۰۷۵۴	۰/۰۶۰۰	۰/۰۷۰۳	۰/۱۱۷۵	۰/۰۸۰۸
A9	۰/۰۷۶۴	۰/۰۴۰۹	۰/۰۲۷۴	۰/۰۴۳۸	۰/۰۴۷۱
A10	۰/۰۹۵۸	۰/۰۸۶۷	۰/۰۶۶۱	۰/۰۸۱۳	۰/۰۸۲۵
A11	۰/۰۷۵۰	۰/۱۱۷۲	۰/۱۱۴۸	۰/۰۵۷۵	۰/۰۹۱۱
A12	۰/۰۲۴۸	۰/۰۸۴۴	۰/۰۷۵۵	۰/۰۷۴۹	۰/۰۶۴۹
A13	۰/۰۷۷۱	۰/۰۳۰۰	۰/۰۶۵۱	۰/۰۴۷۵	۰/۰۵۴۹

بر مبنای میانگین حسابی وزن‌ها، مشاهده می‌شود که سه معیار A7 (سطح پشتیبانی از زبان فارسی و زبان‌های رایج)، A6 (تنوع شیوه ارزیابی مخاطره)، و A4 (پشتیبانی از مراحل مدیریت مخاطره) بالاترین وزن را ب خود اختصاص دادند. این رامی توان نشان از اهمیت مراحل مدیریت مخاطره و تنوع شیوه‌های ارزیابی آن و همچنین اهمیت قابلیت خوانش بومی به‌عنوان معیارهای اصلی ارزیابی برداشت کرد.

در گام دوم، بر پایه روش «تاپسیس»، مقادیر فاصله‌ها از ایده‌آل مثبت(d+) و ایده‌آل منفی(d-) به تفکیک اسناد پایه برای نظرات هر کدام از نفرات محاسبه شد. در گام سوم، بر پایه این روش، پس از به‌دست‌آمدن این فواصل از طریق میانگین هندسی، شاخص شباهت و اولویت‌بندی اسناد پایه نیز محاسبه شد. نتایج این تحلیل در جدول (۴) قابل‌مشاهده است.

جدول (۴). مقادیر فواصل ایده‌آل مثبت و منفی، میانگین هندسی، شاخص شباهت و اولویت اسناد پایه بر اساس روش «تاپسیس گروهی»

کد سند پایه	نوع فاصله	مقادیر فاصله به تفکیک نفرات				میانگین هندسی فاصله‌ها	شاخص شباهت Ci	اولویت
		۱	۲	۳	۴			
D1	d_+	۰/۰۱۷۴	۰/۰۱۶۶	۰/۰۱۷۶	۰/۰۱۹۳	۰/۰۱۷۷	۰/۸۲۸۵	۱
	d_-	۰/۰۸۹۴	۰/۰۷۸۶	۰/۰۹۰۲	۰/۰۸۴۲	۰/۰۸۵۵		
D2	d_+	۰/۰۱۹۸	۰/۰۲۳	۰/۰۲۴۱	۰/۰۳۳۲	۰/۰۲۴۶	۰/۷۵۷۹	۲

کد سند پایه	نوع فاصله	مقادیر فاصله به تفکیک نفرات				میانگین هندسی فاصله‌ها	شاخص شباهت Ci	اولویت
		۱	۲	۳	۴			
	-d	۰/۰۸۶	۰/۰۷۱	۰/۰۸۷۱	۰/۰۶۵۸	۰/۰۷۶۹		
D3	+d	۰/۰۷۴۸	۰/۰۵۷۶	۰/۰۷۴۸	۰/۰۶۸۲	۰/۰۶۸۵	۰/۴۱۷۷	۸
	-d	۰/۰۴۳	۰/۰۵۰۷	۰/۰۵۱۴	۰/۰۵۲	۰/۰۴۹۱		
D4	+d	۰/۰۶۸۱	۰/۰۵۲۴	۰/۰۷۲	۰/۰۷۰۷	۰/۰۶۵۳	۰/۳۵۳۲	۱۱
	-d	۰/۰۳۳	۰/۰۴۴۶	۰/۰۳۴	۰/۰۳۲۳	۰/۰۳۵۷		
D5	+d	۰/۰۸۶۲	۰/۰۷۸۱	۰/۰۸۷۱	۰/۰۸۲۷	۰/۰۸۳۴	۰/۱۹۷۷	۱۸
	-d	۰/۰۲۳۱	۰/۰۱۵۲	۰/۰۲۲۹	۰/۰۲۲۲	۰/۰۲۰۶		
D6	+d	۰/۰۸۲۵	۰/۰۷۷۴	۰/۰۸۵۶	۰/۰۸۱	۰/۰۸۱۶	۰/۲۴۳۹	۱۶
	-d	۰/۰۲۸	۰/۰۲۱۸	۰/۰۲۸	۰/۰۲۷۹	۰/۰۲۶۳		
D7	+d	۰/۰۳۱۸	۰/۰۲۴۷	۰/۰۴۰۷	۰/۰۴۰۸	۰/۰۳۳۸	۰/۶۸۰۱	۳
	-d	۰/۰۸۴۱	۰/۰۷۴۱	۰/۰۶۶۵	۰/۰۶۴۴	۰/۰۷۱۹		
D8	+d	۰/۰۷۹۴	۰/۰۶۷۷	۰/۰۸۱۳	۰/۰۷۵۵	۰/۰۷۵۸	۰/۳۰۸۰	۱۳
	-d	۰/۰۳۸۴	۰/۰۳۱۴	۰/۰۳۲۴	۰/۰۳۳۱	۰/۰۳۳۷		
D9	+d	۰/۰۸۲۲	۰/۰۶۲۸	۰/۰۸۵۷	۰/۰۸۰۶	۰/۰۷۷۳	۰/۲۷۳۴	۱۵
	-d	۰/۰۳۱	۰/۰۳۰۵	۰/۰۲۷۴	۰/۰۲۷۶	۰/۰۲۹۱		
D10	+d	۰/۰۸۳	۰/۰۶۶۳	۰/۰۸۳۶	۰/۰۷۹	۰/۰۷۷۶	۰/۳۰۱۰	۱۴
	-d	۰/۰۳۴۲	۰/۰۳۶۸	۰/۰۳۲۱	۰/۰۳۰۹	۰/۰۳۳۴		
D11	+d	۰/۰۴۴۸	۰/۰۴۳۶	۰/۰۵	۰/۰۵۰۳	۰/۰۴۷۱	۰/۵۸۲۶	۶
	-d	۰/۰۸۱۶	۰/۰۶۴۲	۰/۰۶۰۷	۰/۰۵۸۵	۰/۰۶۵۷		
D12	+d	۰/۰۶۱۳	۰/۰۴۹۱	۰/۰۵۵	۰/۰۵۵۹	۰/۰۵۵۲	۰/۴۸۹۵	۷
	-d	۰/۰۴۹۵	۰/۰۶۳۷	۰/۰۵۱۹	۰/۰۴۷۸	۰/۰۵۲۹		
D13	+d	۰/۰۳۹۲	۰/۰۴۳۳	۰/۰۳۷۶	۰/۰۴۵۷	۰/۰۴۱۳	۰/۶۱۱۵	۵
	-d	۰/۰۶۸۷	۰/۰۵۱۱	۰/۰۸۴۲	۰/۰۶۰۶	۰/۰۶۵		
D14	+d	۰/۰۸۷۳	۰/۰۷۵۸	۰/۰۹۱۹	۰/۰۷۲۹	۰/۰۸۱۶	۰/۲۱۰۰	۱۷
	-d	۰/۰۲۵۱	۰/۰۲۰۶	۰/۰۱۵۸	۰/۰۲۷	۰/۰۲۱۷		
D15	+d	۰/۰۷۵۹	۰/۰۶۳	۰/۰۷۸۹	۰/۰۷۳۵	۰/۰۷۲۶	۰/۴۰۱۲	۱۰
	-d	۰/۰۴۸۷	۰/۰۵۱۱	۰/۰۴۷۵	۰/۰۴۷۲	۰/۰۴۸۶		
D16	+d	۰/۰۲۶۱	۰/۰۲۸	۰/۰۶۳۶	۰/۰۴۳۶	۰/۰۳۷۷	۰/۶۲۲۵	۴
	-d	۰/۰۷۸۵	۰/۰۶۳۹	۰/۰۴۷۳	۰/۰۶۳۱	۰/۰۶۲۲		
D17	+d	۰/۰۷۳۵	۰/۰۵۷۷	۰/۰۷۷۶	۰/۰۷۱۵	۰/۰۶۹۶	۰/۴۰۸۴	۹
	-d	۰/۰۵۱۸	۰/۰۵۱۹	۰/۰۴۴۷	۰/۰۴۴۴	۰/۰۴۸۱		
D18	+d	۰/۰۸۱۵	۰/۰۶۱۶	۰/۰۸۱۵	۰/۰۷۶۱	۰/۰۷۴۷	۰/۳۴۷۳	۱۲
	-d	۰/۰۳۴۶	۰/۰۴۴۶	۰/۰۴۰۴	۰/۰۴۰۱	۰/۰۳۹۷		

بر پایه این تحلیل‌ها، در نهایت فهرست اولویت‌بندی شده اسناد پایه ارزیابی مخاطره امنیت اطلاعات بـه شـرح جـدول (۵) بدسـت آمد. همـانطور کـه در ایـن جـدول مشـخص اسـت، ایـزو ۲۷۰۰۵ بالاترین اولویت را به منظور بکارگیری در ایرانـداک بدسـت آورد، و ایزو ۳۱۰۰۰ و «ماگریت» در رتبه‌های بعدی قرار گرفتند.

جدول (۵). اولویت نهایی اسناد پایه ارزیابی مخاطره امنیت اطلاعات

اولویت	کد سند پایه	نام سند پایه	شاخص شباهت
۱	D1	ISO 27005	۰.۸۲۸۵
۲	D2	ISO 31000	۰.۷۵۷۹
۳	D7	MAGERIT	۰.۶۸۰۱
۴	D16	MEHARI	۰.۶۲۲۵
۵	D13	EBIOUS	۰.۶۱۱۵
۶	D11	CORAS	۰.۵۸۲۶
۷	D12	CRAMM	۰.۴۸۹۵
۸	D3	NIST 800-30	۰.۴۱۷۷
۹	D17	OCTAVE	۰/۴۰۸۴
۱۰	D15	FRAAP	۰/۴۰۱۲
۱۱	D4	BSI Standard 200-3	۰/۳۵۳۲
۱۲	D18	IRAM	۰/۳۴۷۳
۱۳	D8	Microsoft	۰/۳۰۸۰
۱۴	D10	Risk IT	۰/۳۰۱۰
۱۵	D9	COBIT-5 for Risk	۰/۲۷۳۴
۱۶	D6	Austrian IT	۰/۲۴۳۹
۱۷	D14	FAIR	۰/۲۱۰۰
۱۸	D5	TVRA	۰/۱۹۷۷

۵- بحث و نتیجه‌گیری

امنیت اطلاعات همانند گذشته اهمیت دارد، اما چالش‌های تعیین عوامل مؤثر در عدم امنیت اطلاعات ماهیت پیچیده‌ای دارد. برای دسـتیابی بـه سـطح مطلـوبی از محافظـت در برابـر تهدیـدها و فراهم‌کردن سازوکارهای لازم جهت محافظت از دارایی‌ها و دانش سازمان، طیف گسترده‌ای از رویکردهـا و روش‌هـای مـدیریتی در دهه‌های گذشته توسعه‌یافته است. در حالت کلی مدیریت امنیـت اطلاعات بـر دو محـور ۱) مـدیریت دارایـی‌هـای اطلاعـاتی و ۲) مـدیریت مخـاطرات امنیـت اطلاعـات اسـتوار اسـت. مـدیریت مخاطرت امنیت اطلاعات به شکل ویژه می‌تواند بخشی از فرآینـد مدیریت مخاطره سازمانی باشد و یا به‌صورت جداگانه اجرا شـود. فعالیت‌های مـدیریت مخـاطره امنیـت اطلاعـات معمـولاً شـامل پایه‌گذاری محتوا، ارزیابی مخاطره، مقابلـه بـا مخـاطره، پـذیرش مخاطره، ارتباطات مخاطره، پایش و بازبینی مخاطره است. ارزیابی مخاطره به‌عنوان یکی از مراحل اصلی مدیریت مخاطره شامل سه مرحله شناسایی، تحلیل، و سنجش مخاطره است.

همان‌طور که اشاره شـد روش‌هـای متعـددی بـرای ارزیـابی مخاطره امنیت اطلاعات پدیدآمده است و پرسش اصلی آنست که یک سازمان برای انجام این ارزیابی، چگونه باید بین این روش‌هـا انتخاب کند. بدین منظور در ایـن پـژوهش، سـعی شـد بـا ارائـه چـارچوبی شـامل ۱۳ معیـار ارزیـابی، امکـان ارزیـابی تطبیقـی روش‌های مختلف ارزیابی مخـاطره امنیـت اطلاعـات بـرای یـک سازمان فراهم شود. در گام بعـدی ایـن چـارچوب بـرای ارزیـابی تطبیقی ۱۸ روش شناسایی شده، به‌منظور انتخاب بهتـرین روش برای به‌کارگیری در یک مورد (پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)) مورداستفاده قرار گرفت. نتایج این ارزیابی نشان داد که این چارچوب می‌تواند به‌خـوبی بـرای ارزیـابی روش‌هـای ارزیابی مخاطره امنیت اطلاعات مورداستفاده قرار گیرد.

معیارهای ارزیابی در چارچوب ارائـه شـده دودسـته هسـتند. دسته اول میزان انطباق روش را با وضعیت موجود سازمان نشـان می‌دهند و دسته دوم بر روی خود روش و ویژگی‌های آن متمرکز است. این رویکرد دوبخشی بامطالعه «بِرَدی» [۳۷] سازگار اسـت. وی بیان می‌کند برای اینکه یک سازمان روشـی را بـرای ارزیـابی مخاطره امنیت اطلاعات انتخاب کند، سازمان باید هم وضـعیت و هدف سازمان و هم ماهیت روش را مدنظر داشته باشد. در همین راستا «چاندرینوس» [۲۹] بیان می‌کند مناسب‌ترین چارچوب به زمینه و الزامات منحصربه‌فرد سازمان بستگی دارد. مهم است کـه نقاط قوت و ضعف هر چارچوب هم بر اساس ماهیت روش و هـم در ارتباط با نیازها و اهداف سازمان ارزیابی شود و یکی را انتخاب شود که بهترین تناسب را برای برنامه مدیریت مخاطره آن فراهم کند. همچنین یافته‌هـای «دِوی» و همکـارانش [۴۳] نشـان داده است که بهترین چارچوب واحدی وجود ندارد، زیرا بایـد بهتـرین چارچوب مطابق با وضعیت و اهداف سازمانی انتخاب شود.

همان‌طور که نتایج به‌کارگیری چارچوب در ایرانـداک نشـان داد، استاندارد ایزو ۲۷۰۰۵ بالاترین اولویت و منطبـق‌تـرین روش به منظور بکارگیری به منظور ارزیابی مخاطره امنیت اطلاعات در ایرانداک شناخته شد. در انطباق با این نتایج، «جونیر» و «آریما» [۴۴] بر اساس نتـایج مطالعـه خـود بیـان مـی‌کننـد هـم‌اکنـون سازمان‌ها به شکل فزاینده، با انگیزه‌های عملکردی و نهـادی و بـا هدف بهبـود فرآینـدهای مـرتبط بـا مـدیریت امنیـت اطلاعـات، مدیریت مخاطره، ارزیابی مخاطره، بهبود مدیریت امنیت اطلاعات و رعایـت قـوانین، مقـررات و ذینفعـان بـه دنبـال پـذیرش ایـن استاندارد در مقایسه با چارچوب‌ها، استانداردها و روش‌های دیگر هستند. این استاندارد که سند آن اکنون در ویرایش چهارم خـود با نام «ایزو- آی.ای.سـی. ۲۷۰۰۵: ۲۰۲۲»[1] منتشـر شـده اسـت، برای همه سازمان ها صرف نظر از صنعت، اندازه یا نوع آنها قابـل استفاده است. ایـن اسـتاندارد توسـط دسـته‌بنـدی گسـترده و

[1] ISO/IEC 27005:2022

* رایانامه نویسنده مسئول: khedmatgozar@irandoc.ac.ir

استاندارد شده پشتیبانی شده و مدل مفهومی و چارچوب مدیریت مخاطره آن با استاندارد سری ایزو ۳۱۰۰۰ و ایزو ۱۳۳۳۵ سازگاری دارد. فرآیند مدیریت مخاطره در این استاندارد شامل مراحل پایه‌گذاری زمینه، ارزیابی مخاطره (شناسایی مخاطره، تحلیل مخاطره، سنجش مخاطره)، برطرف‌سازی مخاطره، پذیرش مخاطره، ارتباطات مخاطره و مشاوره و در نهایت پایش و بازنگری مخاطره است. اصلی‌ترین مزیت این استاندارد رویکرد ساختاریافته و فرآیندگرا آن است که مدیریت مخاطره امنیت اطلاعات موثر و کارآمد را تسهیل می‌کند. با این حال، پیاده‌سازی آن می‌تواند گران باشد و از نظر زمان و منابع سرمایه‌گذاری قابل توجهی را می‌طلبد [۳۶].

«فنز» و همکارانش [۴۵] بیان می‌کنند در فرآیند مدیریت مخاطره امنیت اطلاعات چالش‌های گوناگونی از جمله ۱- فهرست سیاهه دارایی و اقدامات متقابل، ۲- تخصیص ارزش دارایی، ۳- پیش‌بینی‌های شکست‌خورده از مخاطره، ۴- اثر اطمینان بیش از حد، ۵- اشتراک دانش، و ۶- مخاطره در مقابل هزینه‌های تجاری وجود دارد. اینکه هر کدام از روش‌های ارزیابی مخاطره امنیت اطلاعات چه راهکارهایی برای کاهش این چالش‌ها ارائه می‌دهند، می‌تواند زمینه انجام یک ارزیابی تطبیقی عمیق‌تر در پژوهش‌های آینده باشد.

«کوزا» [۴۱] مبتنی بر نتایج پژوهش خود بیان می‌کند ارزیابی مخاطره‌ها یک چالش حیاتی است و انبوهی از روش‌ها، استانداردها و چارچوب‌ها را می‌توان برای مقابله با این کار مورداستفاده قرارداد. بااین‌حال، برای دستیابی به نتایج موفقیت‌آمیز در مدیریت واکنش به حادثه، استفاده از روش‌های دقیق تئوری و فنی کافی نیست. برای دستیابی به نتایج مطلوب، نحوه اجرای یک روش، چارچوب یا استاندارد در عمل بسیار مهم است [۴۶]. مبتنی بر این، پیشنهاد می‌شود پژوهشگران در آینده مبتنی بر فنون نزدیک‌تر به عمل نسبت به ارزیابی تطبیقی، مانند شبیه‌سازی یا نمونه‌سازی، میزان کارایی و اعتبار روش‌های مورد ارزیابی در این پژوهش را مورد مقایسه قرار دهند.

از سوی دیگر چارچوب پیشنهادی در این پژوهش در یک مورد سازمانی در حوزه فناوری اطلاعات مورداستفاده قرار گرفته است. استفاده از آن در دیگر بافت‌های کاربردی و همچنین توسعه آن از نظر معیارهای مورداستفاده و روش ارزیابی می‌تواند در آینده مورد توجه پژوهشگران این حوزه قرار گیرد.

۶- مراجع

[1] S. Nodeh Farahani, H. Jabari, and H. Panahian, "Proposing a conceptual model of components and indicators of human capital affecting the information security of organizations," protectiv & security researches, vol. 9, pp. 147-170, 2020. (in Persian). DOR: 20.1001.1.26455129.1399.9.35.6.7

[2] N. Feng, H. J. Wang, and M. Li, "A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis," INFORM SCIENCES, vol. 256, pp. 57-73, 2014. doi: 10.1016/j.ins.2013.02.036

[3] Committee on National Security Systems (CNSS), "Committee on National Security Systems (CNSS) Glossary," https://www.niap-ccevs.org/Ref/CNSSI_4009.pdf, 2022.

[4] M. Malekalkalami, "Evaluating the performance of information security management at the central libraries of public universities in Tehran, according to the international standard-ISO/IEC", Journal of Information Processing and Management, vol. 28, No.4, pp. 895-916, 2013. (in Persian) doi: 10.35050/JIPM010.2013.016

[5] S. Kwon, S. Jang, J. Lee, and S. Kim, "Common defects in information security management system of Korean companies," J SYST SOFTWARE, vol. 80, no. 10, pp. 1631-1638, 2007. doi: 10.1016/j.jss.2007.01.015

[6] B. Von Solms, "Information security–the fourth wave," Computers & security, vol. 25, no. 3, pp. 165-168, 2006.

[7] J. F. Van Niekerk, and R. Von Solms, "Information security culture: A management perspective," COMPUT SECUR, vol. 29, no. 4, pp. 476-486, 2010. doi: 0.1016/j.cose.2006.03.004

[8] B. Von Solms, "Information security—the third wave?," COMPUT SECUR, vol. 19, no. 7, pp. 615-620, 2000. doi: 10.1016/S0167-4048(00)07021-8

[9] M. Ostrowska, and S. Mazur, "Risk in a crisis situation," PROC ECON FINANC, vol. 23, no. 10, pp. 615-621, 2015. doi: 10.1016/S2212-5671(15)00373-1

[10] K.S. Chin, D.W. Tang, J.B. Yang, S. Y. Wong, and H. Wang, "Assessing new product development project risk by Bayesian network with a systematic probability generation methodology," EXPERT SYST APPL, vol. 36, pp. 9879-9890, 2009. doi: 10.1016/j.eswa.2009.02.019

[11] J. S. Broderick, "ISMS, security standards and security regulations," information security technical report, vol. 11, pp. 26-31, 2006.

[12] H. Bateni and P. Saeidi, "The effect of information quality integrity on information security risk management," Information Technology Innovation and Applied Communications, vol. 0, pp. 23-35, 2019. (in Persian).

[13] ISO (International Organization for Standardization), "ISO/IEC 27001 Information security management systems: Requirements," https://www.iso.org/standard/27001., 2022.

[14] S. A. Malik and B. Holt, "Factors that affect the adoption of Enterprise Risk Management (ERM)," OR Insight, vol. 26, pp. 253-269, 2013. doi: 10.1057/ori.2013.7

[15] S.A Charsoughi, M.A. Doustari, A. Yazdian Varjani, S.A. Mahdavi Ardestani, "Artificial Neural Network Application in Risk Information Security Assessment", Journal of Electronics & Cyber Defense, vol. 1, no.4, pp 23-33, 2014. (in Persian). DOR: 20.1001.1.23224347.1392.1.4.4.1

[16] S.A Charsoughi, M.A. Doustari, A. Yazdian Varjani, S.A. Mahdavi Ardestani, " Information Security Risk Assessment Using Artificial Neural Network Application in Risk Information Security Assessment", Journal of Electronics & Cyber Defense, vol. 1, no.1, pp

Journal of Computer Trends and Technology (IJCTT), vol. 4, pp. 3685-3692, 2013.

[33] S. M. Sulaman, K. Weyns, and M. Höst, "A review of research on risk analysis methods for IT systems," in Proceedings of the 17th International Conference on Evaluation and Assessment in Software Engineering, 2013, pp. 86-96.

[34] Z. Rodion, "Analysis of information risk management methods," University of Jyvaskyla, 2014.

[35] P. Shamala, R. Ahmad, and M. Yusoff, "A conceptual framework of info structure for information security risk assessment (ISRA)," Journal of Information Security and Applications, vol. 18, pp. 45-52, 2013. Doi: 10.1016/j.jisa.2013.07.002

[36] J. V. Barraza de la Paz, L. A. Rodríguez-Picón, V. Morales-Rocha, and S. V. Torres-Argüelles, "A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0," Systems, vol. 11, p. 218, 2023. doi: 10.3390/systems11050218

[37] M. Berrady, "ISRAM Method Comparison Comparative: framework study for risk assessment methods," University of Oslo, 2021.

[38] M. S. Saleh and A. Alfantookh, "A new comprehensive framework for enterprise information security risk management," Applied computing and informatics, vol. 9, pp. 107-118, 2011. doi: 10.1016/j.aci.2011.05.002

[39] SESAR, "Selection of Risk Assessment Methods Object of Study," University of Trento, SESAR JOINT UNDERTAKING, 2011.

[40] J. L. Spears, "A holistic risk analysis method for identifying information security risks," in Security Management, Integrity, and Internal Control in Information Systems: IFIP TC-11 WG 11.1 & WG 11.5 Joint Working Conference 7, 2005, pp. 185-202.

[41] E. Koza, "Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security," Medicon Engineering Themes, vol. 2, pp. 26-39, 2022.

[42] Central Bank, "Central Bank of The Islamic Republic of Iran," https://www.cbi.ir/, 2023.

[43] R. K. Devi, D. I. Sensuse, and R. R. Suryono, "Information Security Risk Assessment (ISRA): A Systematic Literature Review," Journal of Information Systems Engineering & Business Intelligence, vol. 8, pp. 207-217, 2022. doi: 10.20473/jisebi.8.2.207-217

[44] A. S. C. Junior and C. H. Arima, "Cyber Risk Management and iso 27005 Applied in Organizations: A Systematic Literature Review," REVISTA FOCO, vol. 16, pp. e1188-e1188, 2023.

[45] S. Fenz, J. Heurix, T. Neubauer, and F. Pechstein, "Current challenges in information security risk management," Information Management & Computer Security, vol. 22, pp. 410-430, 2014. doi: 10.1108/IMCS-07-2013-0053

[46] H. Bateni and P. Saeidi, "The effect of information quality integrity on information security risk management," Information and Communication Technology Innovations, vol 1, pp. 23-35, 2019 https://ait.ihu.ac.ir/article_204800.htm

1-13, 2013. (in Persian). DOR: 20.1001.1.23224347.1392.1.1.1.2

[17] M.C. Lee, "Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method," International Journal of Computer Science & Information Technology, vol. 6, p. 29, 2014.

[18] D. Ionita, "Current established risk assessment methodologies and tools," University of Twente, 2013.

[19] G. Wangen, C. Hallstensen, and E. Snekkenes, "A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF," INT J INF SECUR, vol. 17, pp. 681-699, 2018. doi: 10.1007/s10207-017-0382-0

[20] W. Labuschagne, "A comparative framework for evaluating information security risk management methods," Rand Afrikaans University, Standard Bank Academy for Information Technology, 2004.

[21] L. Pan and A. Tomlinson, "A systematic review of information security risk assessment," International Journal of Safety and Security Engineering, vol. 6, pp. 270-281, 2016. doi: 10.2495/SAFE-V6-N2-270-281

[22] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," COMPUT SECUR, vol. 57, pp. 14-30, 2016.

[23] F. Macedo and M. M. Da Silva, "Comparative study of information security risk assessment models," Universidad Técnica de Lisboa, Lisboa, 2012. Doi: 10.1016/j.cose.2015.11.001

[24] A. Behnia, R. Abd Rashid, and J. A. Chaudhry, "A survey of information security risk analysis methods," SmartCR, vol. 2, pp. 79-94, 2012.

[25] V. Agrawal, "A Comparative Study on Information Security Risk Analysis Methods," J. Comput., vol. 12, pp. 57-67, 2017. doi: 10.17706/jcp.12.1.57-67

[26] P. Vartiainen, "On the principles of comparative evaluation," EVALUATION-US, vol. 8, pp. 359-371, 2002. doi: 10.1177/135638902401462484

[27] J. C. Pomerol and S. Barba-Romero, Multicriterion decision in management: principles and practice vol. 25: Springer Science & Business Media, 2012.

[28] H. S. Shih, H. J. Shyur, and E. S. Lee, "An extension of TOPSIS for group decision making," MATH COMPUT MODEL, vol. 45, pp. 801-813, 2007. doi: 10.1016/j.mcm.2006.03.023

[29] T. A. Chandrinos, "Analysis of frameworks/methods for information security risk management," University of Piraeus, Thailand, 2023.

[30] G. Wangen and E. Snekkenes, "A taxonomy of challenges in information security risk management," in Proceeding of Norwegian Information Security Conference/Norsk informasjonssikkerhetskonferanse-NISK 2013-Stavanger, 18th-20th November 2013, 2013.

[31] M. Shokry, A. I. Awad, M. K. Abd-Ellah, and A. A. Khalaf, "When Security Risk Assessment Meets Advanced Metering Infrastructure: Identifying the Appropriate Method," SUSTAINABILITY-BASEL, vol. 15, p. 9812, 2023. doi: 10.3390/su15129812

[32] K. Kiran, S. Mukkamala, A. Katragadda, and D. Reddy, "Performance and analysis of risk assessment methodologies in information security," International