فصلنامه
فن‌آوری اطلاعات و ارتباطات در علوم تربیتی
سال یازدهم ـ شماره دوم ـ زمستان ۱۳۹۹ ـ صفحات ۱۶۶-۱۴۷

DOR: 20.1001.1.22285318.1399.11.2.8.4

شناسایی و رتبه‌بندی ریسک‌های مؤثر بر امنیت منابع اطلاعاتی با استفاده از تکنیک تصمیم‌گیری چند معیاره (TOPSIS)

ناصر زیدانی *

فریبا نظری **

چکیده

پژوهش حاضر با هدف شناسایی و اولویت‌بندی ریسک‌های مؤثر بر سیستم‌های مدیریت امنیت اطلاعات در شرکت بهره برداری نفت و گاز آغاجاری به انجام رسید. پژوهش از لحاظ هدف، کاربردی و از لحاظ ماهیت گردآوری اطلاعات، توصیفی از نوع پیمایشی است. جامعه آماری این تحقیق ۶۳ نفر از مدیران ارشد، مدیران میانی و کارشناسان ارشد فن‌آوری اطلاعات و ارتباطات در شرکت مذکور بودند که به حوزه امنیت سیستم‌های اطلاعاتی این سازمان، اشراف کامل داشتند و از میان آنها ۲۰ نفر به عنوان نمونه انتخاب شد. ابزار اصلی جمع آوری داده‌ها در این تحقیق، سه پرسش‌نامه محقق ساخته بود؛ پرسش‌نامه اول، با هدف شناسایی ریسک‌ها و به‌صورت نیمه ساختاریافته طراحی گردید؛ پرسش‌نامه دوم با هدف غربالگری ریسک‌های شناسایی شده به صورت بسته و بر اساس طیف پنج گزینه‌ای لیکرت تنظیم شد و نهایتا پرسش‌نامه سوم با هدف تعیین اوزان ریسک‌های اصلی (مقایسات زوجی) و هم‌چنین تعیین اولویت ریسک‌های فرعی (طیف پنج گزینه‌ای) طراحی گردید. بعد از توزیع و جمع آوری داده‌ها، انجام تجزیه و تحلیل‌های لازمه از طریق نرم افزارهای SPSS، ExpertChoice و Excel در دستور کار قرار گرفت. نتایج تحقیق منجر به شناسایی ۲۷ ریسک در قالب چهار دسته کلی شد. با توجه به نتایج پیشنهاد می‌شود یک طرح جامع و فراگیر برای امنیت اطلاعات و سرمایه گذاری های مناسب و متناسب با اولویت های امنیتی تدوین یابد.

واژگان کلیدی

ریسک، سیستم‌های امنیت اطلاعات، تصمیم‌گیری چندمعیاره

*دانشجوی کارشناسی ارشد گروه مدیریت فناوری اطلاعات ، واحد اهواز، دانشگاه آزاد اسلامی، اهواز،ایران f.nazari@iauahvaz.ac.ir

** استادیار گروه علم اطلاعات و دانش شناسی ، واحد اهواز، دانشگاه آزاد اسلامی، اهواز، ایران nazari_lib@yahoo.com

نویسنده مسؤول یا طرف مکاتبه: فریبا نظری

تاریخ دریافت مقاله: ۱۳۹۸/۰۸/۲۷ **تاریخ پذیرش مقاله: ۱۳۹۹/۰۹/۰۱**

مقدمه

فن‌آوری اطلاعات و سیستم‌های اطلاعاتی در تمام بخش‌های زندگی بشر ریشه دوانیده‌اند و اگرچه به تسهیل زندگی و ارتباطات بشر کمک می‌کنند اما مانند هر فن‌آوری نوظهور دیگر، با خود خطراتی را نیز به همراه می‌آورند؛ به عنوان مثال سازمانی که برای افزایش اثربخشی و کارایی خود در ارتباطات، از شبکه‌های مخابراتی و اینترنتی کمک می‌گیرد بایستی ریسک ناشی از دسترسی افراد غیر مجاز یا رقبا به اطلاعات سازمان را پذیرفته و یا آن را مدیریت کند. از این رو، تصمیم‌گیری برای پیاده‌سازی سیستم‌های اطلاعاتی و بهره‌گیری از مزایای فن‌آوری اطلاعات، مانند هر نوع تصمیم‌گیری دیگر در زندگی، باید به بررسی خطرات احتمالی آن پرداخته و با مدیریت ریسک‌های موجود، اثربخشی سیستم را ارتقاء بخشید (Yaghobi et al., 2015).

بررسی‌ها نشان داده است که فقدان برنامه مدیریت امنیت اطلاعات از مشکلات عمده در این زمینه بوده است. چالش مهمی که بسیاری از مجموعه‌ها هم اکنون درگیر آن می‌باشند شناسایی و اولویت‌بندی مخاطرات امنیت اطلاعات به عنوان اولین گام در طراحی و پیشبرد یک برنامه مؤثر امنیتی می‌باشد. ارزیابی مخاطرات، ابزار مهمی برای مدیران امنیت اطلاعات در تعیین خط‌مشی‌های امنیتی مناسب و انتخاب فن‌آوری‌ها و روش‌های مقرون به صرفه برای اجرای این خط‌مشی‌ها، محسوب می‌شود. مخاطرات هیچ‌گاه به طور کامل قابل حذف نیستند اما می‌توان با به‌کارگیری کنترل‌های امنیتی اطلاعات آنها را به حداقل مطلوب کاهش داد. ارزیابی مخاطرات، درجه ریسک فعلی را مشخص کرده و امکان تصمیم‌گیری دقیق برای کاهش و مدیریت این مخاطرات را فراهم می‌آورد. از آن‌جایی که تهدیدات و مخاطرات مرتبط با آنها در طول زمان تغییر می‌کنند لازم است تا نسبت به ارزیابی دوره‌ای مخاطرات و بررسی کارایی خط‌مشی‌ها و کنترل‌های امنیتی به‌کار گرفته شده، اقدام شود (Keshtegar et al., 2016).

مدیریت امنیت اطلاعات، بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف امنیت و بررسی موانع سر راه رسیدن به این اهداف را بر عهده دارد (AfKhami et al., 2005). یکی از وظایف مدیریت امنیت، بررسی و ایجاد یک سیستم امنیت اطلاعات است که متناسب با اهداف سازمان باشد. برای طراحی این سیستم باید عوامل مختلفی را در نظر گرفت؛ محاسبه ارزش اطلاعات از نظر اقتصادی، بررسی خطرات و محاسبه خسارت‌های احتمالی و تخمین هزینه

سودمندی استفاده از سیستم امنیت اطلاعات، بررسی تهدیدات احتمالی و انتخاب سودمندترین روش برای طراحی سیستم‌های امنیت اطلاعات، ضروری به نظر می‌رسد (Pipkin, 2000).

شرکت بهره برداری نفت و گاز آغاجاری نیز از این قاعده مستثنی نبوده و با توجه به نقش راهبردی آن در اقتصاد منطقه و حتی کشور، توجه به امنیت سیستم و منابع اطلاعاتی مستقر در آن بسیار حائز اهمیت می باشد. از جمله منابع اطلاعاتی حائز اهمیت در این مجموعه عظیم، داده‌ها و اطلاعات مربوط به عملیات بهره‌برداری، امور فنی، امور مالی، منابع انسانی، امور حقوقی و قراردادها، ایمنی، آزمایشگاه‌ها و تعمیرات می‌باشد. انجام مصاحبه‌های اولیه با مدیران فن‌آوری اطلاعات این شرکت نشان داد از جمله ریسک‌هایی که ممکن است منابع اطلاعاتی شرکت بهره‌برداری نفت و گاز آغاجاری را تهدید نماید می‌توان به ریسک‌های عوامل انسانی، ریسک‌های سیستمی، ریسک‌های فرآیندی و ریسک‌های برخاسته از رویه‌های کنترلی اشاره نمود. هم‌چنین، این مدیران اذعان داشتند که فقدان فعالیت‌های پژوهشی دقیق در حوزه شناسایی و ارزیابی ریسک‌های این حوزه، از نگرانی‌های آنها محسوب شده و انجام چنین پژوهش‌هایی می‌تواند آنها را در پیش بینی و کنترل ریسک‌های احتمالی، بسیار کمک نماید. بر همین اساس، پژوهش پیش رو قصد دارد تا با انجام یک مطالعه نظام‌مند و علمی، به پرسش‌های ذیل پاسخ دهد:

۱) ریسک‌های سیستم مدیریت امنیت اطلاعات در شرکت بهره‌برداری نفت و گاز آغاجاری کدامند؟

۲) بر اساس شاخص‌های احتمال وقوع و میزان تأثیر، چه اولویت‌بندی برای ریسک‌های مؤثر بر امنیت منابع اطلاعاتی در شرکت بهره‌برداری نفت و گاز آغاجاری می‌توان متصور بود؟

مبانی نظری و پیشینه پژوهش

سیستم مدیریت امنیت اطلاعات

با پیشرفت علوم کامپیوتری و هم‌چنین به‌وجود آمدن ابزارهای جدید هک و هم‌چنین وجود صدها مشکل ناخواسته در طراحی نرم‌افزارهای مختلف و روال‌های امنیتی سازمان‌ها، همیشه خطر حمله و دسترسی افراد غیرمجاز وجود دارد. حتی قوی‌ترین سایت‌های موجود در دنیا در معرض خطر افراد غیرمجاز قرار دارند. با وجود این‌که نمی‌توان امنیت ٪۱۰۰ داشت اما نباید به نکات

امنیتی بی‌توجه بود. در حال حاضر، مجموعه‌ای از استانداردهای مدیریتی و فنی ایمن‌سازی فضای تبادل اطلاعات ارائه شده‌اند که استاندارد مدیریتی «بی.اس. ۷۷۹» مؤسسه استاندارد انگلیس، استاندارد مدیریتی «ایزو-ایک ۱۷۷۹۹» موسسه بین‌المللی استاندارد و گزارش فنی «ایزو-ایک تی آر ۱۳۳۳۵» موسسه بین‌المللی استاندارد از برجسته‌ترین استانداردها در این زمینه محسوب می‌گردند (Zargari,2017).

مدیریت ریسک در حوزه فن‌آوری اطلاعات

تحولات عمده در محیط کسب و کار، مثل جهانی شدن کسب و کار و سرعت بالای تغییرات در فن‌آوری، باعث افزایش رقابت و دشواری مدیریت گردیده است. در محیط کسب و کار امروز، مدیریت و کارکنان می‌بایست توانایی برخورد با روابط درونی و وابستگی‌های مبهم و بغرنج میان فن‌آوری، داده‌ها، وظایف، فعالیت‌ها، فرآیندها و افراد را دارا باشند. در چنین محیط‌های پیچیده‌ای سازمان‌ها نیازمند مدیرانی هستند که این پیچیدگی‌های ذاتی را در زمان تصمیم‌گیری‌های مهم‌شان لحاظ و تفکیک کنند. مدیریت ریسک مؤثر که بر مبنای یک اصول مفهومی معتبر قرار دارد بخش مهمی از این فرآیند تصمیم‌گیری را تشکیل می‌دهد. در این بخش، این اصول به وسیله شناسایی عناصر اصلی ریسک و بررسی چگونگی تأثیر بالقوه این عناصر در موفقیت سازمان‌ها و چگونگی مقابله و مدیریت ریسک‌ها مورد بحث قرار می‌گیرد (Gary, 2002). مدیریت ریسک فرآیند سنجش یا ارزیابی ریسک و سپس طرح استراتژی‌هایی برای اداره ریسک است. در مجموع، استراتژی‌های به‌کار رفته شامل: انتقال ریسک به بخش‌های دیگر، اجتناب از ریسک، کاهش اثرات منفی ریسک و پذیرش قسمتی یا تمامی پیامدهای یک ریسک خاص هستند. برای حل مجموعه مشکلاتی که مدیران پروژه‌های فن‌آوری اطلاعات با آن مواجه می‌شوند بهتر است که از سیستم‌های مدیریت ریسک که شامل مجموعه‌ای از فرآیندهای سازمانی، استانداردها، نمونه‌های اسناد و رویه‌ها و روش‌هایی برای مدیریت ریسک می‌باشند استفاده کنند (Hosseini, 2016).

فرآیند مدیریت ریسک را می‌توان به طور مشخص، اقدامات لازم برای تحقق موفقیت‌آمیز پروژه‌های فن‌آوری اطلاعات تعریف نمود. در شرایطی که بازار در حال توسعه می‌باشد و تقاضا برای خدمات فن‌آوری اطلاعات وجود دارد فروشندگان این خدمات باید کیفیت بالای این

خدمات را از طریق کنترل و محاسبه ریسک‌های ممکن تأمین کنند. سیستم‌های اطلاعاتی جدید، مجموعه راه‌حل‌های جامع و ترکیبی و روش به‌کارگیری آنها را ارائه می‌دهد که قاعدتاً سرمایه‌گذاری قابل‌ملاحظه‌ای را از سوی شرکت‌ها می‌طلبد. سیستم‌های تکنولوژی اطلاعات، مجموعه کاملی از امکانات و وسایل برنامه‌ای و فنی می‌باشد که برای تجزیه و تحلیل، حفاظت و پردازش داده‌ها استفاده می‌شوند. ابزار تجزیه و تحلیل که جزء سیستم‌های فن‌آوری اطلاعات می‌باشد این امکان را می‌دهد که با سرعت بالایی حجم وسیعی از اطلاعات را پردازش نمود و بر اساس نتایج دریافتی، اقدامات اصلاحی را انجام داد (Rahnamaii Zakavat, 2017).

مدیریت ریسک پروژه برای به‌کارگیری سیستم‌های اطلاعاتی، نرم‌افزار، تکنولوژی حفاظت اطلاعات، تکنولوژی‌های شبکه‌ای که ارتباطات و سیستم‌های اطلاعاتی را تأمین می‌نمایند باید تمام ریسک‌های ممکن را از پیش شناسایی کند و مجموعه اقداماتی را برای گریز از مشکلات جدی ناشی از آن‌ها در زمان تحقق پروژه در نظر گیرد. ریسک‌های اصلی که قاعدتاً بر روی هر پروژه فن‌آوری اطلاعات، تأثیر می‌گذارند شامل: عدم رعایت مدت زمان انجام پروژه، افزایش قیمت و عدم رعایت پارامترهای کیفیت هستند ولی مهم‌ترین عامل بروز این ریسک‌ها به خصوص در پروژه‌های فن‌آوری اطلاعات،آماده نبودن شرکت برای اجرای پروژه‌های مشابه می‌باشد (Hosseini, 2016).

در این راستا تحقیقاتی را که بتوان مشابه تحقیق حاضر دانست عبارتند از: نتایج پژوهش زندیان و همکاران (Zandian et al., 2018) نشان داد که حمایت مدیریت عالی، آموزش کاربران، فرهنگ امنیتی میان کاربران، مهارت کاربران، تقویت خط‌مشی کاربران، خودباوری و تجربیات کاربران بر اثربخشی امنیت سیستم‌های اطلاعاتی تأثیر مستقیم دارد. طبق نتایج پژوهش رضایی و مصدق (Rezaii & Mosadegh, 2018) شاخص‌های نقش مدیریت، آگاهی از امنیت سیستم اطلاعات و انطباق با آموزش، امنیت سیستم اطلاعات کسب وکار و ارزیابی ریسک امنیت سیستم اطلاعات بر اثربخشی سیستم مدیریت امنیت اطلاعات تأثیرگذار می‌باشند. یوسفی زنوز و همکاران (Yousefi Zenooz, 2015)، ریسک‌های امنیت اطلاعات را شامل ریسک‌های برخاسته از عوامل انسانی (مدیران ارشد، مشاورین و کارکنان)، ریسک‌های برخاسته از خط مشی‌ها و رویه‌ها، ریسک‌های برخاسته از سیستم‌های کنترلی و ریسک‌های برخاسته از سیستم‌های اطلاعاتی دانستند.

این ریسک‌ها مبانی پژوهش حاضر نیز قرار گرفته است و سعی شده ریسک‌های امنیت اطلاعات در شرکت بهره برداری نفت و گاز آغاجاری در قالب این مدل شناسایی گردد.

یعقوبی و همکاران (Yaghobi, 2015)، ریسک‌های نامحسوس را به عنوان مهم‌ترین ریسک‌ها در به‌کارگیری رایانش ابری در سازمان‌های دولتی شناسایی کرده‌اند. در این میان، ریسک محرمانگی داده رتبه نخست را به دست آورد. صیادی و همکاران (Sayadi, 2011)، ساختار جامعی از ریسک‌های اصلی پروژه‌های تونل‌سازی در قالب ۱۷ دسته اصلی و ۱۹۶ زیرسطح تهیه نموده و سپس این ریسک‌ها را رتبه‌بندی کردند. بر اساس نتایج، عوامل اقتصادی و شرایط حقوقی به ترتیب بیش‌ترین و کم‌ترین رتبه ریسک را به خود اختصاص دادند. اندری (Andrii, 2019) برای ادغام موفقیت‌آمیز فرآیندهای تجاری، یک رویکرد جدید برای شناسایی و پیش‌بینی خطر عرضه در شرایط عدم قطعیت، یک راه حل پیچیده برای ایمن سازی داده‌ها در سیستم‌های اطلاعاتی برای مدیریت زنجیره تأمین پیشنهاد دادند. نتایج پژوهش علوی و همکاران (Alavi et al, 2016)، نشان داد که رابطه معناداری بین ریسک‌ها و خطرات امنیت اطلاعات و میزان سرمایه‌گذاری سازمان در این حوزه وجود دارد و استفاده از الگوی سرمایه‌گذاری مبتنی بر ریسک امنیت اطلاعات، نشان می‌دهد که این امر به سازمان‌ها کمک می‌کند تا در حوادث دیگر از آن استفاده کنند. نتایج پژوهش اوانگلوس و همکاران (Evangelos et al, 2013)، نشان داد که ریسک‌های روانی بر کارکنان تأثیرگذار بوده و توانایی آنها را برای محافظت از سیستم‌های اطلاعاتی کاهش می‌دهد.

روش

این پژوهش از لحاظ هدف، کاربردی و از لحاظ ماهیت گردآوری اطلاعات، توصیفی- پیمایشی است. جامعه و نمونه آماری در فاز شناسایی، مدیران ارشد، مدیران میانی و کارشناسان ارشد فن‌آوری اطلاعات و ارتباطات در شرکت بهره برداری نفت و گاز آغاجاری بودند. شاخص خبرگی برای این افراد، تسلط علمی آنها به حوزه امنیت سیستم‌ها و منابع اطلاعاتی شرکت بهره‌برداری نفت و گاز آغاجاری در نظر گرفته شد. تعداد این افراد، ۶۳ نفر بود. جهت انتخاب افراد نهایی از میان جامعه آماری، سعی شد از روش "قضاوتی" استفاده شود. ۲۰ نفر از مطلع‌ترین

افراد در حوزه موضوع پژوهش، در فرآیند پژوهش مشارکت داده شدند. برای جامعه و نمونه آماری در فاز اولویت‌بندی ریسک‌ها نیز سعی شد از خبرگانی که در فاز اول (شناسایی ریسک‌ها) در پژوهش مشارکت داشته‌اندکمک گرفته شود زیرا این خبرگان، مطلع‌ترین افراد به حوزه امنیت سیستم‌ها و منابع اطلاعاتی در شرکت بهره‌برداری نفت و گاز آغاجاری بوده و بهترین گزینه برای اولویت‌بندی ریسک‌های شناسایی شده می باشند.

به طور کلی روش گردآوری داده‌ها در پژوهش حاضر به دو دسته کلی کتابخانه‌ای و میدانی قابل تقسیم می‌باشد. ابتدا بر اساس ادبیات پژوهش و مصاحبه با اعضای نمونه، ۴ دسته ریسک اصلی و ۳۱ دسته ریسک فرعی شناسایی گردید. جهت اجماع نظر خبرگان و غربالگری، پرسش‌نامه مرحله اول توزیع گردید. پرسش‌نامه دوم و سوم بر مبنای روش‌های فرآیند تحلیل سلسله مراتبی و تاپسیس طراحی شدند و هدف از آن وزن‌دهی و اولویت‌بندی نهایی ریسک‌های مؤثر بر امنیت منابع اطلاعاتی در شرکت بهره‌برداری نفت و گاز آغاجاری بود. در پژوهش حاضر، به منظور بررسی روایی ابزار، ابتدا از روش "بررسی روایی صوری" استفاده شده است. بدین منظور پرسش‌نامه در اختیار چند نفر از اساتید دانشگاهی قرار گرفت و از آنها درخواست شد تا نظرات خود را پیرامون میزان تناسب ساختار پرسش‌نامه‌ها با اهداف آنها بیان فرمایند. سرانجام پس از اخذ نظر اساتید، اصلاحات لازم اعمال گردید و روایی ابزار جمع‌آوری داده‌ها مورد تأیید قرار گرفت.

یافته ها

در این پژوهش، بر اساس نظر خبرگان و از طریق پرسش‌نامه باز و به استناد پیشینه پژوهش، ۴ ریسک اصلی و ۳۱ ریسک فرعی شناسایی گردید. به منظور غربالگری ریسک‌ها از آزمون t تک نمونه‌ای انتخاب گردید. در این آزمون حد آستانه ۳ و درجه اطمینان ۹۵٪ قرار داده شد. نتایج آزمون t در جدول ۱ بیان شده است. سطح معناداری همه ریسک‌ها کم‌تر از ۰/۰۵ است که در مورد همه آنها فرض صفر رد شده و فرض یک مورد پذیرش قرار می‌گیرد. جهت دانستن این‌که کدام ریسک میانگین اهمیت بالای سه و کم‌تر از ۳، دارد می بایست به مقدار آماره t در جدول ۳ دقت کنیم. اگر میزان این آماره مثبت باشد ریسک مربوطه بالاتر از میانگین بوده و بالعکس. همان‌گونه که در جدول ۳ مشخص است مقدار t ریسک‌های R9، R10، R19، R25 منفی است و در نتیجه این ریسک‌ها اهمیتی زیر حد میانگین (۳) دارند.

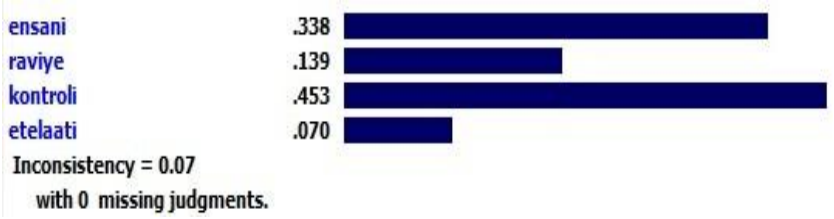
جدول ۱: نتایج آزمون t جهت غربالگری ریسک‌ها

ریسک‌های اصلی	ریسک‌های فرعی	آماره آزمون	درجه آزادی	سطح معناداری	اختلاف میانگین	۹۵٪ بازه اطمینان از اختلاف	
						پایین	بالا
ریسک‌های برخاسته از عوامل انسانی (مدیران ارشد، مشاورین و کارکنان)	R1	۲/۸۹۶	۱۹	۰/۰۰۹	۰/۷	۰/۱۹۴۱۱	۱/۲۰۵۸۹
	R2	۲/۵۷۰	۱۹	۰/۰۱۹	۰/۷	۰/۱۲۹۸۳	۱/۲۷۰۱۷
	R3	۰/۵۱۳	۱۹	۰/۰۱۴	۰/۱۵	-۰/۴۶۲۵۷	۰/۷۶۲۵۷
	R4	۵/۲۱۰	۱۹	۰/۰۰۰	۱	۰/۵۹۸۲۶	۱/۴۰۱۷۴
	R5	۶/۸۵۰	۱۹	۰/۰۰۰	۱/۱	۰/۷۶۳۸۸	۱/۴۳۶۱۲
	R6	۵/۸۷۷	۱۹	۰/۰۰۰	۱/۱۵	۰/۷۴۰۴۴	۱/۵۵۹۵۶
	R7	۳/۰۱۸	۱۹	۰/۰۰۷	۰/۹	۰/۲۷۵۷۸	۱/۵۲۴۲۲
	R8	۴/۳۵۹	۱۹	۰/۰۰۰	۱	۰/۵۱۹۸۳	۱/۴۸۰۱۷
	R9	-۶/۸۶۵۰	۱۹	۰/۰۰۰	-۱/۱	-۱/۴۳۶۱۲	-۰/۷۶۳۸۸
	R10	-۷/۶۶۷	۱۹	۰/۰۰۰	-۱/۱۵	-۱/۴۶۳۹۵	-۰/۸۳۶۰۵
	R11	۳/۳۸۷	۱۹	۰/۰۰۳	۰/۸	۰/۳۰۵۶۳	۱/۲۹۴۳۷
ریسک‌های برخاسته از خط مشی‌ها و رویه‌ها	R12	۵/۳۹۵	۱۹	۰/۰۰۰	۱/۱	۰/۶۷۳۲۱	۱/۵۲۶۷۹
	R13	۰/۵۸۰	۱۹	۰/۰۱۹	۰/۲	-۰/۵۲۱۸۶	۰/۹۲۱۸۶
	R14	۴/۴۱۴	۱۹	۰/۰۰۰	۰/۹	۰/۴۷۳۲۱	۱/۳۲۶۷۹
	R15	۳/۴۷۰	۱۹	۰/۰۰۳	۰/۷۵	۰/۲۹۷۶۴	۱/۲۰۲۳۶
	R16	۵/۳۳۹	۱۹	۰/۰۰۰	۱/۲	۰/۷۲۹۵۳	۱/۶۷۰۴۷
	R17	۲/۸۸۶	۱۹	۰/۰۰۹	۰/۸	۰/۲۱۹۸۱	۱/۳۸۰۱۹
	R18	۳/۳۷۱	۱۹	۰/۰۲۸	۰/۶۵	۰/۰۷۶۳۰	۱/۲۲۳۷۰
	R19	-۶/۷۲۵	۱۹	۰/۰۰۰	-۱/۳	-۱/۷۰۴۶۰	-۰/۸۹۵۴۰
ریسک‌های برخاسته از سیستم‌های کنترلی	R20	۴/۷۲۳	۱۹	۰/۰۰۰	۰/۹	۰/۵۰۱۱۴	۱/۲۹۸۸۶
	R21	۰/۶۰۷	۱۹	۰/۰۳۱	۰/۲	۰/۴۸۹۱۸	۰/۸۸۹۱۸
	R22	۵/۵۱۰	۱۹	۰/۰۰۰	۱/۱۵	۰/۷۱۳۲۰	۱/۵۸۶۸۰
	R23	۰/۶۳۹	۱۹	۰/۰۴۰	۰/۲	۰/۴۵۴۸۷	۰/۸۵۴۸۷

ریسک‌های اصلی	ریسک‌های فرعی	آماره آزمون	درجه آزادی	سطح معناداری	اختلاف میانگین	۹۵٪ بازه اطمینان از اختلاف	
						پایین	بالا
	R24	۲/۳۸۰	۱۹	۰/۰۲۸	۰/۷۵	۰/۰۹۰۳۱	۱/۴۰۹۶۹
	R25	-۵/۳۹۵	۱۹	۰/۰۰۰	-۱/۱	-۱/۵۲۶۷۹	-۰/۶۷۳۲۱
	R26	۳/۴۵۴	۱۹	۰/۰۰۳	۰/۹	۰/۳۵۴۶۳	۱/۴۴۵۳۷
ریسک‌های برخاسته از سیستم‌های اطلاعاتی	R27	۳/۲۱۴	۱۹	۰/۰۰۵	۰/۹	۰/۳۱۳۸۷	۱/۴۸۶۱۳
	R28	۵/۷۷۲	۱۹	۰/۰۰۰	۱/۱	۰/۷۰۱۱۴	۱/۴۹۸۸۶
	R29	۴/۷۹۰	۱۹	۰/۰۰۰	۰/۹۵	۰/۵۳۴۸۵	۱/۳۶۵۱۵
	R30	۲/۶۰۴	۱۹	۰/۰۱۷	۰/۵۵	۰/۱۰۷۹۵	۰/۹۹۲۰۵
	R31	۵/۰۸۲	۱۹	۰/۰۰۰	۱/۱	۰/۶۴۷۰۱	۱/۵۵۲۹۹

تعیین اولویت ریسک‌های اصلی به روش فرآیند تحلیل سلسله مراتبی

پس از ساخت مدل در نرم افزار اکسپرت چویس و ورود ماتریس مقایسات زوجی (برگرفته از نظر ۲۰ نفر خبره)، وزن ریسک‌های اصلی به صورت ذیل به‌دست آمد:



شکل ۱- خروجی نرم افزار اکسپرت چویس در خصوص تعیین وزن نسبی ریسک‌های اصلی

همان‌طور که در شکل شماره ۱ مشخص است ریسک‌های برخاسته از سیستم‌های کنترلی با وزن نسبی ۰/۴۵۳ در رتبه اول، ریسک‌های برخاسته از عوامل انسانی (مدیران ارشد، مشاورین و کارکنان با وزن نسبی ۰/۳۳۸ در اولویت دوم، ریسک‌های برخاسته از خط مشی‌ها و رویه‌ها با وزن نسبی ۰/۱۳۹ در اولویت سوم و ریسک‌های برخاسته از سیستم‌های اطلاعاتی نیز با ۰/۰۷۰ در

رتبه چهارم قرار دارد. نرخ ناسازگاری مقایسات زوجی ۰/۰۷ به‌دست آمده است که چون کم‌تر از ۰/۱۰ است این مقایسات قابل قبول می‌باشد.

تعیین وزن نسبی شاخص‌های تصمیم‌گیری به روش فرآیند تحلیل سلسله مراتبی

در این پژوهش و در پرسش‌نامه تاپسیس، دو معیار احتمال وقوع و میزان تأثیر جهت تعیین اولویت ریسک‌ها در نظر گرفته شد. در زیر، خروجی نرم‌افزار اکسپرت چویس در خصوص وزن نسبی این شاخص تصمیم‌گیری ارائه شده است:

شکل ۲- خروجی نرم افزار اکسپرت چویس در خصوص تعیین وزن نسبی شاخص‌های تصمیم گیری

وزن شاخص «احتمال وقوع» ۰/۶۹۱ و وزن شاخص میزان تأثیر ۰/۳۰۹ محاسبه شده است.

رتبه‌بندی ریسک‌های شناسایی شده با استفاده از روش تاپسیس

در این پژوهش، جهت رتبه‌بندی ریسک‌ها، از روش تاپسیس استفاده شد. بدین منظور، پرسش‌نامه شماره ۳ طراحی و توزیع گردید و در آن از خبرگان خواسته شد با در نظر گرفتن هر یک از معیارهای «احتمال وقوع» و «میزان تأثیر»، به ریسک‌ها نمره دهند. در ادامه، گام‌های طی شده متدولوژی تاپسیس جهت رتبه‌بندی ریسک‌ها تشریح شده‌اند:

به منظور قابل مقایسه شدن، ماتریس تصمیم‌گیری با استفاده از رابطه ۱ به ماتریس به‌هنجار شده یا ماتریس بی‌مقیاس (N_1) تبدیل می‌شوند. در جدول ۲، ماتریس بی‌مقیاس ارائه شده است:

$$n_{ij} = \frac{r_{ij}}{\sqrt{\sum_{i=1}^{m} r_{ij}^2}} \qquad (۱)$$

جدول ۲: ماتریس بی مقیاس

ریسک‌ها	کد	احتمال وقوع	میزان تأثیر
نبود تعهد و حمایت برخی از مدیران ارشد به امنیت اطلاعات	R1	۰/۱۶۴	۰/۰۷۶
عدم تخصیص بودجه‌های مناسب به طرح‌های مربوط به امنیت اطلاعات	R2	۰/۱۶۴	۰/۰۴۶
عدم توجه به زمان‌بندی پیاده سازی و اجرایی نمودن طرح‌های حوزه امنیت اطلاعات	R3	۰/۱۶۴	۰/۰۶۱
عدم بهره گیری از مشاورین برجسته در زمینه امنیت اطلاعات	R4	۰/۱۶۴	۰/۰۷۶
عدم ثبات مدیران در حوزه امنیت اطلاعات	R5	۰/۱۳۱	۰/۰۶۱
کمبود نیروی‌های متخصص در زمینه امنیت اطلاعات	R6	۰/۱۶۴	۰/۰۶۱
آگاهی پایین کارکنان در حوزه امنیت اطلاعات	R7	۰/۱۶۴	۰/۰۷۶
عدم ارائه آموزش‌های مناسب به کارکنان در حوزه امنیت اطلاعات	R8	۰/۱۳۱	۰/۰۶۱
عدم وجود یک طرح جامع و فراگیر برای امنیت اطلاعات و سرمایه گذاری‌های مناسب و متناسب با اولویت‌های امنیتی	R9	۰/۱۳۱	۰/۰۶۱
عدم وجود یک خط مشی امنیت اطلاعات جامع، کامل و قابل بازنگری	R10	۰/۱۳۱	۰/۰۶۱
شفاف نبودن تعریف مسئولیت امنیت اطلاعات	R11	۰/۰۶۶	۰/۰۱۵
عدم وجود رویه ای مناسب در طبقه بندی و کدگذاری اطلاعات	R12	۰/۱۳۱	۰/۰۶۱
عدم انطباق سیستم‌ها با خط مشی‌ها و استانداردهای امنیت اطلاعات	R13	۰/۰۳۳	۰/۰۳۰
عدم مدیریت (شناسایی و رفع) ضعف‌های امنیت اطلاعات	R14	۰/۱۳۱	۰/۰۴۶
عدم وجود رویه‌های مدیریت بحران در حوزه امنیت اطلاعات	R15	۰/۱۳۱	۰/۰۶۱
عدم بازمهندسی دوره ای فرآیندهای حوزه امنیت اطلاعات	R16	۰/۱۳۱	۰/۰۷۶
عدم کنترل مناسب در صحت داده‌های ورودی، پردازش‌های درونی، و صحت داده‌های خروجی	R17	۰/۱۳۱	۰/۰۶۱
عدم نظارت و پایش مناسب در توسعه نرم افزارهای برون سپاری شده حوزه‌های اطلاعاتی	R18	۰/۰۹۹	۰/۰۴۶
عدم گزارش دهی مناسب رویدادها و ضعف‌های حوزه امنیت اطلاعات	R19	۰/۱۳۱	۰/۰۶۱
عدم وجود اقدامات مناسب پیشگیرانه، اکتشافی و اصلاحی (به روز رسانی نرم افزارهای امنیتی) برای حفاظت از سیستم امنیت اطلاعات	R20	۰/۰۹۹	۰/۰۳۰
عدم آشنایی کامل و به روز متخصصین حوزه امنیت اطلاعات با ویروس‌ها ، کرم‌ها ،	R21	۰/۱۶۴	۰/۰۷۶

ریسک‌ها	کد	احتمال وقوع	میزان تأثیر
جاسوس افزارها و اسپم‌ها			
عدم مستند سازی و آرشیوبندی کامل و صحیح فرآیندها، رویدادها و رویه‌ها در حوزه امنیت اطلاعات	R22	۰/۱۳۱	۰/۰۴۶
عدم ایجاد نسخه پشتیبان از برخی اطلاعات و یا نگهداری نامناسب از نسخه‌های پشتیبان	R23	۰/۱۳۱	۰/۰۷۶
سطح بندی نامناسب اطلاعات (جهت تعیین دسترسی‌ها و سلسله مراتب اطلاعاتی)	R24	۰/۱۳۱	۰/۰۶۱
عدم وجود امنیت کافی در فرآیند تبادل اطلاعات و نرم افزارهای تخصصی واحدهای مختلف سازمان	R25	۰/۱۳۱	۰/۰۶۱
عدم وجود امنیت در خدمات شبکه‌های اینترنتی مورد استفاده سازمان	R26	۰/۰۶۶	۰/۰۶۱
عدم امنیت کامل سیستم اینترانت داخلی سازمان و احتمال نفوذ پذیری آن	R27	۰/۱۳۱	۰/۰۴۶

به دست آوردن ماتریس بی‌مقیاس موزون

برای به‌دست آوردن ماتریس بی‌مقیاس موزون(V)، ماتریس بی‌مقیاس شده (به دست آمده از گام دوم) را در ماتریس مربعی($w_{n\times n}$) که عناصر قطر اصلی آن اوزان شاخص‌ها و دیگر عناصر آن صفر می‌باشد ضرب می کنیم. جدول ۳، ماتریس بی‌مقیاس وزین را نشان می‌دهد:

$$V = N_1 \times w_{n\times n} \qquad (۲)$$

جدول ۳: ماتریس بی‌مقیاس وزین (V)

ریسک‌ها	کد	احتمال وقوع	میزان تأثیر
نبود تعهد و حمایت برخی از مدیران ارشد به امنیت اطلاعات	R1	۰/۲۳۸	۰/۲۴۶
عدم تخصیص بودجه‌های مناسب به طرح‌های مربوط به امنیت اطلاعات	R2	۰/۲۳۸	۰/۱۴۸
عدم توجه به زمان‌بندی پیاده سازی و اجرایی نمودن طرح‌های حوزه امنیت اطلاعات	R3	۰/۲۳۸	۰/۱۹۷
عدم بهره گیری از مشاورین برجسته در زمینه امنیت اطلاعات	R4	۰/۲۳۸	۰/۲۴۶

ریسک‌ها	کد	احتمال وقوع	میزان تأثیر
عدم ثبات مدیران در حوزه امنیت اطلاعات	R5	۰/۱۹۰	۰/۱۹۷
کمبود نیروی‌های متخصص در زمینه امنیت اطلاعات	R6	۰/۲۳۸	۰/۱۹۷
آگاهی پایین کارکنان در حوزه امنیت اطلاعات	R7	۰/۲۳۸	۰/۲۴۶
عدم ارائه آموزش‌های مناسب به کارکنان در حوزه امنیت اطلاعات	R8	۰/۱۹۰	۰/۱۹۷
عدم وجود یک طرح جامع و فراگیر برای امنیت اطلاعات و سرمایه گذاری‌های مناسب و متناسب با اولویت‌های امنیتی	R9	۰/۱۹۰	۰/۱۹۷
عدم وجود یک خط مشی امنیت اطلاعات جامع، کامل و قابل بازنگری	R10	۰/۱۹۰	۰/۱۹۷
شفاف نبودن تعریف مسئولیت امنیت اطلاعات	R11	۰/۰۹۵	۰/۰۴۹
عدم وجود رویه ای مناسب در طبقه بندی و کدگذاری اطلاعات	R12	۰/۱۹۰	۰/۱۹۷
عدم انطباق سیستم‌ها با خط مشی‌ها و استانداردهای امنیت اطلاعات	R13	۰/۰۴۸	۰/۰۹۹
عدم مدیریت (شناسایی و رفع) ضعف‌های امنیت اطلاعات	R14	۰/۱۹۰	۰/۱۴۸
عدم وجود رویه‌های مدیریت بحران در حوزه امنیت اطلاعات	R15	۰/۱۹۰	۰/۱۹۷
عدم بازمهندسی دوره ای فرآیندهای حوزه امنیت اطلاعات	R16	۰/۱۹۰	۰/۱۴۸
عدم کنترل مناسب در صحت داده‌های ورودی، پردازش‌های درونی، و صحت داده‌های خروجی	R17	۰/۱۹۰	۰/۱۹۷
عدم نظارت و پایش مناسب در توسعه نرم افزارهای برون سپاری شده حوزه‌های اطلاعاتی	R18	۰/۱۴۳	۰/۰۹۹
عدم گزارش دهی مناسب رویدادها و ضعف‌های حوزه امنیت اطلاعات	R19	۰/۱۹۰	۰/۰۶۱
عدم وجود اقدامات مناسب پیشگیرانه، اکتشافی و اصلاحی (به روز رسانی نرم افزارهای امنیتی) برای حفاظت از سیستم امنیت اطلاعات	R20	۰/۱۴۳	۰/۲۴۶
عدم آشنایی کامل و به روز متخصصین حوزه امنیت اطلاعات با ویروس‌ها ، کرم‌ها ، جاسوس افزارها و اسپم‌ها	R21	۰/۲۳۸	۰/۱۴۸
عدم مستند سازی و آرشیوبندی کامل و صحیح فرآیندها، رویدادها و رویه‌ها در حوزه امنیت اطلاعات	R22	۰/۱۹۰	۰/۲۴۶
عدم ایجاد نسخه پشتیبان از برخی اطلاعات و یا نگهداری نامناسب از نسخه‌های پشتیبان	R23	۰/۱۹۰	۰/۱۹۷

ریسک‌ها	کد	احتمال وقوع	میزان تأثیر
سطح بندی نامناسب اطلاعات (جهت تعیین دسترسی‌ها و سلسله مراتب اطلاعاتی)	R24	۰/۱۹۰	۰/۱۹۷
عدم وجود امنیت کافی در فرآیند تبادل اطلاعات و نرم افزارهای تخصصی واحدهای مختلف سازمان	R25	۰/۱۹۰	۰/۱۹۷
عدم وجود امنیت در خدمات شبکه‌های اینترنتی مورد استفاده سازمان	R26	۰/۰۹۵	۰/۱۹۷
عدم امنیت کامل سیستم اینترانت داخلی سازمان و احتمال نفوذ پذیری آن	R27	۰/۱۹۰	۰/۱۴۸

رتبه‌بندی گزینه‌ها

در این مرحله گزینه‌ها بر اساس مقدار CL رتبه‌بندی می‌شوند؛ به عبارتی هر گزینه‌ای که CL بالاتری داشته باشد رتبه بهتری کسب خواهد کرد. جدول ذیل رتبه‌بندی گزینه‌ها را نشان می‌دهد:

جدول ۴: محاسبه نزدیکی به راه حل ایده‌آل مثبت و منفی همچنین رتبه‌بندی گزینه‌ها

ریسک‌ها	کد	ضریب نزدیکی(CL)
نبود تعهد و حمایت برخی از مدیران ارشد به امنیت اطلاعات	R1	۱
عدم تخصیص بودجه‌های مناسب به طرح‌های مربوط به امنیت اطلاعات	R2	۰/۸۱۶
عدم توجه به زمان‌بندی پیاده سازی و اجرایی نمودن طرح‌های حوزه امنیت اطلاعات	R3	۰/۹۰۱
عدم بهره گیری از مشاورین برجسته در زمینه امنیت اطلاعات	R4	۱
عدم ثبات مدیران در حوزه امنیت اطلاعات	R5	۰/۷۵۰
کمبود نیروی‌های متخصص در زمینه امنیت اطلاعات	R6	۰/۹۰۱
آگاهی پایین کارکنان در حوزه امنیت اطلاعات	R7	۱
عدم ارائه آموزش‌های مناسب به کارکنان در حوزه امنیت اطلاعات	R8	۰/۷۵۰
عدم وجود یک طرح جامع و فراگیر برای امنیت اطلاعات و سرمایه گذاری‌های مناسب و متناسب با اولویت‌های امنیتی	R9	۰/۷۵۰
عدم وجود یک خط مشی امنیت اطلاعات جامع، کامل و قابل بازنگری	R10	۰/۷۵۰
شفاف نبودن تعریف مسئولیت امنیت اطلاعات	R11	۰/۲۲۱

ریسک‌ها	کد	ضریب نزدیکی(CL)
عدم وجود رویه ای مناسب در طبقه بندی و کدگذاری اطلاعات	R12	۰/۷۵۰
عدم انطباق سیستم‌ها با خط مشی‌ها و استانداردهای امنیت اطلاعات	R13	۰/۰۹۹
عدم مدیریت (شناسایی و رفع) ضعف‌های امنیت اطلاعات	R14	۰/۶۹۷
عدم وجود رویه‌های مدیریت بحران در حوزه امنیت اطلاعات	R15	۰/۷۵۰
عدم بازمهندسی دوره ای فرآیندهای حوزه امنیت اطلاعات	R16	۰/۷۷۹
عدم کنترل مناسب در صحت داده‌های ورودی، پردازش‌های درونی، و صحت داده‌های خروجی	R17	۰/۷۵۰
عدم نظارت و پایش مناسب در توسعه نرم افزارهای برون سپاری شده حوزه‌های اطلاعاتی	R18	۰/۵۰۰
عدم گزارش دهی مناسب رویدادها و ضعف‌های حوزه امنیت اطلاعات	R19	۰/۷۵۰
عدم وجود اقدامات مناسب پیشگیرانه، اکتشافی و اصلاحی (به روز رسانی نرم افزارهای امنیتی) برای حفاظت از سیستم امنیت اطلاعات	R20	۰/۴۵۷
عدم آشنایی کامل و به روز متخصصین حوزه امنیت اطلاعات با ویروس‌ها ، کرم‌ها ، جاسوس افزارها و اسپم‌ها	R21	۱
عدم مستند سازی و آرشیوبندی کامل و صحیح فرآیندها، رویدادها و رویه‌ها در حوزه امنیت اطلاعات	R22	۰/۶۹۷
عدم ایجاد نسخه پشتیبان از برخی اطلاعات و یا نگهداری نامناسب از نسخه‌های پشتیبان	R23	۰/۷۷۹
سطح بندی نامناسب اطلاعات (جهت تعیین دسترسی‌ها و سلسله مراتب اطلاعاتی)	R24	۰/۷۵۰
عدم وجود امنیت کافی در فرآیند تبادل اطلاعات و نرم افزارهای تخصصی واحدهای مختلف سازمان	R25	۰/۷۵۰
عدم وجود امنیت در خدمات شبکه‌های اینترنتی مورد استفاده سازمان	R26	۰/۳۶۱
عدم امنیت کامل سیستم اینترانت داخلی سازمان و احتمال نفوذ پذیری آن	R27	۰/۲۶۷

بحث و نتیجه‌گیری

پژوهش حاضر در پی پاسخ به دو پرسش اصلی زیر بود: اولین سؤال پژوهش، بدین صورت مطرح شده بود که: «ریسک‌های سیستم مدیریت امنیت اطلاعات در شرکت بهره‌برداری نفت و گاز آغاجاری کدامند؟». برای پاسخ به سؤال مذکور، بر اساس مبانی نظری مورد بررسی، ۴ ریسک اصلی و ۳۱ ریسک فرعی (ریسک‌های برخاسته از عوامل انسانی (مدیران ارشد، مشاورین و کارکنان)، ریسک‌های برخاسته از خط مشی‌ها و رویه‌ها، ریسک‌های برخاسته از سیستم‌های کنترلی، ریسک‌های برخاسته از سیستم‌های اطلاعاتی) شناسایی و جهت اجماع و غربالگری، در قالب یک پرسش‌نامه بسته در معرض بررسی خبرگان قرار گرفت. ماحصل این دو اقدام، شناسایی ۴ ریسک اصلی و ۲۷ ریسک فرعی بود.

این یافته، با نتایج پژوهش‌های زندیان و همکاران (Zandiyan,2018)، رضایی و مصدق (Rezaii & Mosadegh, 2018)، کشته گر و همکاران (Keshtegar & et.al, 2015)، یوسفی زنوز و همکاران (Yousefi Zenooz & et al., 2014)، ریس و همکاران (Reyes et al, 2010)، اوانگلوس و همکاران (Evangelos et al,2013)، جیکیانگ و همکاران (Jiqiang et al., 2014)، علوی و همکاران (Alavi et al., 2016) در زمینه ریسک‌های سیستم مدیریت امنیت اطلاعات در شرکت بهره برداری نفت و گاز آغاجاری همخوانی دارد.

علاوه بر این، پرسش دوم پژوهش بدین صوت مطرح شده که: «رتبه‌بندی ریسک‌های سیستم مدیریت امنیت اطلاعات در شرکت بهره‌برداری نفت و گاز آغاجاری بر اساس شاخص‌های احتمال وقوع و میزان تأثیر به چه نحو می‌باشد؟». هدف از طرح این پرسش، کاربردی‌تر کردن نتایج پژوهش بود. جهت پاسخ به این پرسش، پرسش‌نامه شماره ۲ طراحی، توزیع و جمع‌آوری شد و دو نوع آنالیز بر روی داده‌ها صورت پذیرفت. ابتدا از طریق فرآیند تحلیل سلسله مراتبی، دو شاخص ارزیابی ریسک (احتمال وقوع، میزان تأثیر) وزن‌دهی شده، آن‌گاه از طریق تحلیل تاپسیس، ریسک‌های فوق‌الذکر اولویت‌بندی گردیدند. در خصوص ریسک‌های اصلی، مشخص شده به ترتیب ریسک‌های برخاسته از سیستم‌های کنترلی، ریسک‌های برخاسته از عوامل انسانی (مدیران ارشد، مشاورین و کارکنان)، ریسک‌های برخاسته از خط‌مشی‌ها و رویه‌ها و نهایتاً ریسک‌های برخاسته از سیستم‌های اطلاعاتی، حائز رتبه‌های اول تا چهارم شده‌اند. در خصوص ریسک‌های فرعی زیر مجموعه این چهار ریسک نیز، در ادامه ریسک‌ها به ترتیب اولویت معرفی

شدند: عدم کنترل مناسب در صحت داده‌های ورودی، پردازش‌های درونی و صحت داده‌های خروجی؛ عدم آشنایی کامل و به‌روز متخصصین حوزه امنیت اطلاعات با ویروس‌ها، کرم‌ها، جاسوس افزارها و اسپم‌ها؛ نبود تعهد و حمایت برخی از مدیران ارشد به امنیت اطلاعات؛ آگاهی پایین کارکنان در حوزه امنیت اطلاعات؛ عدم توجه به زمان‌بندی پیاده‌سازی و اجرایی نمودن طرح‌های حوزه امنیت اطلاعات؛ کمبود نیروی‌های متخصص در زمینه امنیت اطلاعات؛ عدم تخصیص بودجه‌های مناسب به طرح‌های مربوط به امنیت اطلاعات؛ عدم بهره‌گیری از مشاورین برجسته در زمینه امنیت اطلاعات؛ عدم بازمهندسی دوره‌ای فرآیندهای حوزه امنیت اطلاعات؛ عدم ایجاد نسخه پشتیبان از برخی اطلاعات و یا نگهداری نامناسب از نسخه‌های پشتیبان؛ عدم وجود یک طرح جامع و فراگیر برای امنیت اطلاعات و سرمایه‌گذاری‌های مناسب و متناسب با اولویت‌های امنیتی؛ عدم وجود یک خط‌مشی امنیت اطلاعات جامع، کامل و قابل بازنگری؛ عدم وجود رویه‌ای مناسب در طبقه‌بندی و کدگذاری اطلاعات؛ عدم وجود رویه‌های مدیریت بحران در حوزه امنیت اطلاعات؛ عدم گزارش‌دهی مناسب رویدادها و ضعف‌های حوزه امنیت اطلاعات؛ سطح‌بندی نامناسب اطلاعات (جهت تعیین دسترسی‌ها و سلسله مراتب اطلاعاتی)؛ عدم وجود امنیت کافی در فرآیند تبادل اطلاعات و نرم‌افزارهای تخصصی واحدهای مختلف سازمان؛ عدم ثبات مدیران در حوزه امنیت اطلاعات؛ عدم ارائه آموزش‌های مناسب به کارکنان در حوزه امنیت اطلاعات؛ عدم مدیریت (شناسایی و رفع) ضعف‌های امنیت اطلاعات؛ عدم مستند سازی و آرشیوبندی کامل و صحیح فرآیندها، رویدادها و رویه‌ها در حوزه امنیت اطلاعات؛ عدم امنیت کامل سیستم اینترانت داخلی سازمان و احتمال نفوذ پذیری آن؛ عدم نظارت و پایش مناسب در توسعه نرم‌افزارهای برون سپاری شده حوزه‌های اطلاعاتی؛ عدم وجود اقدامات مناسب پیشگیرانه، اکتشافی و اصلاحی (به روزرسانی نرم‌افزارهای امنیتی) برای حفاظت از سیستم امنیت اطلاعات؛ عدم وجود امنیت در خدمات شبکه‌های اینترنتی مورد استفاده سازمان؛ شفاف نبودن تعریف مسئولیت امنیت اطلاعات؛ عدم انطباق سیستم‌ها با خط مشی‌ها و استانداردهای امنیت اطلاعات.

بر اساس نتایج حاصل از تحقیق حاضر و اطلاع از مهم‌ترین ریسک‌های تهدیدکننده امنیت اطلاعات در شرکت بهره‌برداری نفت و گاز آغاجاری، پیشنهاد می‌شود تعهد و حمایت مدیران ارشد نسبت به حوزه امنیت اطلاعات؛ از طریق کسب اطمینان جهت هم‌راستا کردن اهداف

و برنامه‌های امنیت با جهت‌گیری استراتژیک کل سازمان و مناسب بودن خط‌مشی امنیت برای کسب و کار تقویت شود و از بهبود مستمر امنیت اطلاعات اطمینان حاصل کنند. آگاهی‌های لازم به کارکنان در حوزه امنیت اطلاعات ارائه شود و بودجه‌های مناسب به طرح‌های مربوط به امنیت اطلاعات تخصیص یابد و یک طرح جامع برای امنیت اطلاعات و سرمایه‌گذاری‌های مناسب و متناسب با اولویت‌های امنیتی تدوین یابد.

References

Alavi, R., Shareeful, I., Haralambos, M. (2016). An information security risk-driven investment model for analysing human factors, *Information & Computer Security, Vol. 24* Issue: 2, pp.205-227.(in Persian)

Andrii. B (2019).Information systems for supply chain management: uncertainties, risks and cyber security, *Procedia Computer ScienceVolume* 1492019Pages 65-70.(in Persian)

Dashti, A. (2005). Security Standards, *Network Magazine*, No. 54, pp. 163-158. .(in Persian)

Evangelos D. Frangopoulos, P, Mariki M. Eloff, Lucas M. Venter. (2013). Psychosocial risks: Can their effects on the security of information systems really be ignored?, *Information Management & Computer Security, Vol. 21* Issue: 1, pp.53-65.

Gary Stoneburner, Alice Goguen, and Alexis Feringa. (2002). Risk Management Guide for Information Technology Systems, *National Institute of Standards and Technology, July*.

Hosseini, S. (2016). Reasons for Organizational Failure in Strategic Information Technology Planning, *Conference on Management and Humanities Research in Iran*, Tehran: Modbar Management Research Institute, University of Tehran .(in Persian)

Jiqiang, C., Witold, P., Litao, Ma., C, Wang. (2014). A new information security risk analysis method based on membership degree, *Kybernetes, Vol. 43*, Iss: 5, pp.686 – 698.

Keshtegar, AS; Kedri, T; Vazife, z. (2015). An Overview of the Outsourcing Risks of Information Technology Projects, *5th International Conference on Accounting and Management and 2nd Conference on Entrepreneurship and Open Innovation*, Tehran, Mehr Ishraq Conference.(in Persian)

Pipkin, D. L. (2000). Information security, new jersey: Prentice Hall.

Rahnamaii Zakavat, m. (2017). Application of data mining in big data management in the field of health information using CRISP-DM algorithm, *Annual Conference on New Management Paradigms in the field of intelligence*, Tehran, Permanent Conference Secretariat, University of Tehran.(in Persian)

Reyes, G, Jose, Gasco., Juan, Llopis. (2010). Information systems outsourcing reasons and risks: a new assessment, *Industrial Management & Data Systems, Vol. 110*, Iss: 2, pp.284 – 303.

Rezaei, Ali, Mossadegh, Mohammad Javad, Rezaei, Mona. (2018). Factors affecting the effectiveness of information security management system. *Quarterly Journal of Development and Transformation Management*, 1397 (33), 73-82.(in Persian)

Sayadi, A, Hayati, m; Azar, A (2011). Risk Assessment and Rating in Tunneling Projects Using Linear Allocation Method, *International Journal of Industrial Engineering and Production Management*, Volume 22, Number 1, pp. 28-28.(in Persian)

Yaqubi, N.; Jafari, H.; Shokohi, J. (2015). Identification and Ranking of Cloud Computing Risk Factors in Government Organizations, *Information Processing and Management*, Volume 30, Number 3, pp. 784-759.(in Persian)

Yousefi Zenooz, R.; Hassanpour, A.; Mousavi, P. (2015). Presenting a model for prioritizing organizational information security risks using fuzzy AHP and Bayesian network in the banking industry, *Quarterly Journal of Industrial Management Studies*, Volume 13, Number 37, pp. 185-161.(in Persian)

Zandiyan, F, Gharavi, A, Hassanzadeh, M. (2018). Identifying the impact of human factors on information security in the Department of Education. Scientific. *Journal of Information Management*, 4 (2), 110-128.(in Persian) Zargari, K. (2017). The Impact of Internal Organizational Factors on the Efficiency of Human Resource Management Information Systems in Banks of Guilan Province, *2nd International Conference on Management and Accounting*, Tehran, Salehan Institute of Higher Education.(in Persian)