تاریخ دریافت: ۱۴۰۱/۱/۱۵ تاریخ پذیرش: ۱۴۰۱/۵/۵ صفحه ۶۰ تا ۹۱

شناسایی و رتبه‌بندی معیارهای مؤثر امنیت نظام‌های اطلاعاتی شهرداری کلان شهر اهواز با رویکرد ترکیبی دیمتل و ا.ان.پی

حسین محمد شفیع‌پور[۱]، فریبا نظری[۲]

چکیده

امنیت نظام اطلاعاتی به عنوان مجموعه اقداماتی با هدف کنترل، دسترسی و استفاده از نظام اطلاعات در یک سازمان تعریف شده است. هدف این پژوهش شناسایی و رتبه‌بندی معیارهای مؤثر امنیت نظام‌های اطلاعاتی شهرداری کلان شهر اهواز با رویکرد ترکیبی دیمتل و ا.ان.پی بود. پژوهش حاضر از نظر هدف کاربردی و از لحاظ نوع اجرا توصیفی بود. جامعه آماری این پژوهش کلیه کارکنان سازمان فناوری اطلاعات و ارتباطات شهرداری کلان شهر اهواز به تعداد ۵۰ نفر هستند که از میان کارکنان ۱۰ نفر با سابقه بالای ۱۰ سال، مسلط به فناوری اطلاعات و تصمیم‌گیرنده ارشد در سازمان به صورت گلوله برفی انتخاب شدند. در این پژوهش از روش‌های دلفی برای شناسایی، دیمتل برای تعیین روابط و ا.ان.پی برای وزن‌دهی و رتبه‌بندی معیارها استفاده شده است. بر اساس نتایج تکنیک دلفی ۳۲ سؤال مربوط به ۵ معیار و ۲۷ زیرمعیار با اهمیت شناخته شدند. در ادامه از روش دیمتل روابط بین معیارها بررسی گردید. در نهایت برای رتبه‌بندی معیارها از روش ا.ان.پی استفاده شد. بر اساس نتایج معیارهای مدیریتی، فنی، سازمانی، فردی و فرهنگی به ترتیب در رتبه اول تا پنجم قرار گرفتند.

واژگان کلیدی: امنیت نظام اطلاعاتی، شهرداری کلان شهر اهواز، دیمتل، ا.ان.پی

۱. دانشجوی کارشناسی ارشد مدیریت فناوری اطلاعات، واحد اهواز، دانشگاه آزاد اسلامی، اهواز، ایران
shafiepour.M.H@gmail.com

۲. استادیار گروه علم اطلاعات و دانش شناسی، واحد اهواز، دانشگاه آزاد اسلامی، اهواز، ایران. (نویسنده مسئول)
f.nazari@iauahvaz.ac.ir

Identification and ranking of effective metrics of Ahvaz Metropolitan Municipality information systems security using a combined approach of DEMTEL and ANP

Hossein Mohammad Shafi'pour[1],

Fariba Nazari[2]

Abstract

The purpose of this study was to identify and rank effective metrics of Ahvaz metropolitan municipality information security using a combined approach of DEMTEL and ANP. The present study was applied in terms of purpose and descriptive in terms of type of implementation. Statistical population of this research is all employees of ICT of Ahwaz Metropolitan Municipality (50 people). From among 10 employees with more than 10 years of experience, information technology and senior decision makers in the organization were selected as snowball. In this study, Delphi methods were used for identification, DEMTEL for determining relationships, and NNP for weighting and ranking criteria. Based on the results of the Delphi technique, 32 questions related to 5 criteria and 27 sub-criteria were identified. Then, the relationship between the criteria was investigated by DEMATEL method. Finally, the ANP method was used to rank the criteria. Based on the results of management, technical, organizational, individual and cultural criteria were ranked first to fifth respectively.

Keywords: Information System Security, Ahwaz Metropolitan Municipality, Demetel, ANP.

1. Student of Information Technology Management, Ahvaz Branch, Islamic Azad University, Ahvaz, Iran shafiepour.M.H@gmail.com

2. Assistant Professor, Department of knowledge and Information Science, Ahvaz Branch, Islamic Azad University, Ahvaz, Iran. Corresponding author.
f.nazari@iauahvaz.ac.ir

مقدمه و بیان مساله

امنیت اطلاعات مسـئله‌ای حیاتی برای سازمان‌ها در سراسر جهان در عصر حاضر است. امنیت نظام‌های اطلاعاتی[1] شامل دو بعد فناوری و افراد (عوامل انسانی) می‌شود. بررسی‌ها نشان می‌دهد در بیشـتر پژوهش‌هایی که در زمینه امنیت سیسـتم‌های اطلاعاتی صورت گرفته؛ یک نوع دید و رویکرد فنی وجود داشته است. امروزه سازمان‌ها توافق دارند که یکی از اولویت‌های مدیران عالی، افزایش امنیت منابع فناوری و اطلاعات است (رانزباسم و میترا[2]، ۲۰۰۹). نظام‌های اطلاعاتی نقش مهمی در زندگی سـازمانی نوین داشـته و دنیای کسب و کار، تجارت و مدیریت را دچار دگرگونی شـگرفی نموده است. حیات سـازمان‌ها ارتباط نزدیکی با نظام‌های اطلاعاتی آنها دارد. نظام‌های اطلاعاتی نیز همواره در خطر سـرقت اطلاعات و ایجاد وقفه در خدمت‌رسـانی هستند(خیرگو و شـکوهی، ۱۳۹۶). محققان نقش نظام‌های مدیریـت امنیت اطلاعات را بر افزایش دقت و صحت تبادلات اطلاعات، دسترسـی به اطلاعات دقیق و به موقع و کاهش خطاهای نظام اطلاعاتی مؤثر دانسته‌اند(صالح نیا و بختیاری، ۱۳۹۷). امنیت نظام اطلاعاتی به عنوان مجموعه اقداماتی با هدف کنترل، دسترسی و استفاده از نظام اطلاعات در یک سازمان تعریف شده است(تمپینی و لئونلی[3]، ۲۰۱۸). اثربخشی امنیت نظام اطلاعاتی به عنوان دستیابی به اهداف (فردی و سازمانی) می‌باشد (خیرگو و شکوهی، ۱۳۹۶).

به منظور حل مسـأله امنیت اطلاعات، سـازمان‌ها نیازمند کسب اطلاعات گوناگون و حفاظت از اطلاعات و اسـرار خود می‌باشـند. در این راستا ایجاد یک نظام قوی می‌تواند برای حفظ امنیت اطلاعات مؤثر باشد، نظامی که بر اساس نیازهای سازمان و میزان اهمیت اطلاعات در آن طراحی شده و حفاظی برای تأمین سرمایه‌های اطلاعات سازمان باشد. امنیت نظام‌های اطلاعاتی، بخشی از سیسـتم مدیریت کلی و سراسـری در هر سازمان اسـت که بر پایه رویکرد مخاطرات کسب و کار قرار دارد و هدف آن پایه‌گذاری، پیاده‌سـازی، بهره‌برداری، نظارت، بازبینی، نگهداری و بهبود امنیت نظام‌های اطلاعات است. در صورت پیاده‌سازی اثربخش این نوع مدیریت می‌توان با کاهش ریسـک‌های پیرامونی به عنوان عامل مهم، در تضمین سطح امنیتی تعریف شده، نقش به سزایی را ایفا کرد (آستروسکا و مازور[4]، ۲۰۱۵).

1. Information system security
2. Ransbotham & Mitra
3. Tempini & Leonelli
4. Ostrowska & Mazur

از سوی دیگر مدیریت مدرن بدون در نظر گرفتن معیارهای مؤثر بر اثربخشی موفق نبوده و امنیت نظام‌های اطلاعاتی نیز از این قاعده مستثنی نیست(رضایی، مصدق و رضایی، ۱۳۹۷). در مورد شناسایی معیارهای مؤثر اثربخشی امنیت نظام‌های اطلاعاتی پژوهش‌های مختلفی در داخل و خارج کشور صورت گرفته است. از نظر مستقیمی و امین موسوی (۱۳۹۷) برخی شاخص‌های مهم مرتبط با تصمیم به استفاده نظام مدیریت امنیت اطلاعات عبارتند از: مقاومت مدیران و کارکنان در برابر تغییر با نگرش نسبت به استفاده؛ نگرش نسبت به استفاده با تمایل به استفاده؛ سهولت استفاده ادراک شده، کمیته راهبری شایسته، مقاومت مدیران و کارکنان در برابر تغییر، تعیین صحیح دامنه پیاده‌سازی (قلمرو استقرار) و سند خط مشی امنیت اطلاعات مناسب با سودمندی ادراک شده؛ کمیته راهبری شایسته، حمایت کامل و مشارکت مدیران ارشد و هزینه‌های زیاد پیاده‌سازی. از نظر رضایی، مصدق و رضایی (۱۳۹۷) نیز شاخص‌های نقش مدیریت، آگاهی از امنیت نظام اطلاعات و انطباق با آموزش، امینت نظام اطلاعات کسب وکار و ارزیابی ریسک امنیت نظام اطلاعات بر اثربخشی نظام مدیریت امنیت اطلاعات تأثیرگذار می‌باشند. نتایج پژوهش تو و یان[1] (۲۰۱۸) نشان داد هماهنگی کسب و کار، پشتیبانی از مدیریت ارشد و آگاهی سازمانی از خطرات و کنترل‌های امنیتی، کنترل موثر امنیت اطلاعات می‌تواند منجر به مدیریت امنیت اطلاعات موفق شوند. در پژوهش ماروا[2] (۲۰۱۵) تعهد مدیریت ارشد، سیاست امنیت اطلاعات و آگاهی و آموزش کارکنان توانستند ۸۴ درصد از تغییرات اثربخشی نظام‌های اطلاعاتی را پیش‌بینی کنند. کیلو و انزوکی[3] (۲۰۱۵) بیان کردند که عواملی همچون تعهد مدیریت ارشد، ارتباطات اثربخش، آموزش، کیفیت فنی نظام اطلاعاتی، اندازه‌گیری منابع انسانی، فعالیت‌های مدیریت تغییر و اثربخشی آنها، سخت‌کوشی مدیریت پروژه، کیفیت برنامه‌های نظام اطلاعاتی، کار تیمی و ترکیب تیم نظام اطلاعاتی بر موفقیت نظام‌های مدیریت امنیت اطلاعات مؤثرند. در بسیاری از پژوهش‌های انجام شده در رابطه با امنیت اطلاعات چه در داخل و چه خارج از کشور، به موضوع نحوه تأثیرگذاری و مزایای آن در سازمان‌ها بسنده شده است و عملاً موضوع شناسایی و رتبه‌بندی معیارهای مؤثر اثربخشی امنیت نظام‌های اطلاعاتی نادیده گرفته شده است و جای خالی این نوع تحقیقات به وضوح دیده می‌شود.

---

1. Tu & Yuan
2. Maroa
3. Kiilu & Nzuki

همچنیـــن تصمیم‌گیـــری در مورد انتخاب معیارها همواره فرایندی دشـــوار بوده و در شـــرایط فعلی که دگرگونی‌های ســـریع و فزاینده حادث می‌شـــود بی‌شـــک آهنگ شـــتاب زیادی به خود گرفته اســـت. در فرایند تصمیم‌گیری انتخاب معیارهایی که بر ارزیابی راه حل‌ها و انتخاب راه حل رضایت‌بخش مؤثرند از جمله گام‌های اساسی به شمار می‌آید. معیارهایی که در اخذ تصمیم بکار می‌روند، عواملی هســـتند که انتخاب یک راهکار از میان راهکارهای مختلف در راســـتای نیل به هدف را میسر می‌سازند. بنابراین تصمیم‌گیری‌ها غالباً با توجه به معیارهای متعدد انجام می‌پذیرد. روش‌های تصمیم‌گیری در تعریف مســـأله روش‌هایی هستند که به تصمیم‌گیرنده کمک می‌کنند تا بتواند برای رســـیدن به نیازهایش ســـؤالات دقیقی را طراحی کند (اســـماعیلی، ۱۳۹۳). در این میان روش‌های تصمیم‌گیری، روش‌های دیمتل و ا.ان.پی رویه‌های مناســـبی است؛ زیرا زمانی که هم معیارها کمی و هم کیفی موجود باشـــند قابل استفاده هستند. با توجه به نقش فزاینده امنیت اطلاعات در اداره هر جامعه، سازمان‌ها و نهادهای دولتی و خصوصی ناگزیر به تأمین زیرساخت‌های لازم برای تحقق این امر مهم می‌باشـــند. برای اجرای بهینه و موفق سیســـتم‌های مدیریت امنیت اطلاعـــات علاوه بر منابع مادی، تکنیک‌های مدیریتی نیز تأثیر زیادی دارند. ثبت اســـتانداردهای مدیریتی در حوزه امنیت اطلاعات فاوا می‌تواند به صورت برنامه‌ریزی‌شده طراحی شود تا وضعیت امنیتی ســـازمان‌ها متناســـب با نیاز آن ســـازمان تغییر یابد و امنیت از منظر ادامه کسب‌وکار و تا اندازه‌ای در سطوح دیگر (مدیریت بحران و جنگ نرم) تضمین شود(خیری، ۱۳۹۴).

به لحاظ عملی، این پژوهش در مضامین متعدد کاربردی خواهد داشت. انجام این پژوهش سبب می‌شود تا مدیران شهرداری کلان شهر اهواز معیارهای مؤثر اثربخشی امنیت نظام‌های اطلاعاتی را آسیب‌شناسی کرده و دریابند چه معیارهایی می‌توانند باعث اجرای بهتر موضوع امنیت اطلاعات شوند. این امر می‌تواند به برنامه‌ریزی بهتر و مناسب در سازمان در راستای ایجاد مطلوب سازمانی و انجام اعمال مدیریتی مقتضی کمک نماید. همچنین نتایج این پژوهش می‌تواند به شهرداری کلان شهر اهواز در کاهش احتمال غیرفعال شدن سیستم‌ها و برنامه‌ها (از دست دادن فرصت‌ها)، استفاده مؤثر از منابع انسانی و غیرانسانی در یک سازمان (افزایش بهره‌وری)، کاهش هزینه از دست دادن داده توســـط ویروس‌های مخرب و یا حفره‌های امنیتی (حفاظت از داده‌های ارزشـــمند) و افزایش حفاظت از مالکیت معنوی کمک نماید.در سازمان‌هایی مثل شهرداری‌ها که از داده‌های محرمانه شـــهروندان یا مشـــتریان نگهداری می‌کنند، نیاز به ایجاد سیاســـت‌ها و روال‌های رسمی امنیتی بیشتر اهمیت پیدا می‌کند. شهرداری‌ها از طریق توجه به امنیت نظام‌های اطلاعاتی و اطمینان از

اثربخشی آن می‌توانند بر چالش‌های امنیتی غلبه کنند. در شهرداری کلان شهر اهواز نیز، مدیران و کارکنان فناوری اطلاعات بر سیاست‌های امنیت اطلاعات توجه موکد دارند. بر همین اساس در این تحقیق سعی شده تا ضمن شناسایی و اولویت‌بندی این معیارها با رویکرد ترکیبی دیمتل و ا.ان.پی، رهنمودهایی را نیز برای بهبود امنیت برای شهرداری ارائه دهد تا این سازمان بتواند از مشکلات و تهدیدات امنیتی پیشگیری کند. تا کنون پژوهش‌های مختلفی به امنیت نظام‌های اطلاعاتی انجام شده است. بیشتر پژوهش‌های در تیم‌های پروژه‌ای و نرم‌افزاری انجام شده‌اند ولی پژوهش حاضر در شهرداری کلان شهر اهواز انجام شده است و این موضوع از جنبه نوآورانه بودن پژوهش است. لذا با توجه به مطالب گفته شده، این پژوهش در جهت پاسخگویی به این سؤالات طراحی شده است: معیارهای مؤثر اثربخشی امنیت نظام‌های اطلاعاتی شهرداری کلان شهر اهواز کدامند؟ اولویت‌بندی آنها به چه صورت می‌باشد؟

۱. مبانی نظری

تعریف امنیت

امنیت حالت فراغت نسبی از تهدید یا حمله یا آمادگی برای رویارویی با هر تهدید و حمله را گویند. امنیت از ضروری‌ترین نیازهای یک جامعه است. امنیت در گفتمان سلبی بر نبود خطر و تهدیدات استوار است؛ ولی امنیت در گفتمان ایجابی به تأمین و تضمین آسایش و آسودگی نظر دارد. مفهوم‌های مرتبط با امنیت در فارسی کلاسیک با واژه‌های زنهار و زینهاری ادا می‌شد امنیت به معنای ایمنی در برابر خطرات احتمالی و یا واقعی است که موجودیت و بقاء یک پدیده زنده، فرد یا جامعه را تهدید می‌کند (کرمی، صفدری و سلطانی، ۱۳۹۲).

انواع امنیت

مسائل مربوط به امنیت در سال‌های اخیر در حال افزایش بوده است و این واقعیت منجر به توسعه پژوهش‌های مختلف در جنبه‌های مختلف امنیت می‌گردد (لی، ین، چن، چن، لو و چو[1]، ۲۰۱۵). انواع امنیت را می‌توان به صورت زیر تقسیم‌بندی کرد: امنیت مالی (اقتصادی)، امنیت جانی، امنیت سیاسی، امنیت اخلاقی و امنیت اجتماعی (باپیری، کمربیگی و درویشی، ۱۳۹۴).

1. Li, Yen, Chen, Chen, Lu & Cho

تعریف نظام

نظام مجموعه‌ای از اصول و رویه‌ها است که براساس کاری انجام می‌شود (دیکشنری آکسفرد[1]). نظام مجموعه یا گروهی از اشـــیا مرتبط با غیر مرتبط اســـت که هدف یا اهدافی خاص را دنبال می‌کنند، به گونه‌ای که واحد پیچیده‌ای را تشـــکیل می‌دهند؛ نظام مجموعه‌ای از اجزایی اســـت کـــه بـــا هم کار می‌کنند و هدف معینی را دنبال می‌کنند. نظـــام تنها به نوع فیزیکی آن محدود نمی‌شـــود، مفهـــوم نظام را در مورد پدیده‌های مجرد پویا نظیـــر اقتصاد نیز می‌توان بکار برد. در تعریف علوم انســـانی، نظام را می‌توان مجموعه‌هایی از عناصر که برای انجام مأموریت با رسیدن به هدف خاصی با کمیت و کیفیت معلوم طراحی و ســـاخته شـــده و با کمیت و کیفیت معلوم با هم ترکیب شده‌اند، تعریف نمود. نظام مجموعه‌ای از عناصر است که برای رسیدن به یک هدف مشـــخص و مشترک گرد هم آمده‌اند، به طوری که بین این عناصر یک رابطه تعاملی وجود دارد (ملکان و سلیمانی، ۱۳۹۱).

داده و اطلاعات

داده را می‌توان حقایق، رویدادها، دیده‌ها و واقعیت‌های خام دانســـت که یک پدیده را به همان صورت اولیه خود تشـــریح و توصیف می‌کنند و ویژگی‌هایی از پدیده را انتقال می‌دهند. به عقیده تافلر[2] داده‌ها به قضایا و یا وقایع کوچکی گفته می‌شـــود که بین آنها ارتباطی وجود ندارد. داده‌ها چیزی بیش از مواد خام برای نظام‌های اطلاعاتی هستند. داده‌ها منابع سازمانی با ارزش را تشکیل می‌دهند. داده‌ها ارزش تجاری بالایی برای اراه‌دهندگان خدمات دارند (ژانگ[3]، ۲۰۱۸)

تاریخچه امنیت نظام اطلاعاتی

در اوایل دهه ۸۰ میلادی امنیت فقط با دیدگاه فنی مشـــاهده می‌شـــد و برقراری آن منوط به امنیت رایانه و دستگاه‌های جانبی می‌دانستند. اما با گذشت زمان متوجه شدند که بیشتر تجاوزات امنیتی از طریق مسائلی همچون ضعف‌های مدیریتی (از لحاظ امنیتی) و عوامل انسانی (به دلیل عدم آموزش) می‌باشـــد لذا از اواســـط دهه ۸۰ میلادی تا اواســـط دهه ۹۰ میلادی بحث امنیت

1. Oxford dictionary
2. Toffler
3. Zhang

نظام اطلاعاتی مطرح شـــد که آن را منوط به خط‌مشـــی امنیت اطلاعات و ساختارهای سازمانی و مؤلفه‌هایی چون استانداردهای امنیت اطلاعات، گواهی‌نامه‌های بین‌المللی، فرهنگ‌سازی امنیت اطلاعات در ســـازمان، پیاده ســـازی معیارهای ارزیابی دائمی و پویایی امنیت اطلاعات دانســـتند (سلیمانی اصیل، ۱۳۹۴).

تعاریف امنیت نظام اطلاعاتی

امنیـــت اطلاعات عمدتاً به حفاظـــت از اطلاعات و نظام‌های اطلاعاتی از دسترســـی غیرمجاز، استفاده، تخریب، اصلاح، بازرسی و بایگانی اشاره دارد (زو، ژانگ و چی[1]، ۲۰۱۷). واژه‌های امنیت اطلاعات، امنیت کامپیوتری و اطلاعات مطمئن گاه به اشـــتباه به جای هم بکار برده می‌شـــود. به طور خاص مفهوم امنیت اطلاعات شامل موارد زیر می‌باشد:

۱. محرمانه بودن اطلاعات: اطمینان از اینکه اطلاعات می‌توانند تنها در دسترس کسانی باشند که مجوز دارند.

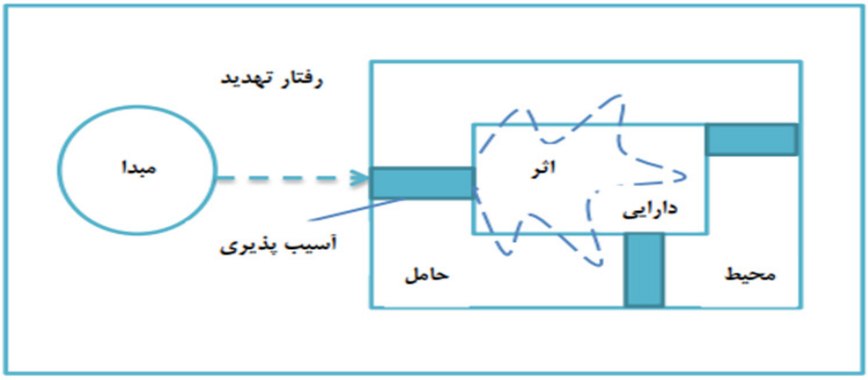
۲. صحـــت اطلاعـــات: حفاظت از دقـــت و صحت اطلاعات و راه‌های مناســـب پردازش آن اطلاعات.

۳. در دســـترس بودن اطلاعات: اطمینان از اینکه کاربران مجاز در هر زمان که نیاز داشـــته باشـــند، امکان دسترسی به اطلاعات وجود داشته باشـــد (حاجی زین‌العابدینی و رفعتی، ۱۳۹۶).

اجزاء امنیت نظام اطلاعاتی

امنیت نظام اطلاعاتی، عمدتاً به توانایی یک سازمان برای پرورش فرهنگی امنیتی وابسته است که در آن کارمندان به دســـتورالعمل‌ها، رویه‌ها و کنترل‌های فنی که در سیاست‌های امنیت نظام اطلاعاتی مشـــخص شده‌اند، پایبند هستند (دارســـی و ته[2]، ۲۰۱۹). امنیت نظام اطلاعاتی از پنج بخش تشکیل شده است. مبدأ، نوع و روش، کانال، گیرنده و نتیجه.

1. Xu, Zhang & Qi
2. D'Arcy & Teh



شکل ۱: اجزاء تشکیل دهنده امنیت نظام اطلاعاتی (غلامشاهی و شفیعی نیک آبادی، ۱۳۹۶)

فرایندهای تجارت سازمان‌ها به طور گسترده‌ای به نظام‌های اطلاعاتی و امنیت آن‌ها بستگی دارد. امنیت نظام اطلاعاتی به کاهش خطرات بالقوه کمک می‌کند (عباس، باینا و بل‌افکیه[1]، ۲۰۱۶). امنیت نظام اطلاعاتی یک فعالیت مستقل نیست، بلکه باید بر روی یک استراتژی امنیتی توسعه‌یافته، بنا شود (بارتون،تجی، لین و ترل[2]، ۲۰۱۶).

جدول ۱: نتایج پیاده‌سازی امنیت نظام اطلاعاتی (تقوا، جعفریان و شفیعی نیک آبادی، ۱۳۹۰)

ردیف	نتایج	توضیح
۱	دقت و صحت اطلاعات	از طریق ایجاد ساز وکار کنترل متمرکز نظام اطلاعاتی که شامل نظامی برای کنترل منشا پیدایش اطلاعات، عدم بروز مشکل در اثر اطلاعات غلط و توقف کارها به دلیل عدم دریافت به موقع اطلاعات است
۲	کنترل دقیق جابجایی‌های فیزیکی	شامل تمهیدات نظارت بر میزان موجودی انبارها و فرایند کنترل دقیق ورود و خروج کالاهاست

1. Abbass, baina & bellafkih
2. Barton, Tejay, Lane & Terrell

۳	جلوگیری از اشتباهات انسانی و سخت‌افزاری	شامل از بین نرفتن اطلاعات در اثر اشتباهات انسانی و یا خرابی، عدم تهدیدات عمدی، تهیه نسخه‌های پشتیبان و خطاناپذیرسازی کاربران است
۴	هماهنگی اطلاعات	شامل همخوانی نرم‌افزارهای مختلف و جمع‌آوری اطلاعات به صورت یکپارچه است که موجب جلوگیری از بازتولید اطلاعات نیز می‌گردد.
۵	درک و ایجاد یک نظام با توجه به نیاز افراد	از طریق نیازسنجی و طراحی مفهومی نظام و سخت‌افزارها بر اساس نیاز کاربران
۶	ایجاد زمینه آموزشی برای کاربران	شامل آموزش‌های لازم برای کار با نرم‌افزارها، با اینترنت و اینترانت

رضایی، مصدق و رضایی (۱۳۹۷) پژوهشـــی با عنوان «عوامل مؤثر بر اثربخشـــی نظام مدیریت امنیـــت اطلاعات» انجام دادند طبق نتایج پژوهش شـــاخص‌های نقش مدیریت، آگاهی از امنیت نظام اطلاعات و انطباق با آموزش، امنیت نظام اطلاعات کسب و کار و ارزیابی ریسک امنیت نظام اطلاعات بر اثربخشی نظام مدیریت امنیت اطلاعات تأثیرگذار می‌باشند. مستقیمی و امین موسوی (۱۳۹۷) پژوهشـــی با عنوان «مدلی برای بهبود پذیرش نظام مدیریت امنیت اطلاعات (ISMS) (مورد مطالعه یکی از سازمان‌های دولتی)» انجام دادند. نتایج نشان داد عواملی چون حمایت کامل مدیریت ارشد، کمیته راهبری شایسته با تصمیم به استفاده نظام مدیریت امنیت اطلاعات بیشترین مقدار رابطه مســـتقیم و مثبت را داشـــته و در نتیجه و بر پذیرش نظام مدیریت امنیت اطلاعات بیشـــترین تأثیر را می‌گذارند. احمدلو و احمدلو (۱۳۹٦) پژوهشـــی با عنوان «ارزیابی اثربخشـــی اســـتقرار نظام مدیریت امنیت اطلاعات» انجام دادند. نتایج نشـــان داد بین استقرار نظام مدیریت امنیت اطلاعات و اثربخشـــی ســـازمان ارتباط معناداری وجود دارد و استقرار نظام مدیریت امنیت اطلاعات در فعالیت‌های ســـازمان اثربخش اســـت. خیری (۱۳۹۵) پژوهشی با عنوان «شناسایی، تحلیل و رتبه‌بندی عوامل مؤثر کلیدی در پیاده‌سازی نظام مدیریت امنیت اطلاعات در سازمان‌های حاکمیتی (مطالعه موردی: ســـازمان بنادر و دریانوردی» انجام داد. شاخص‌ها در سه دسته عوامل فناوری و تکنولوژی، عوامل ســـازمانی یا درونی و عوامل خارجی برون ســـازمانی قرار گرفتند. که عامل فناوری و تکنولوژی با اهمیت‌ترین و عوامل خارجی برون سازمانی کم اهمیت‌ترین شناخته شد. نقی‌لو و احمدی (۱۳۹٤) پژوهشی با عنوان «شناسایی و اولویت‌بندی عوامل کلیدی موفقیت

پیاده‌سازی نظام‌های مدیریت امنیت اطلاعات در دانشگاه‌های ایران» انجام دادند. بر اساس نتایج آزمون فریدمن و تاپسیس فازی عامل فنی رتبه اول، عامل سازمانی رتبه دوم، عامل مدیریتی رتبه سوم، عامل فردی رتبه چهارم و عامل فرهنگی رتبه پنجم را به خود اختصاص دادند.

تو و یان[1] (۲۰۱۸) پژوهشی با عنوان «تراز ارزش استراتژیک برای مدیریت امنیت اطلاعات: تجزیه و تحلیل عوامل مهم موفقیت‌آمیز» انجام دادند. نتایج نشان می‌دهد که با هماهنگی کسب و کار، پشتیبانی از مدیریت ارشد و آگاهی سازمانی از خطرات و کنترل‌های امنیتی، کنترل مؤثر امنیت اطلاعات می‌تواند منجر به مدیریت امنیت اطلاعات موفق شوند. خواجوئی، کاظمی و موسوی‌راد[2] (۲۰۱۷) پژوهشی با عنوان «رتبه‌بندی کنترل‌های امنیتی اطلاعات با استفاده از فرایند تحلیل سلسله مراتبی فازی» انجام دادند مشخص شد که در میان اهداف ۳۹ گانه کنترل، مدیریت دسترسی کاربران و مدیریت تحویل خدمات شخص ثالث به ترتیب بیشترین و کمترین اولویت را دارند. کیلو و انزوکی[3] (۲۰۱۵) پژوهشی با عنوان «عوامل مؤثر بر پذیرش نظام‌های مدیریت امنیت اطلاعات: یک مرور نظری» انجام دادند. نتایج پژوهش حاکی از این بود که عواملی همچون تعهد مدیریت ارشد، ارتباطات اثربخش، آموزش، کیفیت فنی نظام اطلاعاتی، اندازه‌گیری منابع انسانی، فعالیت‌های مدیریت تغییر و اثربخشی آنها، سخت‌کوشی مدیریت پروژه، کیفیت برنامه‌های نظام اطلاعاتی، کار تیمی و ترکیب تیم نظام اطلاعاتی بر موفقیت نظام‌های مدیریت امنیت اطلاعات مؤثرند. علوی، اسلام، جهانخانی و النمراتی[4] (۲۰۱۵) پژوهشی با عنوان «تحلیل عوامل انسانی برای نظام مدیریت امنیت اطلاعات اثربخش» انجام دادند. نتایج نشان داد تعهد مدیریت ارشد، سیاست امنیت اطلاعات و آگاهی و آموزش کارکنان می‌تواند ۸۴ درصد از تغییرات اثربخشی نظام‌های اطلاعاتی را پیش‌بینی کنند. ابوسعد، سعید، الغدبر و خان[5] (۲۰۱۱) پژوهشی با عنوان «پیاده‌سازی ایزو ۲۷۰۰۱ در عربستان سعودی- موانع، انگیزه‌ها، نتایج و درس‌های آموخته شده» انجام داد. نتایج نشان داد با اینکه رضایت مشتری و نیز ارتباطات خوب با مشتریان برای زنده ماندن یک سازمان ضروری می‌باشد هیچ سازمانی نشان نداده است که برآورده کردن نیازهای مشتریان یا قوانین مربوط به شرکاء جزء اهداف آنها می‌باشد یا نه.

1. Tu & Yuan
2. Khajouei, Kazemi & Moosavirad
3. Kiilu & Nzuki
4. Alavi, Islam, Jahankhani & Al-Nemrat
5. AbuSaad, Saeed, Alghathbar & Khan

جدول ۲: معیارهای مؤثر اثربخشی امنیت نظام‌های اطلاعاتی (منبع: ادبیات پژوهش)

معیار	ردیف	زیرمعیار	پژوهش
سازمانی	۱	بکارگیری رویکرد و چارچوبی سازگار با فرهنگ سازمان برای پیاده‌سازی، حفظ، نظارت و بهبود امنیت اطلاعات	توریس، ساریگی، سانتوس و سیرانو (۲۰۰۶)، ابوسعد، سعید، الغدبر و خان (۲۰۱۱)، علوی، اسلام، جهانخانی و النمراتی (۲۰۱۵)، کیلو و انزوکی (۲۰۱۵)، تو و یان (۲۰۱۸)، صفرخانی و شیرمحمدی (۱۳۸۸)، نقی‌لو و احمدی (۱۳۹٤)، خیری (۱۳۹۵) و مستقیمی و امین موسوی (۱۳۹۷)
	۲	هماهنگی ساختار سازمانی با نیازهای نظام مدیریت امنیت اطلاعات	
	۳	برخوردار بودن از کمیته راهبردی شایسته	
	۴	ثبات مدیریت ارشد سازمان	
	۵	تدارک و تأمین بودجه لازم برای فعالیت‌های مدیریت امنیت توسط سازمان	
مدیریتی	۶	توزیع استانداردها و راهنمای سیاست امنیت اطلاعات در میان همه مدیران، کارمندان و سایر گروه‌ها	تایی و گریوال (۲۰۰۵)، توریس، ساریگی، سانتوس و سیرانو (۲۰۰۶)، ابوسعد، سعید، الغدبر و خان (۲۰۱۱)، ماروا (۲۰۱۵)، کیلو و انزوکی (۲۰۱۵)، خواجوئی، کاظمی و موسوی‌راد (۲۰۱۷)، تو و یان (۲۰۱۸)، صفرخانی و شیرمحمدی (۱۳۸۸)، نقی‌لو و احمدی (۱۳۹٤)، خیری (۱۳۹۵)، مستقیمی و امین موسوی (۱۳۹۷) و رضایی، مصدق و رضایی (۱۳۹۷)
	۷	وجود برنامه‌ای جهت بهبود و تقویت مدیریت امنیت در سراسر سازمان (سبک مدیریت)	
	۸	حمایت کامل و مشارکت مدیریت ارشد	
	۹	درک دقیق مسأله امنیت اطلاعات از طرف مدیریت و اجراکنندگان نظام، ارزیابی ریسک و مدیریت نظام	
	۱۰	همسویی هدف‌های سیاست امنیت اطلاعات با اهداف تجاری سازمان (هم ترازی هدف‌ها)	
	۱۱	تعیین و بیان ارزش تجاری امنیت اطلاعات با استفاده از یک ریسک رایج و معیارهایی استاندارد توسط مدیران امنیت اطلاعات	
	۱۲	مدیریت متمرکز امنیت اطلاعات مبتنی بر یک استراتژی و سیاست مشترک در سازمان	

معیار	ردیف	زیرمعیار	پژوهش
فردی	۱۳	تداخل نداشتن مسئولیت‌های کارکنان	توریس، ساریگی، سانتوس و سیرانو (۲۰۰۶)، کیلو و انزوکی (۲۰۱۵)، خواجوئی، کاظمی و موسوی‌راد (۲۰۱۷)، تو و یان (۲۰۱۸)، نقی‌لو و احمدی (۱۳۹٤)، خیری (۱۳۹۵) و مستقیمی و امین موسوی (۱۳۹۷)
	۱۴	همکاری و هماهنگی داشتن کارکنان درگیر در پروژه	
	۱۵	مصرف عاقلانه و قابل قبول منابع سازمانی، به منظور اجرای امنیت توسط مجریان امنیت اطلاعات (مانند پول، نیروی انسانی شایسته، زمان و ...)	
فرهنگی	۱۶	تبلیغات مناسب جهت آگاهی مدیران، کارکنان و سایر گروه‌ها در خصوص ارزش امنیت اطلاعات	تایی و گریوال (۲۰۰۵)، ابوسعد، سعید، الغدبر و خان (۲۰۱۱)، علوی، اسلام، جهانخانی و النمراتی (۲۰۱۵)، ماروا (۲۰۱۵)، تو و یان (۲۰۱۸)، نقی‌لو و احمدی (۱۳۹٤)، خیری (۱۳۹۵)، مستقیمی و امین موسوی (۱۳۹۷) و رضایی، مصدق و رضایی (۱۳۹۷)
	۱۷	ایجاد انگیزش در کارکنان کل سازمان (در جهت پذیرش مقررات و دستورالعمل‌ها)	
	۱۸	بالا بودن میزان رضایت شغلی کارکنان	
	۱۹	مایل بودن سازمان به بازمهندسی فرایندهایش	

معیار	ردیف	زیرمعیار	پژوهش
فنی	۲۰	برخوردار بودن از زیرساخت مناسب فناوری اطلاعات	تایی و گریوال (۲۰۰۵)، توریس، ساریگی، سانتوس و سیرانو (۲۰۰۶)، ابوسعد، سعید، الغدبر و خان (۲۰۱۱)، ماروا (۲۰۱۵)، کیلو و انزوکی (۲۰۱۵)، نقی‌لو و احمدی (۱۳۹٤)، خیری (۱۳۹۵) و مستقیمی و امین موسوی (۱۳۹۷)
	۲۱	تدوین مناسب خط مشی امنیت اطلاعات (پیروی از یک استاندارد به عنوان یک مدل مرجع یکسان)	
	۲۲	استفاده از افراد نخبه و متخصصان و مشاوران امنیت اطلاعات و ممیزین خارجی با توانایی بیشتر	
	۲۳	تعریف درست قلمرو استقرار نظام مدیریت امنیت اطلاعات (ساختاردهی و برنامه‌ریزی پیاده‌سازی نظام مدیریت امنیت اطلاعات در سازمان)	
	۲۴	ایجاد یک نظام اندازه‌گیری برای ارزیابی کارایی نظام مدیریت امنیت اطلاعات	
	۲۵	بازبینی و تجدید نظر مؤثر فرایندهای اجرا شده نظام مدیریت امنیت اطلاعات (بررسی اثربخشی نظام)	
	۲۶	مستندسازی سیاست‌های تعیین شده	
	۲۷	شناسایی آسیب‌پذیری‌ها و تهدیدات	
	۲۸	محاسبه میزان مخاطرات سازمان به ازای هر دارایی با برقراری تناظر بین آسیب‌پذیری‌ها و تهدیدات	
	۲۹	تعیین میزان تأثیرگذاری آسیب‌پذیری‌ها و شدت اثر تهدیدات و اولویت‌بندی عوامل تأثیرگذار در مخاطرات	

۲. روش‌شناسی تحقیق

پژوهش حاضر از نظر هدف، پژوهشـــی کاربردی اســـت. این پژوهش از نظر ماهیت، توسعه‌ای-اکتشـــافی می‌باشـــد زیرا با رویکرد ترکیبی دیمتل و ا.ان.پی به شناسایی معیارهای مؤثر اثربخشی

امنیـــت نظام‌های اطلاعاتی می‌پردازد. از منظر افق زمانی، پژوهش حاضر را می‌توان از نوع مطالعه مقطعی دانســـت. جامعه آماری مورد مطالعه، کلیه کارکنان ســـازمان فناوری اطلاعات و ارتباطات شـــهرداری کلان شهر اهواز می‌باشند. حجم جامعه طبق آخرین اطلاعات اخذ شده از واحد منابع انســـانی این ســـازمان برابر ۵۰ نفر اســـت. در این پژوهش ۱۰ نفر از افراد با سابقه بالای ۱۰ سال، مسلط به فناوری اطلاعات و تصمیم‌گیرنده ارشد در سازمان به عنوان نمونه انتخاب شده‌اند. روش نمونه‌گیری نیز گلوله برفی بود. روش گردآوری داده‌ها در این پژوهش، به صورت میدانی اســـت. با اســـتفاده از پرسشـــنامه دلفی، دیمتل و ا.ان.پی، به معیارهای مؤثر اثربخشـــی امنیت نظام‌های اطلاعاتی شـــهرداری کلان شـــهر اهواز پرداخته شد. در این پژوهش از پرسشنامه برای جمع‌آوری داده در چهار مرحله پرسشنامه توزیع گردید.

- در پرسشنامه اولیه و ثانویه با استفاده از طیف پنج‌گانه (۱-۹) میزان اهمیت هر یک از معیارها و زیرمعیارها ســـنجیده شـــد. لازم به ذکر است که پرسشنامه اولیه شامل ۳۴ سؤال (۵ معیار و ۲۹ زیرمعیار) و پرسشـــنامه ثانویه شـــامل ۳۲ سؤال (۵ معیار اصلی و ۲۷ زیرمعیار) در نظر گرفته شد.
- در گام بعد به منظور تعیین روابط تأثیر و تأثر بین معیارهای پژوهش پرسشنامه دیمتل طراحی شد. این پرسشنامه در بین ۱۰ نفر از کارکنان سازمان فناوری اطلاعات و ارتباطات شهرداری کلان شـــهر اهواز با سابقه بالای ۱۰ سال، مسلط به فناوری اطلاعات و و تصمیم‌گیرنده ارشد در سازمان توزیع شد.
- در گام آخر به منظور تعیین وزن هر یک از معیارها و زیرمعیارها در مقایسه با یکدیگر پرسشنامه مقایســـات زوجی میان معیارها و زیرمعیارها طراحی شد. این پرسشنامه که پرسشنامه اصلی روش ا.ان.پی است، در بین ۱۰ نفر از کارکنان سازمان فناوری اطلاعات و ارتباطات شهرداری کلان شهر اهواز با سابقه بالای ۱۰ سال، مسلط به فناوری اطلاعات و تصمیم‌گیرنده ارشد در سازمان توزیع شد. برای سنجش میزان اهمیت از طیف نه‌گانه دو قطبی استفاده شد.

جدول ۳: مقیاس اندازه‌گیری معیارها و زیرمعیارها در روش ا.ان.پی

میزان اهمیت	اهمیت یکسان	بینابین	کمی مهم	بینابین	مهم	بینابین	خیلی مهم	بینابین	کاملاً مهم
امتیاز	۱	۲	۳	۴	۵	۶	۷	۸	۹

برای کسب اطمینان از میزان روایی پرسشنامه‌ها، مراحل زیر طی گردید:

الف. مطالعه دقیق منابع مختلف موجود و در دسترس و مباحث مرتبط با موضوعات آنها؛

ب. اخذ نظرات خبرگان؛

در این تحقیق همان‌طور که ذکر شد پس از جمع‌آوری پرسشنامه‌های مرحله اول و دوم، داده‌ها وارد نرم‌افزار اس.پی.اس.اس گردید و پایایی با اســـتفاده از روش آلفای کرونباخ ۰/۸۷۶ و ۰/۸۹۲ محاسبه گردید که حاکی از پایایی پرسشنامه تحقیق است.

جهـــت تحلیـــل داده‌ها از تکنیک دلفـــی، آزمون t تک نمونه‌ای، روش دیمتـــل و روش ا.ان.پی استفاده شد.

در پژوهش حاضر سوالات زیر مطرح هستند:

- معیارهای مؤثر اثربخشی امنیت نظام‌های اطلاعاتی شهرداری کلان شهر اهواز با روش دلفی کدامند؟
- رابطه میان معیارهای مؤثر اثربخشـــی امنیت نظام‌های اطلاعاتی شهرداری کلان شهر اهواز با روش دیمتل به چه صورت است؟
- وزن معیارهای مؤثر اثربخشـــی امنیت نظام‌های اطلاعاتی شهرداری کلان شهر اهواز با روش ا.ان.پی به چه صورت است؟
- اولویت‌بندی معیارهای مؤثر اثربخشـــی امنیت نظام‌های اطلاعاتی شهرداری کلان شهر اهواز با روش ا.ان.پی چه صورت است؟

۳. تجزیه و تحلیل یافته‌ها

جدول ٤: معیارهای مؤثر اثربخشی امنیت نظام‌های اطلاعاتی شهرداری کلان شهر اهواز

ردیف	زیرمعیار	معیار
۱	بکارگیری رویکرد و چارچوبی سازگار با فرهنگ سازمان برای پیاده‌سازی، حفظ، نظارت و بهبود امنیت اطلاعات	سازمانی
۲	هماهنگی ساختار سازمانی با نیازهای نظام مدیریت امنیت اطلاعات	
۳	برخوردار بودن از کمیته راهبردی شایسته	
۴	ثبات مدیریت ارشد سازمان	
۵	تدارک و تأمین بودجه لازم برای فعالیت‌های مدیریت امنیت توسط سازمان	
۶	توزیع استانداردها و راهنمای سیاست امنیت اطلاعات در میان همه مدیران، کارمندان و سایر گروه‌ها	مدیریتی
۷	وجود برنامه‌ای جهت بهبود و تقویت مدیریت امنیت در سراسر سازمان (سبک مدیریت)	
۸	حمایت کامل و مشارکت مدیریت ارشد	
۹	درک دقیق مسأله امنیت اطلاعات از طرف مدیریت و اجراکنندگان نظام، ارزیابی ریسک و مدیریت نظام	
۱۰	همسویی هدف‌های سیاست امنیت اطلاعات با اهداف تجاری سازمان (هم ترازی هدف‌ها)	
۱۱	تعیین و بیان ارزش تجاری امنیت اطلاعات با استفاده از یک ریسک رایج و معیارهایی استاندارد توسط مدیران امنیت اطلاعات	
۱۲	مدیریت متمرکز امنیت اطلاعات مبتنی بر یک استراتژی و سیاست مشترک در سازمان	
۱۳	تداخل نداشتن مسئولیت‌های کارکنان	فردی
۱۴	همکاری و هماهنگی داشتن کارکنان درگیر در پروژه	
۱۵	مصرف عاقلانه و قابل قبول منابع سازمانی، به منظور اجرای امنیت توسط مجریان امنیت اطلاعات (مانند پول، نیروی انسانی شایسته، زمان و ...)	

ردیف	زیرمعیار	معیار
۱۶	تبلیغات مناسب جهت آگاهی مدیران، کارکنان و سایر گروه‌ها در خصوص ارزش امنیت اطلاعات	فرهنگی
۱۷	ایجاد انگیزش در کارکنان کل سازمان (در جهت پذیرش مقررات و دستورالعمل‌ها)	
۱۸	بالا بودن میزان رضایت شغلی کارکنان	
۱۹	مایل بودن سازمان به بازمهندسی فرایندهایش	
۲۰	برخوردار بودن از زیرساخت مناسب فناوری اطلاعات	فنی
۲۱	تدوین مناسب خط مشی امنیت اطلاعات (پیروی از یک استاندارد به عنوان یک مدل مرجع یکسان)	
۲۲	استفاده از افراد نخبه و متخصصان و مشاوران امنیت اطلاعات و ممیزین خارجی با توانایی بیشتر	
۲۳	تعریف درست قلمرو استقرار نظام مدیریت امنیت اطلاعات (ساختاردهی و برنامه‌ریزی پیاده‌سازی نظام مدیریت امنیت اطلاعات در سازمان)	
۲۴	ایجاد یک نظام اندازه‌گیری برای ارزیابی کارایی نظام مدیریت امنیت اطلاعات	
۲۵	بازبینی و تجدید نظر مؤثر فرایندهای اجرا شده نظام مدیریت امنیت اطلاعات (بررسی اثربخشی نظام)	
۲۶	شناسایی آسیب‌پذیری‌ها و تهدیدات	
۲۷	محاسبه میزان مخاطرات سازمان به ازای هر دارایی با برقراری تناظر بین آسیب‌پذیری‌ها و تهدیدات	

شکل ۲: در خت تصمیم گیری نهایی پژوهش حاضر

پیاده‌سازی تکنیک دیمتل

جدول ۵: نتیجه گیری و اولویت بندی معیارها

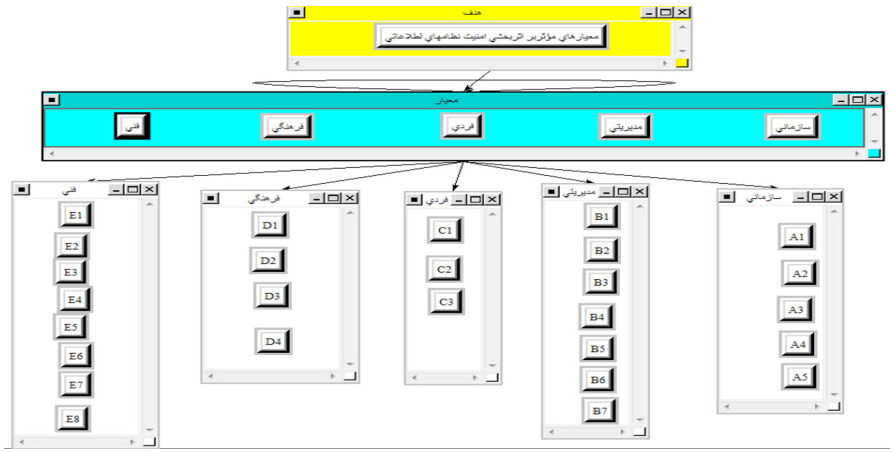
نتیجه	R	J	R+J	R-J
سازمانی	۱/۶۵۴۵	۲/۲۴۲۳	۳/۸۹۶۸	-۰/۵۸۷۹
مدیریتی	۲/۸۸۲۵	۱/۷۹۱۷	۴/۶۷۴۲	۱/۰۹۰۷
فردی	۱/۶۷۱۸	۲/۳۵۸۸	۴/۰۳۰۶	-۰/۶۸۷۰
فرهنگی	۲/۱۹۵۰	۲/۰۳۴۶	۴/۲۲۹۶	۰/۱۶۰۴
فنی	۱/۹۷۹۴	۱/۹۵۵۷	۳/۹۳۵۱	۰/۰۲۳۷

مشـــاهده می‌شـــود که از مقدار R+J، هر چی عدد بزرگتری باشـــد یعنی، محوریت معیار در معیارهای مؤثر اثربخشـــی امنیت نظام‌های اطلاعاتی شهرداری کلان شهر اهواز بیشتر است که با توجه به نتایج بدســـت آمده معیار مدیریتی بیشـــترین تعامل و معیار سازمانی کمترین تعامل را با دیگر معیارها دارد.

جدول ٦: ماتریس تأثیرگذاری و عدم تأثیرگذاری معیارها بر یکدیگر

ماتریس روابط کل	سازمانی	مدیریتی	فردی	فرهنگی	فنی
سازمانی	۰	۰	۰	۰	۰
مدیریتی	۰/۶۴۵۹	۰/۳۵۹۸	۰/۶۵۷۱	۰/۶۰۳۷	۰/۶۱۶۰
فردی	۰	۰	۰	۰	۰
فرهنگی	۰/۴۹۴۲	۰/۴۳۰۹	۰/۵۶۰۵	۰	۰/۳۹۸۵
فنی	۰/۴۶۲۶	۰/۳۸۷۸	۰	۰/۴۱۰۱	۰

پیاده‌سازی تکنیک ا.ان.پی



شکل ۳: نمودار درختچه‌ای تحلیل ا.ان.پی

جدول ۷: اولویت‌بندی معیارهای اصلی

ردیف	معیارهای اصلی	وزن	اولویت
۱	سازمانی	۰/۱۹۰۹	۳
۲	مدیریتی	۰/۲۸۶۵	۱
۳	فردی	۰/۱۵۷۱	۴
۴	فرهنگی	۰/۱۳۴۱	۵
۵	فنی	۰/۲۳۱۴	۲

جدول ۸: مقایسه وزن نسبی و درصد وزن نهایی هر یک از معیارها و زیرمعیارها

معیار	وزن نسبی	زیرمعیار	وزن نسبی	درصد وزن نهایی
سازمانی	۰/۱۹۰۹	بکارگیری رویکرد و چارچوبی سازگار با فرهنگ سازمان برای پیاده‌سازی، حفظ، نظارت و بهبود امنیت اطلاعات	۰/۲۷۳۳	۵,۲۱۷
		هماهنگی ساختار سازمانی با نیازهای نظام مدیریت امنیت اطلاعات	۰/۱۳۷۵	۲,۶۲۵
		برخوردار بودن از کمیته راهبردی شایسته	۰/۱۹۵۱	۳,۷۲۴
		ثبات مدیریت ارشد سازمان	۰/۱۶۲۰	۳,۰۹۳
		تدارک و تأمین بودجه لازم برای فعالیت‌های مدیریت امنیت توسط سازمان	۰/۲۳۲۲	۴,۴۳۳
مدیریتی	۰/۲۸۶۵	توزیع استانداردها و راهنمای سیاست امنیت اطلاعات در میان همه مدیران، کارمندان و سایر گروه‌ها	۰/۱۰۱۴	۲,۹۰۵
		وجود برنامه‌ای جهت بهبود و تقویت مدیریت امنیت در سراسر سازمان (سبک مدیریت)	۰/۲۱۲۸	۶,۰۹۷
		حمایت کامل و مشارکت مدیریت ارشد	۰/۱۸۴۴	۵,۲۸۳
		درک دقیق مسأله امنیت اطلاعات از طرف مدیریت و اجراکنندگان نظام، ارزیابی ریسک و مدیریت نظام	۰/۱۵۷۲	۴,۵۰۴
		همسویی هدف‌های سیاست امنیت اطلاعات با اهداف تجاری سازمان (هم ترازی هدف‌ها)	۰/۰۸۷۵	۲,۵۰۷
		تعیین و بیان ارزش تجاری امنیت اطلاعات با استفاده از یک ریسک رایج و معیارهایی استاندارد توسط مدیران امنیت اطلاعات	۰/۱۳۸۲	۳,۹۵۹
		مدیریت متمرکز امنیت اطلاعات مبتنی بر یک استراتژی و سیاست مشترک در سازمان	۰/۱۱۸۵	۳,۳۹۵

معیار	وزن نسبی	زیرمعیار	وزن نسبی	درصد وزن نهایی
فردی	۰/۱۵۷۱	تداخل نداشتن مسئولیت‌های کارکنان	۰/۲۷۳۳	۴,۲۹۴
		همکاری و هماهنگی داشتن کارکنان درگیر در پروژه	۰/۳۹۸۹	۶,۲۶۷
		مصرف عاقلانه و قابل قبول منابع سازمانی، به منظور اجرای امنیت توسط مجریان امنیت اطلاعات (مانند پول، نیروی انسانی شایسته، زمان و ...)	۰/۳۲۷۶	۵,۱۴۷
فرهنگی	۰/۱۳۴۱	تبلیغات مناسب جهت آگاهی مدیران، کارکنان و سایر گروه‌ها در خصوص ارزش امنیت اطلاعات	۰/۲۷۱۸	۳,۶۴۵
		ایجاد انگیزش در کارکنان کل سازمان (در جهت پذیرش مقررات و دستورالعمل‌ها)	۰/۲۲۴۶	۳,۰۱۲
		بالا بودن میزان رضایت شغلی کارکنان	۰/۳۲۲۱	۴,۳۱۹
		مایل بودن سازمان به بازمهندسی فرایندهایش	۰/۱۸۱۳	۲,۴۳۱

معیار	وزن نسبی	زیرمعیار	وزن نسبی	درصد وزن نهایی
فنی	۰/۲۳۱۴	برخوردار بودن از زیرساخت مناسب فناوری اطلاعات	۰/۱۹۲۱	۴,۴۴۵
		تدوین مناسب خط مشی امنیت اطلاعات (پیروی از یک استاندارد به عنوان یک مدل مرجع یکسان)	۰/۱۷۴۵	۴,۰۳۸
		استفاده از افراد نخبه و متخصصان و مشاوران امنیت اطلاعات و ممیزین خارجی با توانایی بیشتر	۰/۱۵۳۹	۳,۵۶۱
		تعریف درست قلمرو استقرار نظام مدیریت امنیت اطلاعات (ساختاردهی و برنامه‌ریزی پیاده‌سازی نظام مدیریت امنیت اطلاعات در سازمان)	۰/۰۸۷۸	۲,۰۳۲
		ایجاد یک نظام اندازه‌گیری برای ارزیابی کارایی نظام مدیریت امنیت اطلاعات	۰/۱۰۶۲	۲,۴۵۷
		بازبینی و تجدید نظر مؤثر فرایندهای اجرا شده نظام مدیریت امنیت اطلاعات (بررسی اثربخشی نظام)	۰/۱۲۰۳	۲,۷۸۴
		شناسایی آسیب‌پذیری‌ها و تهدیدات	۰/۰۹۵۱	۲,۲۰۱
		محاسبه میزان مخاطرات سازمان به ازای هر دارایی با برقراری تناظر بین آسیب‌پذیری‌ها و تهدیدات	۰/۰۶۹۹	۱,۶۱۷

۴. نتیجه‌گیری

در این پژوهش ۳ عامل و ۱۶ زیرعامل بی‌اهمیت شناخته شدند. زیرمعیارهای شناسایی شده با توجه به نتایج دور اول و دوم دلفی عبارتند از:

- سازمانی: بکارگیری رویکرد و چارچوبی سازگار با فرهنگ سازمان برای پیاده‌سازی، حفظ، نظارت و بهبود امنیت اطلاعات؛ هماهنگی ساختار سازمانی با نیازهای نظام مدیریت امنیت اطلاعات؛ برخوردار بودن از کمیته راهبردی شایسته؛ ثبات مدیریت ارشد سازمان؛ تدارک و تأمین بودجه لازم برای فعالیت¬های مدیریت امنیت توسط سازمان
- مدیریتی: توزیع استانداردها و راهنمای سیاست امنیت اطلاعات در میان همه مدیران، کارمندان و سایر گروه‌ها؛ وجود برنامه‌ای جهت بهبود و تقویت مدیریت امنیت در سراسر سازمان (سبک مدیریت)؛ حمایت کامل و مشارکت مدیریت ارشد؛ درک دقیق مسأله امنیت اطلاعات از طرف مدیریت و اجراکنندگان نظام، ارزیابی ریسک و مدیریت نظام؛ همسویی هدف‌های سیاست امنیت اطلاعات با اهداف تجاری سازمان (هم ترازی هدف‌ها)؛ تعیین و بیان ارزش تجاری امنیت اطلاعات با استفاده از یک ریسک رایج و معیارهایی استاندارد توسط مدیران امنیت اطلاعات؛ مدیریت متمرکز امنیت اطلاعات مبتنی بر یک استراتژی و سیاست مشترک در سازمان
- فردی: تداخل نداشتن مسئولیت‌های کارکنان؛ همکاری و هماهنگی داشتن کارکنان درگیر در پروژه؛ مصرف عاقلانه و قابل قبول منابع سازمانی؛ به منظور اجرای امنیت توسط مجریان امنیت اطلاعات (مانند پول، نیروی انسانی شایسته، زمان و ...)
- فرهنگی: تبلیغات مناسب جهت آگاهی مدیران، کارکنان و سایر گروه‌ها در خصوص ارزش امنیت اطلاعات؛ ایجاد انگیزش در کارکنان کل سازمان (در جهت پذیرش مقررات و دستورالعمل‌ها)؛ بالا بودن میزان رضایت شغلی کارکنان؛ مایل بودن سازمان به بازمهندسی فرایندهایش
- فنی: برخوردار بودن از زیرساخت مناسب فناوری اطلاعات؛ تدوین مناسب خط مشی امنیت اطلاعات (پیروی از یک استاندارد به عنوان یک مدل مرجع یکسان)؛ استفاده از افراد نخبه و متخصصان و مشاوران امنیت اطلاعات و ممیزین خارجی با توانایی بیشتر؛ تعریف درست قلمرو استقرار نظام مدیریت امنیت اطلاعات (ساختاردهی و برنامه‌ریزی پیاده‌سازی نظام مدیریت امنیت اطلاعات در سازمان)؛ ایجاد یک نظام اندازه‌گیری برای ارزیابی کارایی نظام مدیریت

امنیت اطلاعات؛ بازبینی و تجدید نظر مؤثر فرایندهای اجرا شده نظام مدیریت امنیت اطلاعات (بررسی اثربخشی نظام)؛ شناسایی آسیب‌پذیری‌ها و تهدیدات؛ محاسبه میزان مخاطرات سازمان به ازای هر دارایی با برقراری تناظر بین آسیب‌پذیری‌ها و تهدیدات

همچنانکه در جدول (۸) نیز دیده می‌شود در میان معیارهای اصلی پژوهش، معیار «مدیریتی» با وزن نسبی ۰/۲۸۶۵ بیشترین اهمیت را دارد و معیار «فرهنگی» با وزن نسبی ۰/۱۳۴۱ در اولویت آخر قرار دارد. همچنین معیارهای فنی، سازمانی و فرهنگی به ترتیب در رتبه دوم تا چهارم قرار گرفتند.

همچنانکه در جدول (۸) نیز دیده می‌شود در میان زیرمعیارهای سازمانی، زیرمعیار «بکارگیری رویکرد و چارچوبی سازگار با فرهنگ سازمان برای پیاده‌سازی، حفظ، نظارت و بهبود امنیت اطلاعات» با وزن نسبی ۰/۲۷۳۳ بیشترین اهمیت را دارد و زیرمعیار «هماهنگی ساختار سازمانی با نیازهای نظام مدیریت امنیت اطلاعات» با وزن نسبی ۰/۱۳۷۵ در اولویت آخر قرار دارد. نتایج پژوهش همسو با نتایج پژوهش توریس، ساریگی، سانتوس و سیرانو (۲۰۰۶)، ابوسعد، سعید، الغدبر و خان (۲۰۱۱)، علوی، اسلام، جهانخانی و النمراتی (۲۰۱۵)، کیلو و انزوکی (۲۰۱۵)، تو و یان (۲۰۱۸)، صفرخانی و شیرمحمدی (۱۳۸۸)، نقی‌لو و احمدی (۱۳۹٤)، خیری (۱۳۹۵) و مستقیمی و امین موسوی (۱۳۹۷) می‌باشد. تأثیر عوامل سازمانی بر اثربخشی امنیت نظام‌های اطلاعاتی مورد توجه پژوهشگران متعددی قرار گرفته است؛ بدین صورت که از اصطلاح‌های متفاوتی مانند زمینه‌ها، متغیرها و عواملی که به ابعاد سازمانی مربوط می‌شود، استفاده کرده‌اند. سازمان‌هایی که نسبت به امنیت نظام‌های اطلاعاتی از آگاهی لازم برخوردارند، ممکن است راهکارهای بهتری در زمینه مسائل امنیتی داشته باشد و به اهداف سازمان به نحو مطلوبتری دست یابند. در سازمان‌هایی که فرایندهای رسمی ایجاد شده است، آمادگی پذیرش شیوه‌های نوین امنیتی بهتری مشاهده می‌شود.

همچنانکه در جدول (۸) نیز دیده می‌شود در میان زیرمعیارهای مدیریتی، زیرمعیار «وجود برنامه‌ای جهت بهبود و تقویت مدیریت امنیت در سراسر سازمان (سبک مدیریت)» با وزن نسبی ۰/۲۱۲۸ بیشترین اهمیت را دارد و زیرمعیار «همسویی هدف‌های سیاست امنیت اطلاعات با اهداف تجاری سازمان (هم‌ترازی هدف‌ها)» با وزن نسبی ۰/۰۸۷۵ در اولویت آخر قرار دارد. نتایج پژوهش همسو با نتایج پژوهش تایی و گریوال (۲۰۰۵)، توریس، ساریگی، سانتوس و سیرانو (۲۰۰۶)، ابوسعد، سعید، الغدبر و خان (۲۰۱۱)، ماروا (۲۰۱۵)، کیلو و انزوکی (۲۰۱۵)، خواجوئی،

کاظمی و موســـوی‌راد (۲۰۱۷)، تو و یان (۲۰۱۸)، صفرخانی و شـــیرمحمدی (۱۳۸۸)، نقی‌لو و احمدی (۱۳۹٤)، خیری (۱۳۹۵)، مستقیمی و امین موسوی (۱۳۹۷) و رضایی، مصدق و رضایی (۱۳۹۷) می‌باشـــد. طرح‌های تحقیقاتی مختلف در خصوص روانشناســـی سازمانی نشان داده‌اند که ســـطح بالایی از تعهد مدیریت در ســـازمان نقش تعیین‌کننده‌ای در اثربخشی امنیت نظام‌های اطلاعاتی دارد. مشـــارکت مدیریت ارشـــد محرک غالب تلاش‌های سازمان می‌باشد. سازمان‌هایی که از حمایت و تعهد مدیریتی بیشـــتر در برنامه‌های اطلاعاتی برخوردارند، عملکرد سالانه بهتری داشـــته و از مزیت رقابتی بالاتری نیز نســـبت به رقبا برخوردار خواهند بود. در صورتی که مدیریت ارشد بتواند چشم‌انداز مناسبی برای فعالیت‌های امنیت نظام‌های اطلاعاتی قائل شده و برنامه‌های مربوط به این حوزه را به عنوان یک فاکتور مهم در بحث تصمیم‌گیری‌های استراتژیک وارد نماید، فعالیت‌های امنیت نظام‌های اطلاعاتی به بهترین شکل صورت خواهند گرفت.

همچنانکه در جدول (۸) نیز دیده می‌شـــود در میـــان زیرمعیارهای فردی، زیرمعیار «همکاری و هماهنگی داشـــتن کارکنان درگیر در پروژه» با وزن نســـبی ۰/۳۹۸۹ بیشترین اهمیت را دارد و زیرمعیار «تداخل نداشـــتن مســـئولیت‌های کارکنان» با وزن نسبی ۰/۲۷۳۳ در اولویت آخر قرار دارد. نتایج پژوهش همســـو با نتایج پژوهش توریس، ســـاریگی، سانتوس و سیرانو (۲۰۰۶)، کیلو و انزوکـــی (۲۰۱۵)، خواجوئی، کاظمی و موســـوی‌راد (۲۰۱۷)، تو و یان (۲۰۱۸)، نقی‌لو و احمدی (۱۳۹٤)، خیری (۱۳۹۵) و مســـتقیمی و امین موســـوی (۱۳۹۷) می‌باشد. گونزالز عامل فردی را به عنوان پاشـــنه آشـــیل امنیت نظام‌های اطلاعاتی معرفی کرده است. شرکت ای.بی.ام (۲۰۰۶) بیان کرده اســـت که یکی از مهمترین کانون‌های توجه نفوذگران، «ســـهل انگاری و ساده اندیشی افراد» اســـت. به گفته ماکی، رئیس بخش آگاهی شرکت کامپیوتری آرمونک، «افراد» همچنان به عنوان ســـست‌ترین عنصر آســـیب‌پذیر در مدل‌های امنیتی، مورد سوء استفاده قرار خواهد گرفت. وی در ســـال (۲۰۰۴) مقاله‌ای با عنوان «ده خطـــای مهلک مدیریت امنیت نظام‌های اطلاعاتی» منتشـــر کرد. در این مقاله ده خطای زیر به عنوان خطاهای مهلک امنیت نظام‌های اطلاعاتی ذکر شـــدند و بیان شـــد که حتی اگر یکی از این جنبه‌ها نادیده گرفته شـــود و یا به درستی مورد توجه قرار نگیرد، مشـــکلاتی جدی در حفظ یک برنامه امنیت نظام‌های اطلاعاتی وجود خواهد داشـــت. قسمت عمده‌ای از این خطاها مبتنی بر عوامل فردی می‌باشد.

همچنانکه در جدول (۸) نیز دیده می‌شود در میان زیرمعیارهای فرهنگی، زیرمعیار «بالا بودن میزان رضایت شـــغلی کارکنان» با وزن نسبی ۰/۳۲۲۱ بیشترین اهمیت را دارد و زیرمعیار «مایل

بودن سازمان به بازمهندسی فرایندهایش» با وزن نسبی ۰/۱۸۱۳ در اولویت آخر قرار دارد. نتایج پژوهش همسو با نتایج پژوهش تایی و گریوال (۲۰۰۵)، ابوسعد، سعید، الغدبر و خان (۲۰۱۱)، علوی، اسلام، جهانخانی و النمراتی (۲۰۱۵)، ماروا (۲۰۱۵)، تو و یان (۲۰۱۸)، نقی‌لو و احمدی (۱۳۹٤)، خیری (۱۳۹۵)، مستقیمی و امین موسوی (۱۳۹۷) و رضایی، مصدق و رضایی (۱۳۹۷) می‌باشد. پیش نیاز اثربخشی امنیت نظام‌های اطلاعاتی، ارزیابی آمادگی و اعتبار سازمانی قبل از اجرا می‌باشد. در صورتی که همسانی بین فرهنگ سازمانی و فرهنگ پیش فرض که در پیاده سازی و بررسی اثربخشی امنیت نظام‌های اطلاعاتی در نظر گرفته شده وجود نداشته باشد، فرهنگ سازمانی می‌تواند به عنوان یک چالش مهم مطرح شود. الگوهای اعتبار تکنیکی در اجرای مسائل امنیتی در نظام‌های اطلاعاتی شامل زمان پاسخ، طراحی سیستم، صفحات نمایش و پینیدگی وظایف پشتیبانی شده می‌باشد. از طرفی اعتبارات سازمانی، ارتباط بین سازمان و امنیت نظام اطلاعاتی را مشخص می‌کند. جنبه‌های خرد اعتبارات سازمانی شامل آشنایی کارکنان با وظایف، انگیزش‌های کارکنان و سبک شناسایی کاربران می‌باشد. همچنین جنبه‌های کلان اعتبارات سازمانی شامل سلسله مراتب سازمان، کانال‌های ارتباطی سازمان، توزیع قدرت در سازمان و فرهنگ سازمانی می‌باشند. در میان عوامل کلان اعتبارات سازمانی، فرهنگ سازمانی بیشترین پیچیدگی را دارد و موانع فرهنگی زیادی در سازمان برای امنیت نظام‌های اطلاعاتی و رسیدن به اهداف مورد نظر در اثربخشی این نظام‌ها وجود دارد.

همچنانکه در جدول (۸) نیز دیده می‌شود در میان زیرمعیارهای فنی، زیرمعیار «برخوردار بودن از زیرساخت مناسب فناوری اطلاعات» با وزن نسبی ۰/۱۹۲۱ بیشترین اهمیت را دارد و زیرمعیار «محاسبه میزان مخاطرات سازمان به ازای هر دارایی با برقراری تناظر بین آسیب‌پذیری‌ها و تهدیدات» با وزن نسبی ۰/۰۶۹۹ در اولویت آخر قرار دارد. نتایج پژوهش همسو با نتایج پژوهش تایی و گریوال (۲۰۰۵)، توریس، ساریگی، سانتوس و سیرانو (۲۰۰۶)، ابوسعد، سعید، الغدبر و خان (۲۰۱۱)، ماروا (۲۰۱۵)، کیلو و انزوکی (۲۰۱۵)، نقی‌لو و احمدی (۱۳۹٤)، خیری (۱۳۹۵) و مستقیمی و امین موسوی (۱۳۹۷) می‌باشد. بکارگیری زیرساخت مناسب و فناوری اطلاعات، تحول گسترده‌ای را در امور اداری و سیستم‌های اطلاعاتی باعث شده است، طوریکه امکان انتقال الکترونیکی داده‌ها، مدارک، اسناد و مکاتبات مختلف از طریق کامپیوتر و خطوط ارتباطات مخابراتی فراهم‌شده است. استفاده از فناوری‌های جدید و زیرساخت مناسب برای رسیدن به سرعت بیشتر با هزینه کمتر یکی از موارد ضروری در اثربخشی امنیت نظام‌های اطلاعاتی است.

فنـــاوری می‌تواند به ارزیابی وضعیت امنیتی نظام‌های ســـازمانی بـــا حداقل هزینه ممکن کمک کند. یکی از مشـــکلات شـــهرداری کلان شهر اهواز عدم اســـتفاده مناسب از فناوری و عدم وجود زیرســـاخت‌های مناسب جهت بهره‌برداری است. لذا این نقص موجب می‌شود که ارزیابی وضعیت امنیت نظام‌ها به درستی انجام نشود و به ایجاد فرصت حملات امنیتی و نفوذ در نظام‌ها بینجامد. فناوری‌های پیشـــرفته و بســـترهای اطلاعاتی قوی فاکتورهای مهمی در شـــناخت بهتر مشکلات امنیتی و حفره‌های موجود در نظام‌ها و ... می‌باشد.

پیشنهاد

با توجه به نتایج پژوهش پیشـــنهاد می‌شود، جلب حمایت مدیران ارشد سازمان از طریق نشان دادن مزایای توجه به امنیت نظام‌های اطلاعاتی صورت پذیرد. انواع ســـبک‌های مدیریت بررســـی و بهترین ســـبک جهت امنیت نظام‌های اطلاعاتی استفاده شود. افراد و مدیران جهت درک دقیق مسئله امنیت اطلاعات آموزش ببینند. راهبردها و سیاست‌های مشترک در حوزه امنیت اطلاعات در کل ســـازمان تدوین شوند. تلاش در جهت همسوسازی اهداف سیاست‌های امنیت اطلاعات با اهداف تجاری سازمان جهت بهره‌گیری بهتر از فرصت‌های حاصل صورت پذیرد. همچنین پیشنهاد می‌شود برای اجرای مناسب مدیریت اطلاعات می‌توان یک کمیته راهبردی تشکیل داد تا به طور مداوم اثربخشی امنیت نظام‌های اطلاعاتی را مورد مطالعه قرار دهد.

فهرست منابع

احمدلو، مهدی؛ احمدلو، مجید (۱۳۹۶)، ارزیابی اثربخشی استقرار سیستم مدیریت امنیت اطلاعات، چهارمین همایش بین‌المللی مدیریت، اقتصاد و توسعه، تهران، مؤسسه علمی کیان پژوهان، ۱-۱۲.

اسماعیلی، محمد حسین (۱۳۹۳)، شناسایی و ارزیابی شاخص‌های تأمین‌کنندگان با استفاده از روش‌های تصمیم‌گیری چندمعیاره خاکستری در شرکت فولاد آلیاژی ایران، پایان‌نامه کارشناسی ارشد رشته مهندسی صنایع، دانشگاه علم و هنر وابسته به جهاد دانشگاهی، دانشکده مهندسی صنایع، ۱-۱۲۷.

باپیری، امید علی؛ کمربیگی، خلیل؛ درویشی، فرزاد (۱۳۹۴)، بررسی میزان احساس امنیت اجتماعی و برخی عوامل مرتبط با آن (مورد مطالعه: دانشجویان دانشگاه‌ها و مراکز آموزش عالی استان ایلام)، فرهنگ ایلام، ۱۶ : ۷۵-۹۰.

تقوا، محمدرضا؛ جعفریان، احمد؛ شفیعی نیک آبادی، محسن (۱۳۹۰)، نقش نظام‌های مدیریت امنیت اطلاعات در بهبود عملکرد زنجیره تأمین، علوم و فناوری اطلاعات، ۱-۲۱.

حاجی زین العابدینی، محسن؛ رفعتی، مینا (۱۳۹۶)، بررسی نظام مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران، پژوهشنامه کتابداری و اطلاع رسانی، ۷ (۱): ۱-۲۳.

خیری, سعید. (۱۳۹۴). شناسایی، تحلیل و رتبه‌بندی عوامل موثر کلیدی در پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان‌های حاکمیتی (مطالعه موردی: سازمان بنادر و دریانوردی. صنعت حمل و نقل دریایی, ۲(۳), ۳۶-۴۶.

خیرگو، منصور؛ شکوهی، جواد (۱۳۹۶)، شناسایی و رتبه بندی عوامل کلیدی موثر بر اثربخشی سیستم‌های اطلاعاتی در سازمان‌های دولتی، فصلنامه پردازش و مدیریت اطلاعات، ۲۳ (۳): ۶۹۵-۷۱۲.

رضایی، علی؛ مصدق، محمد جواد؛ رضایی، مونا (۱۳۹۷)، عوامل مؤثر بر اثربخشی سیستم مدیریت امنیت اطلاعات، مجله مدیریت توسعه و تحول، ۳۳: ۷۳-۸۲.

سلیمانی اصل، محبوبه (۱۳۹۴)، شناسایی چالش‌های امنیت فناوری اطلاعات در حسابرسی دیوان محاسبات کشور، امنیت ملی، ۷ (۵۹): ۱۳۳-۱۵۹.

صالح نیا, علی, بختیاری, حسین. (۱۳۹۷). اولویت‌بندی تهدیدات امنیت ملی جمهوری اسلامی ایران با روش تحلیل سلسله مراتبی(AHP). مطالعات راهبردی سیاستگذاری عمومی, ۸(۲۷), ۲۵۵-۲۷۷.

صفرخانی، مینا؛ شیرمحمدی، مهدی (۱۳۸۸)، ارائه مدلی برای اثربخشی امنیت در سیستم‌های اطلاعاتی، ششـــمین کنفرانس بین‌المللی مدیریت فناوری اطلاعات و ارتباطات، تهران، موسســـه مدیریت فناوری اطلاعات، ۱-۹.

کرمی، مهتاب؛ صفدری، رضا؛ سلطانی، احمد (۱۳۹۲)؛ حقوق اطلاعاتی بیمار: راهکارهایی برای امنیت اطلاعات در محیط الکترونیکی، اخلاق پزشکی، ۷ (۲۵): ۸۳-۹۶.

مســـتقیمی، محمد؛ امین موســـوی، ســـیدعبدالله (۱۳۹۷)، مدلی برای بهبود پذیرش سیستم مدیریت امنیت اطلاعات (ISMS) (مورد مطالعه یکی از سازمان‌های دولتی)، پنجمین کنفرانس ملی پژوهش‌های کاربردی در مدیریت و حسابداری، تهران، انجمن مدیریت ایران، ۱-۱۶.

ملکان، اســـفندیار؛ ســـلمانی، رســـول (۱۳۹۱)، ویروس‌های کامپیوتری تهدیدی برای امنیت سیستم اطلاعات حسابداری، پژوهش حسابداری، ۲ (۳): ۱-۱۱.

نقی‌لو، فرح؛ احمدی، فرید (۱۳۹٤)، شناسایی و اولویت‌بندی عوامل کلیدی موفقیت پیاده‌سازی سیستم‌های مدیریت امنیت اطلاعات در دانشگاه‌های ایران، هفتمین کنفرانس بین‌المللی فناوری اطلاعات و دانش، ارومیه، دانشگاه ارومیه، ۱-۸.

Abbass, W., baina, A., bellafkih, M. (2016), Improvement of Information System Security Risk Management, IEEE International Colloquium on Information Science and Technology (CiSt), 1-6.

AbuSaad, B., Saeed, F.A., Alghathbar, K., Khan, B. (2011), Implementation of ISO 27001in Saudi Arabia–obstacles, motivations, outcomes, and lessons learned, Australian Information Security Management Conference, 1-9.

Alavi, R., Islam, S., Jahankhani, H., Al-Nemrat, A. (2015), Analyzing Human Factors for an Effective Information Security Management System, IGI GLOBAL: Disseminator knowledge, 60: 1253-1278.

Atymtayeva, L., Kozhakhmet, K., Bortsova, G. (2014), Building a Knowledge Base for Expert System in Information Security, Soft Computing in Artificial Intelligence. Advances in Intelligent Systems and Computing, 270 : 57-76.

Barton, K.A., Tejay, G., Lane, M., Terrell, S. (2016), Information system security commitment: A study of external influences on senior management, Computers & Security, 59 : 9-25.

D'Arcy, J.D., Teh, P.L. (2019), Predicting employee information security pol-

icy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization, Information & Management, 1-52.

Khajouei, H., Kazemi, M., Moosavirad, S.H. (2017), Ranking information security controls by using fuzzy analytic hierarchy process, Information Systems and e-Business Management, 15 (1): 1-19.

Kiilu, P.K., Nzuki, D.M. (2015), Factors Affecting Adoption of Information Security Management Systems: A Theoretical Review, International Journal of Science and Research (IJSR), 162-168.

Li, SH ., Yen, DC., Chen, SC., Chen, PS., Lu, W.H., Cho, C.C. (2015), Effects of virtualization on information security, Computer Standards & Interfaces, 42 : 1-8.

Maroa, M.S. (2015), Factors affecting information systems security effectiveSness in university of Nairobi, A research project submitted in partial fulfillment of the requirement for the award of a Master of Science degree in information systems of the University of Nairobi, 1-66.

Ransbotham, S., Mitra, S. (2009), Choice and chance: A conceptual model of paths to information security compromise, Information Systems Research 20, (1): 121-139.

Thai-Van, V., GREWAL, D. (2005), Critical success factors of effective security management: a survey of Vietnamese maritime transport service providers, (IAMU) 6thAnnual General Assembly and Conference, ed. D. Nielsen, World MaritimeUniversity, Sweden, 1-10.

Torres, J.M., Sarriegi, J.M., Santos, J., Serrano, N. (2006), Managing informan tion systems security: critical success factors and indicators to measure effectiveness, Information Security Springer Berlin Heidelberg, 530-545.

Tu, C.Z., Yuan, Y., Archer, N., Connelly, C.E. (2018), Strategic value alignment for information security management: a critical success factor analysis, Information & Computer Security, 26(2): 150-170.

Xu, C., Zhang, J.F, Qi, H. (2017), System Identification under Information Security, IFAC-PapersOnLine, 50 (1): 3756-3761.

Zhang, D. (2018), Big Data Security and Privacy Protection, 8th International Conference on Management and Computer Science, 77: 1-4.