Journal of Information Technology Management
ISSN: 2008-5893
EISSN: 2423-5059
Vol. 9, No. 4; PP. 851-870
Winter 2018
DOI: 10.22059/jitm.2017.239211.2127

University of Tehran
Faculty of Management

Identifying the Effective Components of Information Security Management in Information Technology of Iranian Offshore Oil Company

Yaser Seif [1], Nahid Naderi beni [2]

Abstract: Security problems and barriers are one of the most fundamental issues in information systems. Security has long been regarded as an integral part of IT infrastructure. In this regard, the present research aimed to identify the effective components of information security management in Iran's Offshore Oil Company Information Technology. The population of this research includes Iran's Offshore Oil Company IT managers and experts. The research is considered as mixed method in nature. In the qualitative section, the effectiveness components were identified using semi-structured interviews. Then these identified components were developed in the form of a secondary questionnaire and proposed to the population so the necessary data were collected. Data analysis was performed using SPSS20 and Lisrel software. The results of the research showed the components related to technical human, managerial, leadership, financial and economic issues, components related to management and leadership issues affecting information security management of information technology department of Iran's offshore oil company.

Key words: ***Human factors, Information security management, Information technology, Iranian offshore oil company, Management factors.***

1. MSc. Student in IT, Faculty of Management and Accounting, Farabi Campus, Qom, Iran

2. Assistant Prof. Faculty of Management and Accounting, Farabi Campus, Qom, Iran

Submitted: 18 / September / 2016
Accepted: 06 / December / 2017
Corresponding Author: Nahid Naderibani
Email: n.naderi.b@ut.ac.ir

مدیریت فناوری اطلاعات
دانشکدهٔ مدیریت دانشگاه تهران
دورهٔ ۹، شمارهٔ ۴
زمستان ۱۳۹۶
صص. ۸۷۰- ۸۵۱

Journal of Information Technology Management
DOI: 10.22059/jitm.2017.239211.2127

شناسایی مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قارهٔ ایران

یاسر سیف[۱]، ناهید نادری بنی[۲]

چکیده: مشکلات و موانع امنیتی یکی از اساسی‌ترین موضوعات مطرح در زمینهٔ سیستم‌های اطلاعاتی است. از دیرباز، امنیت یکی از اجزای اصلی زیرساخت‌های فناوری اطلاعات شمرده می‌شد. در این رابطه، پژوهش حاضر با هدف شناسایی مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قارهٔ ایران انجام شده است. جامعهٔ آماری پژوهش، مدیران و کارشناسان واحد فناوری اطلاعات شرکت نفت فلات قارهٔ ایران هستند. پژوهش به‌صورت روش آمیختهٔ کیفی ـ کمی انجام شده است. در بخش کیفی با مصاحبهٔ نیمه ساختاریافته، مؤلفه‌های مؤثر شناسایی شدند و در بخش کمی، مؤلفه‌های مؤثر شناسایی شده در قالب پرسشنامهٔ دومی تدوین شد و در اختیار جامعهٔ آماری قرار گرفت و داده‌های لازم برای بررسی سؤالات پژوهش به‌دست آمد. تجزیه و تحلیل داده‌ها با استفاده از نرم‌افزارهای Lisrel و نسخهٔ SPSS ۲۰ انجام گرفت. بر اساس نتایج پژوهش، مؤلفه‌های مرتبط با مسائل فنی، انسانی، مدیریت و رهبری و نیز، مالی و اقتصادی مؤثر بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قاره ایران مشخص شدند.

واژه‌های کلیدی: شرکت نفت فلات قارهٔ ایران، عوامل انسانی، عوامل مدیریتی، فناوری اطلاعات، مدیریت امنیت اطلاعات.

۱. دانشجوی کارشناسی ارشد IT، دانشکدهٔ مدیریت و حسابداری، پردیس فارابی، دانشگاه تهران، قم، ایران
۲. استادیار گروه مدیریت، دانشکدهٔ مدیریت و حسابداری پردیس فارابی، دانشگاه تهران، قم، ایران

تاریخ دریافت مقاله: ۱۳۹۵/۰۵/۱۳
تاریخ پذیرش نهایی مقاله: ۱۳۹۶/۰۹/۱۵
نویسندهٔ مسئول مقاله: ناهید نادری بنی
E-mail: n.naderi.b@ut.ac.ir

مقدمه

امروزه با توجه به توسعه و تنوع محصولات و خدمات سازمان‌ها و نیز، رقابت شدید میان آنها، سازمان‌ها در حال تحول و دگرگونی هستند و موفقیت نهایی و حتی بقای سازمان‌ها به توانایی آنها در جذب و به‌کارگیری اطلاعات و دانش فناوری‌های جدید وابسته است تا بتوانند نوعی مزیت در سازمان خلق کنند؛ بنابراین، سازمان‌ها به‌دنبال ایجاد و مدیریت مناسب سیستم‌های اطلاعات هستند تا اطلاعات و دانش فناوری‌های جدید را به‌موقع کسب و منتشر کرده، از آن به نحو بهینه استفاده کنند (رمضانیان و بساق‌زاده، ۱۳۹۱).

سیستم‌های اطلاعاتی و کاربردی سازمان، سیستم‌های پیچیده‌ای هستند که معمولاً بسیاری از عملیات درون سازمان را پوشش می‌دهند. از آنجا که معمولاً سازمان به این‌گونه سیستم‌ها وابستگی زیادی دارد، هر نوع عاملی که موجب اختلال در عملکرد آنها شود، می‌تواند صدمات سنگین و جبران‌ناپذیری به سازمان وارد کند. مشکل امنیت در سیستم‌های اطلاعاتی مسئلهٔ عمومی است و به‌دلیل کاربرد وسیع سیستم‌های اطلاعاتی و کاربردی سازمان، مقولهٔ امنیت در این سیستم‌ها اهمیت زیادی دارد. هدف از این پژوهش، بررسی و سنجش مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت مجتمع نفت فلات قاره‌ای است (زنجیرچی، مروتی شریف‌آبادی و شاه‌حسینی بیده، ۱۳۹۳).

امنیت اطلاعات یک مسئلهٔ حیاتی است و امروزه سازمان‌ها در سراسر دنیا با آن روبه‌رو هستند. امنیت سیستم‌های اطلاعاتی، هم فناوری و هم افراد را دربرمی‌گیرد. در بیشتر تحقیقاتی که در زمینهٔ امنیت سیستم‌های اطلاعاتی صورت گرفته، نوعی دید و رویکرد فنی در آن به چشم می‌خورد (زنجیرچی و همکاران، ۱۳۹۳).

شرکت ملی پالایش و پخش معتقد به استفاده از فناوری اطلاعات و ارتباطات، به‌عنوان یک ابزار اصلی مدیریتی و تصمیم‌سازی برای نیل به اهداف بلندمدت و به‌کارگیری فناوری اطلاعات و ارتباطات در عملیات روزانهٔ تولید، پالایش و توزیع است. این مدیریت با توجه به دانش و تجربهٔ نیروی انسانی متخصص خود، آمادهٔ اجرای پروژه‌های نوین مبتنی بر فناوری اطلاعات به‌منظور بسط و توسعهٔ کسب‌وکار شرکت، در راستای ایجاد دولت الکترونیک است (سایت شرکت ملی پالایش و پخش فراورده های نفتی، ۱۳۹۶).

به عقیدهٔ نگارندگان، گروه‌های مختلفی در استفاده از فناوری‌های اطلاعات در صنعت نفت مؤثرند. این گروه‌ها عبارت‌اند از: دولت با اعمال ضوابط و سیاست‌ها، استفاده‌کنندگان تجاری با ارائهٔ نیازهای سطوح قابل تقاضا؛ تولیدکنندگان فناوری اطلاعات با ارائهٔ فناوری و تعیین سطوح

قابل قبول؛ تأمین‌کنندگان با شبکه‌سازی و مجتمع‌سازی سازگار؛ مصرف‌کنندگان با انتظارات و عملکردشان؛ رقبا با ارائهٔ محصولات جدید در بازارهای تازه و کارمندان صنعت نفت.

مشکلی که صنعت نفت ایران با آن روبه‌روست، بسیار حیاتی و حساس است. این مشکل در واقع امنیت اطلاعات در برابر حملات سایبری و فضای اطلاعات حساس است که در دنیا رقبای بسیار زیادی دارد. بنابراین در این پژوهش مسائلی همچون بررسی وضعیت امنیت اطلاعات در این مجتمع و همچنین مشکلات امنیتی سیستم‌های اطلاعاتی موجود در شرکت نفت فلات قاره بررسی می‌شود. به بیانی، در این پژوهش به شناسایی عوامل کلیدی مؤثر بر امنیت اطلاعات در این مجتمع پرداخته می‌شود که در این زمینه از نظر خبرگان متخصص و آگاه در این مجتمع استفاده خواهد شد.

سؤالات اصلی پژوهش به قرار زیر است:

- مؤلفه‌های مرتبط با مسائل فنی مؤثر بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قارهٔ ایران کدام‌اند؟
- مؤلفه‌های مرتبط با مسائل انسانی مؤثر بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قارهٔ ایران کدام‌اند؟
- مؤلفه‌های مرتبط با مسائل مدیریت و رهبری مؤثر بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قارهٔ ایران کدام‌اند؟
- مؤلفه‌های مرتبط با مسائل مالی و اقتصادی مؤثر بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قارهٔ ایران کدام‌اند؟

پیشینهٔ پژوهش

امنیت اطلاعات مسئله‌ای است که سازمان‌ها را در سراسر دنیا تهدید می‌کند. با توجه به اینکه اقتصادها و کسب‌وکارهای مدرن برای بقا به‌طور کامل به فناوری اطلاعات وابسته‌اند، نیاز به حفاظت از اطلاعات از قبل بیشتر شده است. اکنون در سراسر جهان اطلاعات الکترونیکی شده و فناوری نیز به‌طور مداوم تغییر می‌کند. از آنجا که کمابیش تمام جنبه‌های زندگی ما به‌وسیلهٔ ابزارها، رویه‌ها و فرایندهای فناوری تحت کنترل قرار گرفته است، این مورد اهمیتی فزاینده می‌یابد که در کنار مزیت‌های گستردهٔ فناوری‌های الکترونیک، ضعف‌ها و موارد مجرمانهٔ آنها را بشناسیم و در سیستم‌های اطلاعات الکترونیکی لحاظ کنیم (وولف و وولف، ۲۰۰۳). امروزه در بیشتر سازمان‌ها اطلاعات کسب‌وکار نقش بسیار مهمی دارد و تلاش برای حفاظت از این اطلاعات از اهمیت شایان توجهی برخوردار است. اطلاعات یکی از مهم‌ترین دارایی‌های هر سازمان محسوب می‌شود و

به‌دلیل ارزش زیاد و حیاتی آن برای هر سازمان، باید از آن به خوبی محافظت شود. این اهمیت تا جایی است که عده‌ای آن را به خونی در رگ‌های سازمان تشبیه کرده و آن را عامل حیاتبخش سازمان می‌دانند (مسکل و همکاران، ۲۰۱۵) که با به خطر افتادن این جریان، سازمان می‌میرد. اهمیت‌دادن به اطلاعات برای سازمان ضمن داشتن مزیت‌های بسیار، در موفقیت سازمان در عرصه‌هایی چون جریان نقدینگی و ارزش بازار، نیز سهم عمده‌ای دارد. همچنین اطلاعات عاملی است که موجب پیوند سایر منابع سازمان می‌شود (کوزیکاس، ۲۰۱۶).

به‌طور سنتی محققان برای نشان‌دادن ریسک‌های مؤثر بر این اطلاعات، به زیرساخت فناوری اطلاعات توجه کرده‌اند و دلیل آن، اهمیت فناوری اطلاعات در ذخیرهٔ پردازش و انتقال دارایی‌های اطلاعاتی باارزش است. به هر حال باید در نظر داشت طی سال‌های اخیر مسلم شده است که امنیت اطلاعات دیگر یک موضوع فنی نیست، بلکه مسئله‌ای مدیریتی محسوب می‌شود و ابعاد دیگری مانند مباحث راهبردی و قانونی را نیز دربرمی‌گیرد (بیرمان، ۲۰۰۰).

دو عامل دیگر در اهمیت مدیریت امنیت اطلاعات، شبکه‌های جهانی و تجارت الکترونیکی است. با اشاعهٔ اینترنت و جهانی‌شدن آن، زندگی روزمرهٔ ما دچار تغییر شده و سازمان‌های مدرن از اینترنت برای عملیات کسب‌وکار خود استفاده می‌کنند و به آن وابسته شده‌اند. بر این اساس، تجارت الکترونیکی رواج یافته و موجب تغییر فرایندهای کسب‌وکار سازمان‌ها شده است. این وابستگی به کسب‌وکارهای الکترونیکی نیز، ضرورت حفاظت از اطلاعات را مطرح کرده و رویکردهای گوناگونی را برای مدیریت امنیت اطلاعات به‌وجود آورده است (زوکاتو، ۲۰۰۷).

اغلب سازمان‌ها در معرض انواع تهدیدهای داخلی و خارجی خرابکاران اطلاعاتی قرار می‌گیرند؛ تهدیدهایی همچون دستکاری اطلاعات مرجع، سرقت اطلاعات حیاتی و سرمایه‌های اطلاعاتی. در چنین وضعیتی، عواملی که جزء مزیت‌های سیستم به‌شمار می‌روند (مثل سرعت و قابلیت دسترسی زیاد)، اگر تحت کنترل نباشند، ممکن است باعث بروز آسیب‌پذیری شوند و سوءاستفادهٔ افراد از آنها به نفوذ، خرابکاری و کلاهبرداری بینجامد. علاوه‌بر این، چنانچه روند صحیحی برای حفاظت از اطلاعات وجود نداشته باشد، مشکلات طبیعی و خطاهای غیرعمدی توسط کاربران رایانه‌ای، می‌تواند نتایج مخربی به بار آورد. بنابراین ضرورت توجه به «امنیت اطلاعات» و «مدیریت امنیت اطلاعات» بیش از پیش احساس می‌شود (پاساری و سونار، ۲۰۱۲).

تاکنون بیشتر تحقیقاتی که در زمینهٔ امنیت سیستم‌های اطلاعاتی انجام شده، در زمینهٔ مسائل فنی و تکنیکی بوده و تحقیقات و تمرین‌های تحقیقاتی از دید مسائل فنی به امنیت اطلاعات نگریسته‌اند. همان‌طور که بلونه، باسکوئیت و رود ریگز (۲۰۰۸) بیان کرده است، در بیشتر تحقیقاتی که در زمینهٔ امنیت اطلاعات صورت‌گرفته، یک نوع دید و رویکرد فنی وجود دارد و متخصصان امنیت اطلاعات برای برطرف‌کردن مشکلات امنیتی بیشتر به‌دنبال یک سری ابزارهای فنی مانند

آنتی‌ویروس‌ها، فایروال‌ها و... بوده‌اند. بـه هـر حـال، بـه‌گفتـهٔ تامسـون و نیکـرک (۲۰۱۲)، امنیـت اطلاعات هم فناوری و هم فرد را دربرمی‌گیرد، اما بیشتر سازمان‌ها راه‌حل‌های فنی را جواب فـوری به مشکلات امنیتی خود می‌دانند، در حالی که موانع زیادی برای رویکرد فنی وجود دارد. در یکـی از تحقیقات (بهاتاچاریا، ۲۰۱۱)، عامل انسانی به‌عنوان پاشنهٔ آشیل امنیت اطلاعات معرفی شده اسـت. مدیر شرکت IBM بیان کرد در سال ۲۰۰۹، نه‌تنها حمله بـه سیسـتم‌هـای اطلاعـاتی سـازمان‌هـا کوچک‌تر، متمرکزتر و پنهان‌کارانه‌تر می‌شود، بلکه نفوذگران «سهل‌انگاری و ساده‌اندیشی کاربران» را در کانون توجه قرار می‌دهند. به‌گفتهٔ رئیس بخش آگاهی شرکت کـامپیوتری آرمونـگ، «کـاربر» همچنان به‌عنوان سست ترین عنصر آسیب پذیر در مسئلهٔ امنیتی اطلاعات، مورد سوء اسـتفاده قـرار خواهد گرفت. امروزه به نظر می رسد، موفقیت امنیت اطلاعات تـا حـد زیـادی بـه رفتـار اثـربخش کاربران وابسته است. رفتارهای درست و سازندهٔ کاربران، مدیران سیستم و افـراد دیگـر، مـی‌توانـد اثربخشی امنیت اطلاعات را تا حد زیادی افزایش دهد؛ در حالی که رفتارهای نادرست و مخرب، در واقع مانع اثربخشی آن می‌شود (هاگن، آلبرچسن و جونسن، ۲۰۱۱).

خیرگو و شکوهی (۱۳۹۶)، در پژوهشی با عنوان «شناسایی و رتبه‌بندی عوامل کلیدی مـؤثر بـر اثربخشی سیستم‌های اطلاعاتی در سازمان‌هـای دولتـی» بیـان کردنـد کـه امـروزه سیسـتم‌هـای اطلاعاتی از عوامل مؤثر در دستیابی به مزیت رقابتی برای سازمان‌ها محسوب مـی‌شـوند؛ چـرا کـه کیفیت خروجی این سیستم‌ها نقش مهمـی در بهبـود عملکـرد سـازمان دارد. نتـایج پـژوهش آنهـا نشان‌دهندهٔ تأثیر مثبت عوامل سازمانی، عوامل انسانی و فنی بر اثربخشی سیسـتم‌هـای اطلاعـاتی است. همچنین، از بین شاخص‌های مؤثر بر اثربخشی سیستم‌های اطلاعاتی، حمایـت مـدیر ارشـد، امنیت، پذیرش و مدیریت دانش فناوری اطلاعات و سیستم‌هـای اطلاعـاتی، بـه‌ترتیـب رتبـه‌هـای نخست را به خود اختصاص داده‌اند.

نجاتی و حقیقت منفرد و رمضان (۱۳۹۳)، در پژوهشـی بـا عنـوان «شناسـایی و اولویـت‌بنـدی عوامل مؤثر بر استقرار سیسـتم مـدیریت امنیـت اطلاعـات (مـورد مطالعـه: ادارات مرکـزی بانـک کشاورزی در شهر تهران)»، بیان کردند که اطلاعات برای تمام سازمان‌ها دارایی با ارزشی محسوب می‌شود؛ بنابراین حفاظت از این دارایی به‌ویژه در عصر ارتباطـات الکترونیـک، بسـیار حـائز اهمیـت است. نتایج پژوهش ایشان حاکی از تأثیر مثبت عوامل یاد شده بر استقرار موفـق سیسـتم مـدیریت امنیت اطلاعات است و تمام فرضیه‌های پژوهش آنهـا تأییـد شـدند. بیشـترین اولویـت در اسـتقرار سیستم مدیریت امنیت اطلاعات به عامل کنترل با تأثیر ۶۷ درصد اختصاص داشت.

زنجیرچی و همکارانش (۱۳۹۳)، در پژوهشی با عنوان «شناسایی و اولویت‌بندی عوامل انسـانی مؤثر بر امنیت اطلاعات با استفاده از رویکرد ترکیبی ANP و DEMATEL فـازی» بیـان کردنـد که امروزه امنیت اطلاعات مسئله‌ای حیاتی بوده و موفقیت سازمان‌ها در سراسر دنیا بـه آن وابسـته

است. امنیت سیستم‌های اطلاعاتی هم فناوری و هم افراد (عوامل انسانی) را دربرمی‌گیرد. بر اساس نتایج آنان، پنج شاخص اصلی عبارت‌اند از: ۱. اشاعه و استفاده از اطلاعات محرمانه (امنیتی)؛ ۲. سوءاستفاده از سیستم اطلاعات (سوءاستفادهٔ عمدی کارمندان داخلی از منابع IS)؛ ۳. آگاهی از اهمیت و ضرورت پیروی از قوانین و اجرای فعالیت‌های امنیتی؛ ۴. استفاده از ابزارهای آموزشی متنوع برای آموزش فعالیت‌های مرتبط با امنیت سیستم‌های اطلاعاتی؛ ۵. تعهد و وفاداری کارمندان به سازمان و حفظ اطلاعات.

بررسی تحقیقات پیشین نشان می‌دهد که تحقیقات زیادی در خصوص شناسایی عوامل مؤثر بر امنیت اطلاعات در شرکت نفت انجام نگرفته و تحقیقات انجام شده نیز بیشتر بر تخلفات عمدی و سهوی کاربران، یعنی نیروی انسانی تأکید بیشتری داشته‌اند. هچنین مؤلفه‌های مدیریتی از قبیل ارائهٔ اطلاعات لازم در زمینهٔ اهمیت و امنیت اطلاعات در سازمان، جزء مؤلفه‌ها و عوامل مؤثر بر امنیت اطلاعات در تحقیقات قبلی است. آموزش و برگزاری سمینارهای توجیهی برای کارکنان در زمینهٔ امنیت و سرقت اطلاعات، یکی دیگر از مؤلفه‌های تأثیرگذار بررسی شده است.

روش‌شناسی پژوهش

این پژوهش از لحاظ هدف یا جهت‌گیری، کاربردی است و از لحاظ اجرا یا راهبرد، از دسته پژوهش‌های توصیفی از نوع روش مطالعهٔ موردی آمیخته به‌شمار می‌رود. این پژوهش دو دسته جامعهٔ آماری دارد:

۱. جامعهٔ آماری در بخش کیفی: خبرگان فناوری اطلاعات و مدیریت امنیت اطلاعات که نسبت به موضوع پژوهش آگاهی داشتند. تعداد خبرگان در مجموع ۴۵ نفر بود که با همهٔ این افراد مصاحبه شد (اشباع). معیار انتخاب خبرگان، حداقل ۱۰ سال سابقهٔ کار در بخش فناوری اطلاعات یا مدیریت امنیت اطلاعات شرکت نفت بود.
۲. جامعهٔ آماری در بخش کمی: کارشناسان فناوری اطلاعات و مدیران ارشد مرتبط با مدیریت امنیت اطلاعات در نفت فلات قاره که با استفاده از فرمول کوکران ۱۲۶ نفر برای نمونه انتخاب شدند.

ابزار گردآوری اطلاعات در بخش کیفی پژوهش، مصاحبهٔ نیمه ساختاریافته و در بخش کمی پرسشنامهٔ محقق ساخته است. برای تجزیه و تحلیل داده‌ها در بخش کیفی، از روش تحلیل محتوا و در بخش کمی از تحلیل عامل تأییدی استفاده شده است. به‌منظور شناسایی مؤلفه‌های مؤثر بر امنیت اطلاعات، با مطالعهٔ مبانی و ادبیات نظری پژوهش و بررسی پژوهش‌های پیشین، مؤلفه‌های مد نظر استخراج شدند و با توجه به این مؤلفه‌ها سؤال‌های مصاحبه طراحی گردید. در

مرحلهٔ مصاحبه یا بخش کیفی، مؤلفه‌های انتخاب شده با توجه به نظر خبرگان دسته‌بندی شدند و میزان اهمیت و تأثیر آنها بر امنیت اطلاعات، مشخص شد. در نهایت مقوله‌های شناسایی شده در قالب پرسشنامهٔ دیگری طراحی شد و در اختیار جامعهٔ آماری قرار گرفت. پرسشنامهٔ محقق‌ساخته متشکل از نتایج مرحلهٔ کیفی بود. برای بررسی روایی پرسشنامه از روش تحلیل محتوا استفاده شد؛ بدین ترتیب که سؤال‌ها در اختیار ۵ نفر از استادان فن و مدیران شرکت نفت فلات قاره قرار گرفت و پس از بازبینی‌های مکرر، پرسشنامهٔ نهایی تهیه شد. همچنین از آزمون بارتلت برای بررسی روایی گویه‌های پرسشنامه استفاده شد که نتایج نشان‌دهندهٔ روایی همهٔ گویه‌های پرسشنامه بود. برای بررسی پایایی پرسشنامه نیز از آزمون آلفای کرونباخ استفاده شد. بر اساس نتایج آزمون آلفای کرونباخ، مقدار این ضریب ۰/۸۲۱ به‌دست آمد که چون از مقدار آستانهٔ ۰/۷ بیشتر است، می‌توان گفت پرسشنامه پایایی مناسبی دارد.

برای تجزیه و تحلیل داده‌ها در بخش کیفی از تجزیه و تحلیل تم و در بخش کمی، از تحلیل اکتشافی و تحلیل عامل تأییدی استفاده شده است.

یافته‌های پژوهش

در این بخش، از گزاره‌های بیان شده در مصاحبه با استادان، مدیران صنعتی و خبرگان صنعت، جدول‌هایی تهیه شده است که چگونگی دستیابی به نتایج این مصاحبه‌ها را نشان می‌دهد. با تهیهٔ نسخه‌های کتبی از محتوای مصاحبه‌ها و پاسخ افراد به سؤال‌های مصاحبه، داده‌های کیفی پژوهش براساس شمارهٔ سؤال مرتب شدند و پاسخ هر خبره به هر سؤال در کنار هم نوشته شد. پس از مطالعهٔ صحبت‌های مصاحبه‌شوندگان و تحلیل کیفی آنها، برای خلق معنا از جدول‌های به‌دست آمده، همهٔ آنها در قالب یک جدول یکپارچه قرار گرفتند و بعد از منظم کردن آنها بر اساس کد تعیین شده، به جمله‌های مربوط به یک کد با توجه به مفاهیم آنها و اشتراکشان، عنوانی تعلق گرفت.

در این مرحله با مرور چندبارهٔ داده‌های گردآوری شده از طریق مصاحبه، به بررسی زوایای مختلف آن پرداخته شد. در واقع با مرور مجموعه داده‌های گردآوری شده، مفاهیم مستتر در داده‌های جمع‌آوری شده، بازیابی شدند. در این مرحله بدون هیچ‌گونه محدودیتی به نام‌گذاری مفاهیم پرداخته شد. بعد از انجام کدگذاری باز، محورهای اصلی در مجموعه داده‌ها مشخص شدند؛ سپس در مرحلهٔ بعدی، کدگذاری حول این محورها انجام گرفت. نتایج تحلیل داده‌ها در بخش کیفی، به شناسایی مؤلفه‌های مؤثر بر امنیت اطلاعات در چهار بخش مؤلفه‌های مربوط به عامل مدیریت و رهبری، عامل فنی، عامل نیروی انسانی و عامل مالی و اقتصادی منجر شد.

جدول ۱. کدگذاری داده‌ها بر اساس نتایج مصاحبه دربارهٔ عوامل مؤثر بر مدیریت امنیت اطلاعات

کد محوری	کد باز	گزارهٔ کلامی	کد مصاحبه‌شوندگان
مؤلفه‌های مرتبط با مسائل فنی	یکپارچگی سیستم‌های نرم‌افزاری	یکپارچگی سیستم‌های نرم‌افزاری در مدیریت امنیت اطلاعات تأثیرگذارند.	I4, I5, I8, I10
	استفاده از نرم‌افزارها و سخت‌افزارهای به‌روز	استفاده از نرم‌افزارها و سخت‌افزارهای به‌روز عامل مهمی در امنیت اطلاعات است.	I3, I5, I6, I7
	مانیتورینگ و نظارت بر لاگ‌های سیستم‌های نرم‌افزاری	مانیتورینگ و نظارت بر لاگ‌های سیستم‌های نرم‌افزاری عامل مهمی در امنیت اطلاعات است.	I1, I2, I4
	نوع سیستم عامل استفاده شده	نوع سیستم عامل استفاده شده عامل مهمی در امنیت اطلاعات است.	I1, I3, I6
	کاربرد بسته‌های نرم‌افزاری متنوع	کاربرد بسته‌های نرم‌افزاری متنوع عامل مهمی در امنیت اطلاعات است.	I2, I4, I8
	امنیت محیط فیزیکی منابع اطلاعاتی	امنیت محیط فیزیکی منابع اطلاعاتی عامل مهمی در امنیت اطلاعات است.	I2, I3, I5
	تأثیر زیرساخت‌های IT کشور	تأثیر زیرساخت‌های IT کشور عامل مهمی در امنیت اطلاعات است.	I5, I6, I2
	استفاده از مارک‌های شناخته‌شدهٔ تجاری	استفاده از مارک‌های شناخته شدهٔ تجاری سخت‌افزاری و نرم‌افزاری عامل مهمی در امنیت اطلاعات است.	I6, I7
	گرفتن نسخهٔ پشتیبان (Backup) از اطلاعات	گرفتن نسخهٔ پشتیبان (Backup) از اطلاعات مهم عامل مهمی در امنیت اطلاعات است.	I4, I5, I8, I10
	پیاده‌سازی سازوکارهای تصدیق هویت و مجوزدهی	پیاده‌سازی سازوکارهای تصدیق هویت و مجوزدهی عامل مهمی در امنیت اطلاعات است.	I2, I4, I6, I9
	پایش به‌منظور عدم پردازش غیرمجاز اطلاعات (Monitoring)	پایش به‌منظور عدم پردازش غیرمجاز اطلاعات (Monitoring) عامل مهمی در امنیت اطلاعات است.	I3, I5, I6,I9
	مستندسازی و حفظ رخدادهای امنیت اطلاعات	مستندسازی و حفظ رخدادهای امنیت اطلاعات عامل مهمی در امنیت اطلاعات است.	I1, I11, I12
	پیاده‌سازی کنترل‌های خاص تبادل آنلاین	پیاده‌سازی کنترل‌های خاص تبادل آنلاین، کار از راه دور و دسترسی عمومی، عامل مهمی در امنیت اطلاعات است.	I12, I14, I18
	رعایت استانداردهای امنیتی	رعایت استانداردهای امنیتی، تدوین نیازهای امنیتی و معیارهای پذیرش امنیتی سیستم‌های اطلاعاتی، عامل مهمی در امنیت اطلاعات است.	I14, I25, I28, I30
	شناسایی و طبقه‌بندی اطلاعات و پیاده‌سازی کنترل دسترسی	شناسایی و طبقه‌بندی اطلاعات و کاربران و پیاده‌سازی کنترل دسترسی عامل مهمی در امنیت اطلاعات است.	I31, I35, I36, I37
	رمزنگاری اطلاعات محرمانه و با ارزش	رمزنگاری اطلاعات محرمانه و با ارزش عامل مهمی در امنیت اطلاعات است.	I21, I22, I24

ادامهٔ جدول ۱

کد محوری	کد باز	گزارهٔ کلامی	کد مصاحبه‌شوندگان
مؤلفه‌های مرتبط با مسائل فنی	نصب سیستم شناساگر متجاوز (IDS) و دیوار آتش	نصب سیستم شناساگر متجاوز (IDS) و دیوار آتش برای جلوگیری از نفوذ غیرمجاز عامل مهمی در امنیت اطلاعات است.	I21, I33, I36
	وجود دیتا سنتر	وجود دیتا سنتر عامل مهمی در امنیت اطلاعات است.	I32, I34, I38
	توپولوژی و آرایش بستر شبکه	توپولوژی و آرایش بستر شبکه عامل مهمی در امنیت اطلاعات است.	I24, I25, I26, I32
مؤلفه‌های مرتبط با مسائل مدیریتی	همراهی مدیریت ارشد سازمان	همراهی مدیریت ارشد سازمان بر کیفیت مدیریت امنیت اطلاعات تأثیرگذار است.	I4, I5, I8, I10
	همراستایی خطمشی امنیت اطلاعات با برنامه‌ریزی راهبردی و خطمشی IT	همراستایی خطمشی امنیت اطلاعات با برنامه‌ریزی راهبردی و خطمشی IT عامل مهمی در امنیت اطلاعات است.	I1, I4, I7
	پیاده‌سازی و وجود سیستم مدیریت یکپارچه (IMS)	پیاده‌سازی و وجود سیستم مدیریت یکپارچه (IMS) در سازمان عامل مهمی در امنیت اطلاعات است.	I2, I6, I9
	مشاوره و ممیزی استانداردهای امنیت	مشاوره و ممیزی استانداردهای امنیت بر مدیریت امنیت اطلاعات تأثیرگذار است.	I3, I5, I6, I7
	تعریف چشم‌انداز، اهداف، مرزها و خطمشی مدیریت امنیت اطلاعات	تعریف چشم‌انداز، اهداف، مرزها و خطمشی مدیریت امنیت اطلاعات عامل مهمی در امنیت اطلاعات است.	I1, I2, I4
	تعیین معماری امنیت اطلاعات سازمان	تعیین معماری امنیت اطلاعات سازمان عامل مهمی در امنیت اطلاعات است.	I14, I25, I28, I33
	نحوهٔ ارتباط با رقبا و شرکای تجاری	نحوهٔ ارتباط با رقبا و شرکای تجاری عامل مهمی در امنیت اطلاعات است.	I12, I14, I16, I19
	استقرار سیستم‌های نظارت و پایش و گزارش‌های دوره‌ای	استقرار سیستم‌های نظارت و پایش و گزارشات روزانه، هفتگی و ماهانه عامل مهمی در امنیت اطلاعات است.	I3, I5, I6,I9
	میزان تأکید و علاقه مدیریت به پیگیری مسائل امنیت اطلاعات	تأکید و علاقهٔ مدیریت به پیگیری مسائل امنیت اطلاعات عامل مهمی در امنیت اطلاعات است.	I1, I11, I12
	اقدام مؤثر مدیریت در برابر نقض موارد امنیت اطلاعات	نقش اقدام مؤثر و مناسب مدیریت در برابر نقض موارد امنیت اطلاعات عامل مهمی در امنیت اطلاعات است.	I4, I5, I8, I10
	نقش اختیار و استقلال مدیریت در پیشبرد مدیریت امنیت اطلاعات	نقش اختیار و استقلال مدیریت در پیشبرد مدیریت امنیت اطلاعات عامل مهمی در امنیت اطلاعات است.	I2, I4, I6, I9
	پیاده‌سازی استانداردهای مدیریت امنیت اطلاعات نظیر ISMS یا ISO 27001	پیاده‌سازی استانداردهای مدیریت امنیت اطلاعات نظیر ISMS یا ISO 27001 عامل مهمی در امنیت اطلاعات است.	I3, I5, I6,I9
	وجود سیستم مدیریت منابع سازمان (ERP)	وجود سیستم مدیریت جامع منابع (ERP) در سازمان عامل مهمی در امنیت اطلاعات است.	I1, I11, I12

ادامهٔ جدول ۱

کد محوری	کد باز	گزاره کلامی	کد مصاحبه‌شوندگان
نقش نیروی انسانی در مدیریت امنیت اطلاعات	تدوین خط‌مشی آموزش امنیت اطلاعات نیروی انسانی	تدوین خط‌مشی آموزش امنیت اطلاعات نیروی انسانی عامل مهمی در امنیت اطلاعات است.	I4, I5, I8, I10
	ارزیابی توانایی کارکنان در حفظ امنیت اطلاعات سازمان	ارزیابی توانایی کارکنان واحد امنیت اطلاعات در حفظ امنیت اطلاعات سازمان عامل مهمی است.	I5, I6, I7
	آگاهی‌بخشی و آموزش امنیتی کارکنان پیش و حین استخدام	آگاهی‌بخشی و آموزش امنیتی کارکنان پیش و حین استخدام عامل مهمی در امنیت اطلاعات است.	I3, I5, I6, I7
	تلاش برای حفظ وفاداری و تعهد و ایجاد انگیزش در کارکنان سازمان	تلاش برای حفظ وفاداری و تعهد و ایجاد انگیزش در کارکنان سازمان عامل مهمی در امنیت اطلاعات است.	I5, I6, I7, I8, I10
	اجرای اقدامات امنیتی مناسب هنگام تغییر پست یا ترک خدمت کارکنان	اجرای اقدامات امنیتی مناسب هنگام تغییر پست یا ترک خدمت کارکنان عامل مهمی در امنیت اطلاعات است.	I5, I8, I1
نقش مسائل اقتصادی و مالی در مدیریت امنیت اطلاعات	انگیزه و وفاداری و رضایت نیروی انسانی	نقش انگیزه و وفاداری و رضایت نیروی انسانی عامل مهمی در امنیت اطلاعات است.	I1, I2, I4
	وجود فرهنگ امنیت اطلاعات	وجود فرهنگ امنیت اطلاعات عامل مهمی در امنیت اطلاعات است.	I5, I7, I9
	وجود سیستم مبتنی بر تشویق و تنبیه کارکنان	وجود سیستم مبتنی بر تشویق و تنبیه کارکنان عامل مهمی در امنیت اطلاعات است.	I1, I2, I4
	میزان بودجهٔ سازمان	میزان بودجهٔ سازمان عامل مهمی در امنیت اطلاعات است.	I4, I5, I8, I10
	منفعت‌سنجی اقدامات امنیتی و بودجهٔ لازم برای آنها پیش از اجرا	منفعت‌سنجی اقدامات امنیتی و بودجهٔ لازم برای آنها پیش از اجرا عامل مهمی در امنیت اطلاعات است.	I3, I5, I6, I7
	تأمین بودجه برای استخدام و به‌کارگیری متخصصان و مشاوران	تأمین بودجه برای استخدام و به‌کارگیری متخصصان و مشاوران خبره عامل مهمی در امنیت اطلاعات است.	I5, I8, I10
	تأمین بودجه برای آموزش‌های لازم به کاربران و کارکنان	تأمین بودجه برای آموزش‌های لازم به کاربران و کارکنان عامل مهمی در امنیت اطلاعات است.	I1, I2, I4
	تأمین بودحه برای خرید سخت‌افزارها و نرم‌افزارهای مناسب	تأمین بودحه برای خرید سخت‌افزارها و نرم‌افزارهای مناسب عامل مهمی در امنیت اطلاعات است.	I5, I7, I9

عوامل شناسایی شده از نتایج تحلیل مصاحبه با خبرگان، در یک پرسشنامهٔ ساختاریافته تنظیم شد و در اختیار جامعهٔ آماری پژوهش قرار گرفت تا میزان اهمیت هر یک از این عوامل بر امنیت اطلاعات سنجیده شود؛ سپس داده‌های به‌دست آمده با استفاده از تحلیل عاملی اکتشافی و تحلیل عامل تأییدی بررسی و تحلیل شدند.

نتایج تحلیل عاملی اکتشافی برای متغیر عوامل مؤثر فنی نشان داد، میزان شاخص KMO بیشتر از ۰/۶ است؛ به این معنا که نمونه‌گیری برای انجام تحلیل عاملی اکتشافی کفایت می‌کند. همچنین میزان سطح معناداری آمارهٔ بارتلت کمتر از ۰/۰۵ به‌دست آمد که گویای مناسب‌بودن ساختار داده‌ها برای انجام تحلیل عاملی اکتشافی است، به این معنا که وجود ارتباط مناسب بین ساختار داده‌ها تأیید می‌شود. همچنین نتایج نشان داد میزان اشتراک سؤال‌های ۱، ۲، ۴، ۶، ۱۲، ۱۳، ۱۴ و ۱۶ (ضرایب تعیین سؤال‌ها) در پرسشنامه بیشتر از ۰/۵ است و سایر سؤال‌های پرسشنامه حذف می‌شوند. میزان تبیین واریانس متغیر مؤلفه‌های مرتبط با مسائل فنی نیز توسط ۱۹ سؤال در حدود ۷۶ درصد است. بنابراین می‌توان گفت که مؤلفه‌های مرتبط با مسائل فنی مؤثر بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قارهٔ ایران عبارت‌اند از: یکپارچگی سیستم‌های نرم‌افزاری در مدیریت امنیت اطلاعات، استفاده از نرم‌افزارها و سخت‌افزارهای به‌روز، نوع سیستم عامل استفاده‌شده، امنیت محیط فیزیکی منابع اطلاعاتی، مستندسازی و حفظ رخدادهای امنیت اطلاعات، پیاده‌سازی کنترل‌های خاص تبادل آنلاین، کار از راه دور و دسترسی عمومی، رعایت استانداردهای امنیتی، تدوین نیازهای امنیتی و معیارهای پذیرش امنیتی سیستم‌های اطلاعاتی، رمزنگاری اطلاعات محرمانه و با ارزش.

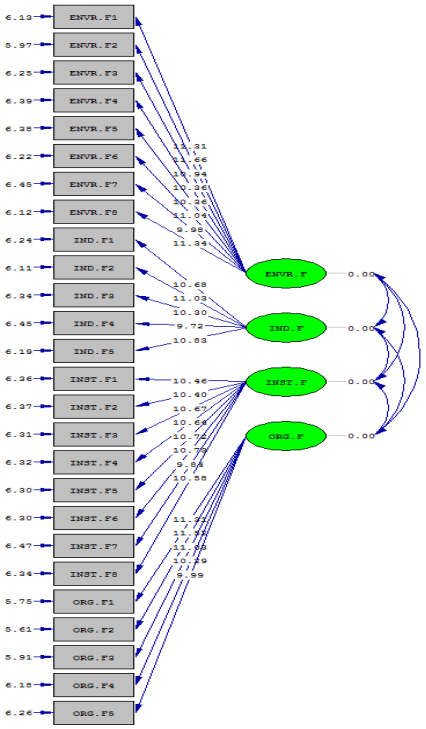
همچنین مؤلفه‌های مرتبط با مدیریت و رهبری که بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قارهٔ ایران مؤثرند، عبارت‌اند از: تأثیر همراهی مدیریت ارشد سازمان بر کیفیت مدیریت امنیت اطلاعات، پیاده‌سازی و وجود سیستم مدیریت یکپارچه (IMS) در سازمان، تعریف چشم‌انداز، اهداف، مرزها و خط‌مشی مدیریت امنیت اطلاعات، میزان تأکید و علاقهٔ مدیریت به پیگیری مسائل امنیت اطلاعات، نقش اقدام مؤثر و مناسب مدیریت در برابر نقض موارد امنیت اطلاعات.

مؤلفه‌های مرتبط با مسائل نیروی انسانی که بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قارهٔ ایران مؤثرند، عبارت‌اند از: تدوین خط‌مشی آموزش امنیت اطلاعات نیروی انسانی، ارزیابی توانایی کارکنان واحد امنیت اطلاعات در حفظ امنیت اطلاعات سازمان، آگاهی‌بخشی و آموزش امنیتی کارکنان پیش و حین استخدام، نقش انگیزه و وفاداری و رضایت نیروی انسانی، تأثیر آداب، سنن و اخلاقیات حاکم بر جامعه بر مدیریت امنیت اطلاعات،

تأثیر استفاده از متخصصان و افـراد خبـره در واحـد امنیـت اطلاعـات، رعایـت اخـلاق و حـریم خصوصی در پیاده‌سازی کلیهٔ اقدامات امنیتی، تعیین و اجرای نیازهای آموزشی کاربران در زمینـهٔ امنیت اطلاعات.

مؤلفه‌های مرتبط با مسائل مالی و اقتصادی که بـر مـدیریت امنیـت اطلاعـات واحـد فنـاوری اطلاعات شرکت نفت فلات قارهٔ ایـران تأثیرگذارنـد، عبـارت‌انـد از: تـأثیر میـزان بودجـهٔ سـازمان، منفعت‌سنجی اقدامات امنیتی و بودجهٔ لازم برای آنها پیش از اجرا، تأمین بودجـه بـرای اسـتخدام و به‌کارگیری متخصصان و مشاوران خبره، تأمین بودجـه بـرای آمـوزش‌هـای لازم بـه کـاربران و کارکنان، تأمین بودجه برای خرید سخت‌افزارها و نرم‌افزارهای مناسب.

در ادامه با استفاده از تحلیل عامل تأییدی به بررسی میزان همبستگی شاخص‌هـا بـا عوامـل مؤثر در قالب مدل اندازه‌گیری پژوهش پرداخته می‌شود.



شکل ۱. مدل اندازه‌گیری عوامل مؤثر در حالت اعداد معناداری

با توجه به شکل ۱ مشاهده می‌شود که تمام سؤال‌هـای مربـوط بـه متغیرهـا دارای ضـرایب همبستگی معناداری با متغیرهای مکنون هستند؛ چرا که میزان آمارهٔ تی بیشتر از ۱/۹۶ است. در

ادامه به بررسی شاخص‌های برازش مدل اندازه‌گیری عوامل مؤثر بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قاره ایران پرداخته می‌شود. نتایج تحلیل عامل تأییدی نشان می‌دهد میزان آمارهٔ تی برای همهٔ شاخص‌هایی که به‌عنوان مؤلفه‌های مؤثر بر امنیت اطلاعات در شرکت نفت فلات قاره شناسایی شده‌اند، بیشتر از ۱/۹۶ است، بنابراین شاخص‌های شناسایی شده تأثیر معناداری بر امنیت اطلاعات در شرکت نفت فلات قاره دارند و به‌عنوان شاخص‌های مؤثر نهایی معرفی می‌شوند.

جدول ۲. نتایج تحلیل عاملی تأییدی برای متغیرهای چهارگانه

سؤال یا سازه		میزان همبستگی با متغیر مکنون (بارعاملی)	آمارهٔ تی	نتیجه
عوامل فنی	سؤال ۱	۰/۹۱	۱۲/۳۱	تأیید
	سؤال ۲	۰/۹۲	۱۱/۶۶	تأیید
	سؤال ۳	۰/۸۹	۱۰/۹۴	تأیید
	سؤال ۴	۰/۸۶	۱۰/۳۶	تأیید
	سؤال ۵	۰/۸۶	۱۰/۳۶	تأیید
	سؤال ۶	۰/۸۹	۱۱/۰۴	تأیید
	سؤال ۷	۰/۸۴	۹/۹۸	تأیید
	سؤال ۸	۰/۹۱	۱۱/۳۴	تأیید
عوامل مدیریتی و رهبری	سؤال ۱	۰/۸۸	۱۰/۶۸	تأیید
	سؤال ۳	۰/۸۹	۱۱/۰۳	تأیید
	سؤال ۳	۰/۸۶	۱۰/۳۰	تأیید
	سؤال ۴	۰/۸۳	۹/۷۲	تأیید
	سؤال ۵	۰/۸۹	۱۰/۸۳	تأیید
عوامل انسانی	سؤال ۱	۰/۸۷	۱۰/۴۶	تأیید
	سؤال ۲	۰/۸۶	۱۰/۴۰	تأیید
	سؤال ۳	۰/۸۸	۱۰/۶۷	تأیید
	سؤال ۴	۰/۸۸	۱۰/۶۴	تأیید
	سؤال ۵	۰/۸۸	۱۰/۷۲	تأیید
	سؤال ۶	۰/۸۸	۱۰/۷۳	تأیید
	سؤال ۷	۰/۸۳	۹/۸۴	تأیید
	سؤال ۸	۰/۸۷	۱۰/۵۸	تأیید
عوامل اقتصادی و مالی	سؤال ۱	۰/۹۱	۱۱/۳۱	تأیید
	سؤال ۲	۰/۹۰	۱۱/۵۲	تأیید
	سؤال ۳	۰/۹۰	۱۱/۰۳	تأیید
	سؤال ۴	۰/۸۶	۱۰/۲۹	تأیید
	سؤال ۵	۰/۸۴	۹/۹۹	تأیید

پس از آن که برآورد پارامترها برای یک مدل تدوین شده و مشخص، به‌دست آمد، باید تعیین شود که داده‌ها تا چه حد با مدل برازش دارند؛ یعنی تا چه اندازه مدل نظری به‌وسیلهٔ داده‌های نمونه حمایت می‌شود. برای سنجیدن این موضوع که مدل تا چه حد روابط مشاهده شده بین متغیرهای قابل اندازه‌گیری را توصیف می‌کند، چند آزمون به‌کار می‌رود. جدول ۲ معرف انواع شاخص‌های برازش و معناداری مدل است.

جدول ۳. شاخص‌های معناداری و برازش مدل

	نام شاخص	اختصار	برازنده است	میزان در مدل به‌دست آمده	نتیجه
شاخص‌های معناداری	ریشهٔ میانگین مربعات خطای برآورد	RMSEA	کوچک‌تر از ۰/۱ باشد	۰/۰۴۶	تأیید
	کای اسکوئر به درجهٔ آزادی	$\frac{x^2}{d_f}$	مساوی وکوچک‌تر از ۵ باشد	۱/۹۷	تأیید
شاخص‌های برازش	شاخص نیکویی برازش	GFI	بزرگ‌تر از ۰/۸باشد	۰/۸۷	تأیید
	شاخص برازش هنجارنشده	NNFI	بزرگ‌تر از ۰/۸باشد	۰/۹۷	تأیید
	شاخص برازش هنجارشده	NFI	بزرگ‌تر از ۰/۸باشد	۰/۹۵	تأیید
	شاخص برازش تطبیقی	CFI	بزرگ‌تر از ۰/۸باشد	۰/۹۷	تأیید
	شاخص برازش افزایشی	IFI	بزرگ‌تر از ۰/۸باشد	۰/۹۷	تأیید

با توجه به نتایج به‌دست آمده، مدل پژوهش از نظر شاخص‌های معناداری و برازش تأیید می‌شود. بدین ترتیب و با توجه به نتایج به‌دست آمده می‌توان گفت مؤلفه‌های مرتبط با مسائل فنی، مسائل انسانی، مسائل مدیریت و مسائل مالی و اقتصادی از عوامل مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قاره ایران هستند.

اولویت عوامل اثرگذار

اولویت عوامل اثرگذار بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قارهٔ ایران بدین ترتیب است. با توجه به جدول ۳ مشاهده می‌شود که سطح معناداری به‌دست آمده کوچک‌تر از ۰/۰۵ است، در نتیجه بین میانگین رتبهٔ هر بعد از عوامل اثرگذار تفاوت معناداری وجود دارد. با توجه به میانگین رتبه‌ها، اولویت‌بندی رتبه‌ها بدین ترتیب است: مؤلفه‌های مرتبط با مسائل انسانی، مسائل فنی، مسائل مدیریت و رهبری و مسائل مالی و اقتصادی. این اطلاعات را به‌صورت گرافیکی در زیر مشاهده می‌کنید.

جدول ٤. آزمون فریدمن برای اولویت‌بندی عوامل اثرگذار بر مدیریت امنیت اطلاعات در فناوری اطلاعات

	میانگین رتبه	کای‌دو	درجهٔ آزادی	سطح معناداری
مؤلفه‌های مرتبط با مسائل انسانی	۳/۰۴	۳۷/۵۲۳	۳	۰/۰۰۰
مؤلفه‌های مرتبط با مسائل فنی	۲/۷۲			
مؤلفه‌های مرتبط با مسائل مدیریتی و رهبری	۲/۲۰			
مؤلفه‌های مرتبط با مسائل مالی و اقتصادی	۲/۰۴			

نتیجه‌گیری و پیشنهادها

در این پژوهش به بررسی و شناسایی مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قارهٔ ایران پرداخته شد که نتایج پژوهش در ادامه ارائه شده است.

ابتدا برای شناسایی مؤلفه‌های تأثیرگذار بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قارهٔ ایران، پس از برگزاری مصاحبهٔ نیمه ساختاریافته با خبرگان، داده‌های لازم برای این بخش جمع‌آوری شد؛ سپس داده‌ها به‌صورت باز و بسته کدگذاری شدند که نتیجهٔ آن شناسایی مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قارهٔ ایران بود. در ادامه نتایج با استفاده از تحلیل عامل تأییدی تجزیه و تحلیل شدند و نتایج زیر بر مبنای سؤال‌های تحقیق به‌دست آمد:

سؤال اول پژوهش: مؤلفه‌های مرتبط با مسائل فنی تأثیرگذار بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قارهٔ ایران کدام‌اند؟

نتایج تحلیل کیفی و کمی پژوهش نشان داد مؤلفه‌های مرتبط با مسائل فنی که بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قارهٔ ایران تأثیرگذارند، عبارت‌اند از: یکپارچگی سیستم‌های نرم‌افزاری در مدیریت امنیت اطلاعات، استفاده از نرم‌افزارها و سخت‌افزارهای به‌روز، نوع سیستم عامل استفاده شده، امنیت محیط فیزیکی منابع اطلاعاتی، مستندسازی و حفظ رخدادهای امنیت اطلاعات، پیاده‌سازی کنترل‌های خاص تبادل آنلاین، کار از راه دور و دسترسی عمومی، رعایت استانداردهای امنیتی، تدوین نیازهای امنیتی و معیارهای پذیرش امنیتی سیستم‌های اطلاعاتی، رمزنگاری اطلاعات محرمانه و با ارزش.

سؤال دوم پژوهش: مؤلفه‌های مرتبط با مسائل مدیریت و رهبری مؤثر بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قارهٔ ایران کدام‌اند؟

نتایج تحلیل کیفی و کمی پژوهش نشان داد که مؤلفه‌های مرتبط با مسائل مدیریت و رهبری که بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قارهٔ ایران تأثیرگذارند، عبارت‌اند از: تأثیر همراهی مدیریت ارشد سازمان بر کیفیت مدیریت امنیت اطلاعات،

پیاده‌سازی و وجود سیستم مدیریت یکپارچه (IMS) در سازمان، تعریف چشم‌انداز، اهداف، مرزها و خط‌مشی مدیریت امنیت اطلاعات، میزان تأکید و علاقهٔ مدیریت بـه پیگیـری مسـائل امنیـت اطلاعات، نقش اقدام مؤثر و مناسب مدیریت در برابر نقض موارد امنیت اطلاعات.

سؤال سوم پژوهش: مؤلفه‌های مرتبط با مسـائل نیـروی انسـانی مـؤثر بـر مـدیریت امنیـت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قارهٔ ایران کدام‌اند؟

نتایج تحلیل کیفی و کمی پژوهش نشان داد مؤلفه‌های مرتبط با مسائل نیروی انسانی که بر مدیریت امنیت اطلاعات واحد فناوری اطلاعـات شـرکت نفـت فـلات قـارهٔ ایـران تأثیرگذارنـد، عبارت‌اند از: تدوین خط‌مشی آموزش امنیت اطلاعات نیروی انسـانی، ارزیـابی توانـایی کارکنـان واحد امنیت اطلاعات در حفظ امنیت اطلاعات سازمان، آگاهی‌بخشی و آموزش امنیتـی کارکنـان پیش و حین استخدام، نقش انگیـزه و وفـاداری و رضـایت نیـروی انسـانی، تـأثیر آداب، سـنن و اخلاقیات حاکم بر جامعه بر مدیریت امنیت اطلاعات، تأثیر استفاده از متخصصان و افراد خبره در واحد امنیت اطلاعات، رعایت اخلاق و حریم خصوصی در پیاده‌سازی کلیهٔ اقدامات امنیتی، تعیین و اجرای نیازهای آموزشی کاربران در زمینهٔ امنیت اطلاعات.

سؤال چهار پژوهش: مؤلفه‌های مرتبط با مسائل مالی و اقتصادی مـؤثر بـر مـدیریت امنیـت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قارهٔ ایران کدام‌اند؟

نتایج تحلیل کیفی و کمی پژوهش نشان داد مؤلفه‌های مرتبط با مسائل مالی و اقتصادی که بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فـلات قـارهٔ ایـران تأثیرگذارنـد، عبارت‌اند از: تأثیر میزان بودجهٔ سازمان، منفعت‌سنجی اقدامات امنیتی و بودجـهٔ لازم بـرای آنهـا پیش از اجرا، تأمین بودجه برای استخدام و به‌کارگیری متخصصان و مشاوران خبره، تأمین بودجه برای آموزش‌هـای لازم بـه کـاربران و کارکنـان، تـأمین بودجـه بـرای خریـد سـخت‌افزارهـا و نرم‌افزارهای مناسب.

نتایج پژوهش حاضر با نتایج پژوهش خیرگو و شکوهی (۱۳۹۶)، مطابقت دارد. آنها دریافتنـد که عوامل سازمانی، عوامل انسانی و فنی به‌ترتیب بـر اثربخشـی سیسـتم‌هـای اطلاعـاتی تـأثیر می‌گذارند و از بین شاخص‌های مؤثر بر اثربخشی سیستم‌های اطلاعاتی، به‌ترتیب حمایـت مـدیر ارشد، امنیت، پذیرش و مدیریت دانش فناوری اطلاعـات و سیسـتم‌هـای اطلاعـاتی، رتبـه‌هـای بیشتری داشتند. همچنین نجاتی و همکاران (۱۳۹۳) نشان داد عامل کنترل و عوامـل مـرتبط بـا مسائل مدیریتی از مهم‌ترین عوامل مـؤثر بـر امنیـت اطلاعـات هسـتند. بـر اسـاس یافتـه‌هـای زنجیرچی و همکاران (۱۳۹۳)، پنج شـاخص اشـاعه و اسـتفاده از اطلاعـات محرمانـه (امنیتـی)؛ سوءاستفاده از سیستم اطلاعات (سوءاستفادهٔ عمـدی کارمنـدان داخلـی از منـابع IS)؛ آگـاهی از

اهمیت و ضرورت پیروی از قوانین و اجرای فعالیت‌های امنیتی؛ استفاده از ابزارهای آموزشی متنوع برای آموزش فعالیت‌های مرتبط با امنیت سیستم‌های اطلاعاتی؛ و تعهد و وفاداری کارمندان نسبت به سازمان و حفظ اطلاعات بر مدیریت امنیت اطلاعات تأثیرگذارند. نتایج این پژوهش‌ها با نتایجی که در پژوهش حاضر به‌دست آمده، مطابقت دارد. جعفری، رحمانی و مهرآزمای (۱۳۸۷) نیز نشان دادند که چهار عامل کنترل محیطی و مدیریتی، مدیریت تسهیلات فیزیکی، حفاظت از مرکز داده و کنترل کارکنان از عوامل مهم بر امنیت اطلاعات در سازمان است.

پیشنهادهای کاربردی

با توجه به نتایج به‌دست آمده از این پژوهش، پیشنهادهای زیر برای بهبود مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قارهٔ ایران ارائه می‌شود.

با توجه به نتایج بررسی سؤال اول تحقیق که در بعد مؤلفه‌های مرتبط با مسائل فنی است، پیشنهاد می‌شود راهکارهای زیر دنبال شود:

- سیستم‌های نرم‌افزاری در مدیریت امنیت اطلاعات یکپارچه شود؛
- از نرم‌افزارها و سخت‌افزارهای به‌روز در بخش مدییت امنیت اطلاعات استفاده شود؛
- نوع سیستم عامل استفاده شده، مبتنی بر توانایی بهبود امنیت اطلاعات سیستم باشد؛
- امنیت محیط فیزیکی منابع اطلاعاتی ارتقا یابد؛
- کنترل‌های خاصی برای تبادل آنلاین پیاده‌سازی شود تا در زمان‌هایی که کار از راه دور انجام می‌شود و دسترسی عمومی بیشتر است، امنیت حفظ اطلاعات بیشتر شود؛
- اطلاعات محرمانه و با ارزش رمزنگاری شوند.

با توجه به نتایج بررسی سؤال دوم تحقیق که در بعد مؤلفه‌های مرتبط با مسائل مدیریت و رهبری است، پیشنهاد می‌شود راهکارهای زیر دنبال شود:

- مدیریت ارشد سازمان بر کیفیت مدیریت امنیت اطلاعات نظارت کند و همکاری و همراهی مناسبی با سایر مدیران داشته باشد؛
- سیستم مدیریت یکپارچه (IMS) در سازمان پیاده‌سازی شود؛
- مدیریت سازمان بر پیگیری مسائل امنیت اطلاعات تأکید بیشتری داشته باشد و اهمیت آن را برای کارکنان روشن کند؛
- مدیریت در برابر نقض موارد امنیت اطلاعات اقدام مؤثر و مناسبی داشته باشد.

با توجه به نتایج بررسی سؤال سوم تحقیق که در بعد مؤلفه‌های مرتبط با مسائل نیروی انسانی است، پیشنهاد می‌شود راهکارهای زیر دنبال شود:

- خط‌مشی آموزش امنیت اطلاعات نیروی انسانی تدوین شود؛
- توانایی کارکنان واحد امنیت اطلاعات در حفظ امنیت اطلاعات سازمان ارزیابی شود؛
- برای کارکنان سازمان پیش و در حین استخدام کلاس‌های آموزشی برگزار شود؛
- آداب، سنن و اخلاقیات حاکم بر نیروی انسانی بیشتر در کانون توجه قرار گیرد؛
- از متخصصان و افراد خبره در واحد امنیت اطلاعات استفاده شود؛
- در پیاده‌سازی کلیهٔ اقدامات امنیتی، اخلاق و حریم خصوصی رعایت شود.

با توجه به نتایج بررسی سؤال چهارم تحقیق که در بعد مؤلفه‌های مرتبط با مسائل مالی و اقتصادی است، پیشنهاد می‌شود راهکارهای زیر دنبال شود:

- برای تهیهٔ ابزارهای لازم سازمان، بودجهٔ مورد نیاز پیش‌بینی و تأمین شود؛
- برای اجرای اقدامات امنیتی، بودجهٔ لازم پیش‌بینی و تأمین شود؛
- برای استخدام و به‌کارگیری متخصصان و مشاوران خبره بودجهٔ کافی در نظر گرفته شود؛
- برای آموزش‌های لازم به کاربران و کارکنان بودجهٔ کافی در نظر گرفته شود؛
- برای خرید سخت‌افزارها و نرم‌افزارهای مناسب، بودجهٔ کافی در نظر گرفته شود.

فهرست منابع

جعفری، ع.، رحمانی، م. و مهرآزمای، ح. (۱۳۸۷). شناسایی و رتبه بندی عوامل و شاخصهای کلیدی موثر بر مدیریت تهدیدات امنیت فیزیکی و محیطی اطلاعات. *پنجمین کنفرانس بین‌المللی مدیریت فناوری اطلاعات و ارتباطات*، تهران، ندای اقتصاد بامداد.

خیرگو، م. و شکوهی، ج. (۱۳۹۶). شناسایی و رتبه‌بندی عوامل کلیدی مؤثر بر اثربخشی سیستم‌های اطلاعاتی در سازمان‌های دولتی. *پژوهشنامهٔ پردازش و مدیریت اطلاعات*، ۳۲(۳)، ۷۱۲-۶۹۵.

رمضانیان، م.ر. و بساق‌زاده، ن. (۱۳۹۱). تأثیر توانایی جذب و فرهنگ سازمانی بر موفقیت اجرای IS در شرکت‌های تولیدی قطعات خودروی استان گیلان. *مدیریت فناوری اطلاعات*، ۳ (۹)، ۶۸-۴۱.

زنجیرچی،س.م.، مروتی شریف‌آبادی، ع. و شاه‌حسینی بیده، ش. (۱۳۹۳). مقایسهٔ عملکرد سازمان‌ها در پیاده‌سازی مدیریت ارتباط با مشتری با استفاده از رویکرد ترکیبی NAP و DEMATEL فازی. *فصلنامهٔ بازاریابی نوین*، ۴(۳)، ۲۱۲-۱۹۵.

شرکت ملی پالایش و پخش فراورده های نفتی ایران(۱۳۹۶).مدیریت فناوری اطلاعات و ارتباطات. قابل دسترس در http://niordc.ir/index.aspx?siteid=77&pageid=520

نجاتی، ی.، حقیقت منفرد، ج. و رمضان، م. (۱۳۹۳). شناسایی و اولویت‌بندی عوامل مؤثر بر استقرار سیستم مدیریت امنیت اطلاعات (مورد مطالعه: ادارات مرکزی بانک کشاورزی در شهر تهران). *کنفرانس*

بین‌المللی حسابداری و مدیریت، تهران، مؤسسهٔ همایشگران مهر اشـراق، مرکـز همـایش‌هـای دانشـگاه تهران.

Bellone, J, Basquiat, S. D., Rodriguez, J. (2008). *Reaching escape velocity: A practiced approach to information security management system implementation*, Information Management & Computer Security, 16 (1), 49-57.

Bhattacharya, D. (2011). Leadership styles and information security in small businesses. *Information Management & Computer Security*, 19(5), 300-312.

Birman, K.P. (2000). The next-generation internet: unsafe at any speed. *IEEE computer,* 33(8), 54-60.

Hagen, J., Albrechtsen, E., Johnsen, S.O. (2011). The long-term effects of information security e-learning on organizational learning, *Information Management & Computer Security*,19 (3), 140-154.

Iranian Offshore Oil Company (2017). Information and Communication Technology Management. Available in: *http://niordc.ir/index.aspx?siteid=77&pageid =520*.

Jafari, A., Rahmani, M. & Mehrazmai, H. (2008). Identification and ranking of key factors and factors affecting the management of threats to physical and environmental information security. *Fifth International Conference on Information and Communication Technology Management,* Nedaye Bamdad, Tehran, (*in Persian*)

Kheirgoo, M., Shukuhy, J. (2017). Identification and Ranking of Key Factors Influencing the Effectiveness of Information Systems in State-Owned Organizations. *Iranian Research Institute for Science and Technology*, 32(3), 694-711. (*in Persian*)

Kouziokas, G.N. (2016). Technology-based management of environmental organizations using an Environmental Management. *Environmental Technology & Innovation*, 5, 106–116.

Meskell, P., Burke, E., Kropmans, T. J., Byrne, E., Setyonugroho, W. & Kennedy, K.M. (2015). Back to the future: An online OSCE Management Information System for nursing OSCEs. *Nurse Education Today,* 35(11), 1091-1096.

Nejati, Y., Haghighat-Monfared, J., Ramezan, M. (2014). Identification and Prioritization of Factors Affecting the Establishment of Information Security Management System (Case Study: Central Office of Agricultural Bank in Tehran). *International Conference on Accounting and Management*, Tehran. (*in Persian*)

Pathari, V., Sonar, R. (2012). Identifying linkages between statements in information security policy, procedures and controls. *Information Management & Computer Security*, 20(4), 264-280.

Ramezaniyan, M. R., Bssaghzadeh, N. (2012). The Effect of Absorptive Capacity and Corporate Culture on IS Implementation Success in Production Companies of Automobile Segments in the Guilan Province. *Journal of Information Technology Management (JITM)*,3(9), 41-68. (*in Persian*)

Thomson, K. & Van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behavior. *Information Management & Computer Security,* 20(1), 39-46.

Wolf, J., Wolfe, B. (2003). Management strategies for implementing forensic security measures. *Information Security Technical Report*. 8(2), 55-64.

Zangirchi, S. M., Morovvati Sharifabadi, A., Shahoseini Bideh, SH. (2014). The comparison of organization's performance on Customer Relationship Management (CRM) implementation using an integrative approach of Fuzzy ANP and DEMATEL. *Journal of New Marketing Research*,4(4), 195-212. (*in Persian*)

Zuccato, A. (2007). Holistic security management framework applied in electronic commerce. *Computers and Security*, 26 (3), 256-265.