عوامل موثر بر اثربخشی سیستم مدیریت امنیت اطلاعات

علی رضایی[۱] ، محمد جواد مصدق [۲*]، مونا رضایی [۳]
[۱] کارشناس ارشد، شرکت خدمات انفورماتیک ایران، تهران، ایران
[۲]استادیار، گروه مدیریت صنعتی، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران (عهده دار مکاتبات)
[۳] استادیار، گروه تربیت بدنی و علوم ورزشی، واحد ساوه، دانشگاه آزاد اسلامی، ساوه، ایران
تاریخ دریافت: آذر ۱۳۹۶، اصلاحیه: فروردین ۱۳۹۷، پذیرش: خرداد ۱۳۹۷

چکیده

اطلاعات یکی از مهمترین سرمایه‌های یک سازمان است و حفاظت از آن یکی از ارکان مهم بقای سازمان است. سیستم مدیریت امنیت، حفاظت از اطلاعات را در سه مفهوم خاص محرمانه بودن، صحت و در دسترس بودن اطلاعات تعریف می‌کند. هدف اصلی پژوهش شناسایی عوامل انسانی موثر بر اثربخشی سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک است. پژوهش به روش توصیفی ـ همبستگی انجام گرفته و از نظر هدف، کاربردی است. جامعه آماری این پژوهش کلیه بانکهای تحت پوشش شرکت خدمات انفورماتیک ایران می‌باشد. ابزار جمع‌آوری اطلاعات پرسشنامه محقق ساخته است که روایی و پایایی آن موردتأیید قرار گرفته است. تجزیه و تحلیل اطلاعات با استفاده از آمار توصیفی و آمار استنباطی با استفاده از تحلیل رگرسیون انجام شده است. طبق نتایج پژوهش شاخص‌های نقش مدیریت، آگاهی از امنیت سیستم اطلاعات و انطباق با آموزش، امینت سیستم اطلاعات کسب وکار و ارزیابی ریسک امنیت سیستم اطلاعات بر اثربخشی سیستم مدیریت امنیت اطلاعات تاثیرگذار می‌باشند.
کلمات کلیدی: سیستم مدیریت امنیت اطلاعات، اثربخشی سیستم، نقش کلی مدیریت، امنیت سیستم اطلاعات.

۱- مقدمه

حیات سازمان‌ها ارتباط نزدیکی با سیستم‌های اطلاعاتی آنها دارد. سیستم‌های اطلاعاتی نیز همواره در خطر سرقت اطلاعات، تغییر اطلاعات و ایجاد وقفه در خدمات‌رسانی هستند. به منظور حل مسئلهٔ امنیت اطلاعات، سازمان نیازمند به کارگیری طیف گسترده ای از دانش، فناوری و قوانین سازمانی هستند[۲۰ و ۲۸]. بدیهی است که مدیریت مدرن بدون در نظر داشتن شاخصهای موثر بر اثربخشی موفق نبوده و سیستم مدیریت امنیت اطلاعات نیز از این قاعده مستثنی نیست. جستجو در شبکه‌ها برای کسب هوشمندی رقابتی به منظور استفاده از اطلاعات در برابر رقبا رایج‌تر شده است و اغلب به رفتارهای منفی مانند جاسوسی‌های سازمانی و سوءاستفاده اطلاعاتی می‌انجامد[۱۶]. بنابراین هر سازمان برای ادامه حیات و بقای خود نیازمند کسب اطلاعات گوناگون و حفاظت از اطلاعات و اسرار خود می‌باشد و بعضا دستیابی یا نشر اطلاعات سیستم باعث نابودی آن سیستم می‌گردد. در این راستا ایجاد یک سیستم امنیتی قوی می‌تواند برای حفظ امنیت اطلاعات هر سازمان مؤثر باشد، سیستمی که بر اساس نیازهای سازمان و میزان اهمیت اطلاعات در آن طراحی شده و حفاظی جهت تأمین سرمایه‌های اطلاعات سازمان باشد. یکی از زیرساخت‌های لازم برای بهبود امنیت فضای اطلاعات و ارتباطات سیستم مدیریت امنیت اطلاعات می‌باشد. این سیستم در واقع مجموعه‌ای از نیروهای انسانی، مستندات و سیاست‌ها و روش‌های شبکه، مستندات شناسایی و ارزیابی مخاطرات (اعم از سخت‌افزار و نرم‌افزار و...) می‌باشد. نظام مدیریت امنیت اطلاعات در مجموع یک رویکرد نظام‌مند به مدیریت اطلاعات حساس به منظور محافظت از آنهاست. درچنین رویکردی بسیار مهم است که فعالیت‌های گوناگون امنیتی را با راهبردی مشترک به منظور تدارک یک سطح بهینه از حفاظت همراستا کنیم[۱]. سازمان‌هایی که موجودیتشان به طور عمومی به فن‌آوری اطلاعات وابسته است باید از تمامی ابزارهای ممکن برای محافظت از اطلاعات استفاده کنند[۲].

هدف اصلی این پژوهش، شناسایی عوامل تعیین‌کننده اثربخشی سیستم مدیریت امنیت اطلاعات است. مورد مطالعه این پژوهش شرکت خدمات انفورماتیک می‌باشد.

۲-چارچوب نظری

هر سازمان برای ادامه حیات و بقای خود نیازمند کسب اطلاعات گوناگون و حفاظت از اطلاعات و اسرار خود می‌باشد و بعضا دستیابی یا نشر اطلاعات سیستم باعث نابودی آن سیستم می‌گردد. امروزه کشورهای در حال توسعه، تأمین امنیت اطلاعات را به عنوان یک اولویت در نظر می‌گیرند، چرا که خطر فعالیت‌های تبهکارانه بیشتر متوجه آن‌هایی است که از کنترل کافی برخوردار نبوده و ناامن هستند، با توجه به اهمیت

* mjmosadegh@qiau.ac.ir

مسائل مطرح شده در این بخش ازریابی اثرگذاری سیستم مدیریت امنیت اطلاعات یک مسئله بسیار مهم می‌باشد[۳۵]. در سازمان‌های کسب وکار، مدیریت امنیت اطلاعات یک نگرانی اصلی می‌باشد چون نقض داده، سرقت هویت و برای سازمان‌ها مضر می‌باشد[۳۱].

سیستم مدیریت امنیت اطلاعات دارای ویژگی‌های گوناگونی است. برای مثال باید متمرکز بوده و واحد و فرایندهایی مجزا از سایر بخش‌های سازمانی (به ویژه بخش فناوری اطلاعات) داشته باشد؛ البته باید هماهنگی و هم راستایی میان قسمت‌های گوناگون حفظ شود[۸]. همچنین رویکرد صحیح مدیریت امنیت باید تکرارشونده، نظام‌مند، کامل، قابل درک و تجزیه و تحلیل باشد[۲۵]. رویکرد مدیریت امنیت، باید تعادلی میان حفاظت اطلاعات و دسترسی مجاز باشد. نکتهٔ مهم این است که امنیت اطلاعات باید در تمام سطح سازمانی (راهبردی، تاکتیکی و عملیاتی) مدیریت شود و کنترل‌های لازم پیاده‌سازی شوند. بهتر است امنیت اطلاعات به صورت فرایندی مداوم اجرا شود و شناسایی، ارزیابی و پیاده‌سازی را برای همهٔ اجزا دربرگیرد[۳۴]. چارچوب آن باید به‌گونه‌ای باشد که بتوان آسان، کم هزینه و مناسب با نیازهای تجارت الکترونیکی آن را اجرا کرد[۳۹].

برای محافظت از اطلاعات سازمان نمی‌توان به نوع خاصی از امنیت یا به یک محصول خاص اکتفا کرد[۳]. بحث مدیریت امنیت اطلاعات به دلیل پیچیدگی زیاد با مسائل بحث‌انگیز زیادی مواجه می‌شود که این مباحث درراستای فراهم آوردن چارچوب، روش و فناوری‌هایی برای بهبود پیاده‌سازی امنیت اطلاعات در سازمان است[۷]. پیاده‌سازی اثربخش امنیت اطلاعات به رویکردی یکپارچه نیاز دارد (ورمولن و ونسلمز[1] ، ۲۰۰۲). در وضعیت کنونی، امنیت اطلاعات ماهیتی مدیریتی پیداکرده و به آموزش و توجه مدیران سازمان‌ها نیازمند است[۲۴]. نبود حمایت مستمر مدیریت ارشد یکی از موانعی است که کوک و لانگلی در سال ۱۹۹۹ و بلون[2] در سال ۲۰۰۸ به طور مشترک بر آن تأکید کرده اند. همچنین به باور سیپونن و ویلسون (۲۰۰۹) چنانچه دانش و آگاهی کافی دربارهٔ سیستم مدیریت امنیت اطلاعات وجود نداشته باشد، سازمان هنگام پیاده‌سازی این استاندارد با مشکلاتی مواجه خواهد شد. عاملی که به عقیدهٔ بلون نیز از اهمیت بسیار بالایی برخوردار است[۱۰ ، ۲۹ ، ۲۳].

برخی محققان عواملی از جمله آگاهی کم و عدم آموزش کافی کارمندان سازمان، تجهیزات نامناسب فنی، مدیریت ریسک نامناسب، عدم انجام ممیزی دوره‌ای، نداشتن درک صحیح از شروط و مفاد استاندارد، هزینه‌های بالای مالی و زمانی پیاده‌سازی، برخوردار نبودن از دانش کافی دربارهٔ تهدیدهای امنیت اطلاعات، نبود برنامهٔ مناسب مدیریت تداوم کسب وکار، شرح وظایف و مسئولیت‌های نامناسب امنیتی، پشتیبانی نامناسب مدیریت، نظرخواهی نکردن از کارکنان سازمان هنگام اخذ تصمیمات مرتبط با امنیت اطلاعات، نظارت ناکافی بر رفتار کارکنان در حوزهٔ امنیت اطلاعات و تخصیص نادرست مسئولیت را از جمله علل اختلال در روند امنیت اطلاعات بیان کرده‌اند[۸ ، ۱۹ ، ۲۱]. از طرفی، عواملی از جمله پشتیبانی و مشارکت مدیریت عالی سازمان، سیاست‌های مناسب امنیتی، شرح وظایف مناسب امنیتی، انگیزهٔ کارمندان، سازگاری رویهٔ کسب وکار سازمان با رویه های امنیتی و مشاور مجرب خارجی از موارد حیاتی موفقیت امنیت اطلاعات شناسایی شدند[۶ ، ۴].

همچنین اریک[3] (۲۰۱۵) معتقد است فرآیندهای کار مبتنی بر فناوری اطلاعات و ارتباطات به منظور بهبود بهره‌وری و ایمنی در این صنعت در حال توسعه می‌باشد و حفاظت از منابع اطلاعات و فن‌آوری، حصول اطمینان از پردازش امن و مطمئن از اطلاعات، حصول اطمینان از جریان قابل اعتماد و امن از اطلاعات برای تولید و حفاظت در چنین سازمان فناوری اطلاعات و ارتباطات فشرده ضروری است. در فرآیندهای کار مبتنی بر فناوری اطلاعات و ارتباطات چالش‌های جدید مربوط به افزایش نیاز به در دسترس بودن و یکپارچگی اطلاعات، ادغام سیستم‌های ایمنی فرایند و فناوری اطلاعات و ارتباطات سیستم، استفاده از منابع اطلاعاتی کتابچه راهنمای کاربر، جریان اطلاعات بین بازیگران توزیع و حاکی از شرایط جدید مدیریت می‌باشد. تمرکز بیشتر بر روی در دسترس بودن و صداقت به عنوان اصول حفاظت روش‌های مبتنی بر انعطاف‌پذیری به عنوان یک مکمل به روش رسمی مدیریت اعتبارسنجی جریان اطلاعات برای امنیت رخ می‌دهد[۱۷].

در ادامه به معرفی متغیرهای اثرگذار بر اثربخشی سیستم مدیریت امنیت اطلاعات خواهیم پرداخت.

۲-۱-سیستم مدیریت امنیت اطلاعات

بخشی از سیاست‌های مدیریت به سیستم مدیریت امنیت اطلاعات مربوط می‌شود که شامل ابزارها و روش‌هایی برای آگاهی مدیریت در جهت طرح، اتخاذ، پیاده‌سازی، نظارت و بهبود این سیستم می‌باشد. امنیت اطلاعات عبارت است از حفاظت اطلاعات و به حداقل رساندن دسترسی غیر مجاز به آن‌ها، همچنین علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر تغییرات غیر مجاز است. محرمانگی یکی از عوامل مهم و موثر بر حفاظت اطلاعات می‌باشد که عبارتست از حصول اطمینان از دردسترس بودن اطلاعات برای کاربران مجاز. سیستم مدیریت امنیت اطلاعات برای ایمن‌سازی فضای تبادل اطلاعات در یک سازمان استانداردهایی را ارائه می‌دهد. این استانداردها شامل مجموعه‌ای از دستورالعمل‌ها است تا فضای تبادل اطلاعات یک سازمان را با اجرای یک طرح مخصوص به آن سازمان ایمن نماید.

بنابر نتایج تحقیقات پیشین لیستی از متغیرها موثر استخراج شد و با استفاده از روش لاوشه، روایی محتوای متغیرهای تحقیق بررسی شد و متغیرهای تایید شده در ادامه آمده است:

۲-۲-نقش مدیریت

امنیت اطلاعات در درجه اول موضوع مدیریت و کسب وکار است، بنابراین مدیران ارشد باید از اهمیت توسعه سیاست امنیت اطلاعات آگاه باشند و

[1] Vermeulen & Von Solms
[2] Bellone
[3] Erick

باید توجه بیشتری به انجام موثر کنترل‌های امنیتی از پیش تنظیم شده داشته باشند[۱۵]. نقش پاسخگویی سازمان در برابر فشارهای امنیت اطلاعات بسیار مهم است[۳۹]. مدیریت امنیت اطلاعات به دو بخش عمده فنی و مدیریتی تقسیم می‌شود. ادغام این دو جنبه کارآیی امنیت اطلاعات را تضمین خواهد کرد [۱۲ ، ۳۷]. مدیریت باید به جنبه‌های غیر فنی امنیت اطلاعات مانند توسعه سیاست امنیتی، آموزش، سخت‌افزار و نرم‌افزار امنیت، کنترل و تصمیم‌گیری در مورد پردازش داده‌ها بپردازد. بدون پشتیبانی فنی از IT و افراد حرفه‌ای امنیت، برای مدیریت دشوار خواهد بود که امنیت اطلاعات را مدیریت نماید. از سوی دیگر، افراد حرفه‌ای نمی‌توانند منابع اطلاعاتی را بدون حمایت و دخالت مدیریت حفظ نمایند[۳۶]. بنابراین، می‌توان نتیجه گرفت که حفاظت از دارایی‌های اطلاعاتی و امنیت اطلاعات می‌تواند از طریق ادغام فعالیت‌های فنی و مدیریتی تضمین شود[۳۷].

بنابراین فرضیه اول عبارت است از: نقش مدیریت بر اثربخشی سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک تاثیر مثبت دارد.

۲-۳-آموزش و آگاهی از امنیت سیستم اطلاعات

سیاست امنیت اطلاعات نقش مهمی در امنیت داده‌های سازمانی دارد. آگاهی از سیاست امنیت اطلاعات به کارمندان برای حفظ اطلاعات و جلوگیری از حملات مخرب و آسیب‌پذیری‌های دیگر کمک می‌کند، در حالی‌که آموزش آن‌ها را قادر می‌سازد که به‌طور موثر این را انجام دهند. یکی از مهمترین مباحث مربوط به توسعه سیاست‌های امنیتی اطلاعات، آگاهی کارکنان از سیاست و آموزش و پیروی از سیاست امنیت اطلاعات می‌باشد. تدوین سیاست امنیت اطلاعات و اجرای موثر دو کمک‌دهنده اصلی به اثربخشی امنیت اطلاعات می‌باشند[۳۰،۱۴]. سیپونن و همکاران (۲۰۰۹) نشان دادند در عمل باید یک سیاست امنیت اطلاعات روشن وجود داشته باشد، به‌گونه‌ای که آگاهی از آن‌ها تاثیر مثبت بر روی پایبندی کارکنان به سیاست امنیت اطلاعات دارد. آموزش نقش مهمی در توسعه آگاهی و درک دارد.

بنابراین فرضیه دوم عبارت است از: آموزش و آگاهی ازسیاست امنیت اطلاعات بر اثربخشی سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک تاثیر مثبت دارد.

۲-۴-امنیت سیستم اطلاعات کسب وکار

امنیت اطلاعات بیشتر از اینکه یک موضوع فنی باشد باید به عنوان امنیت کسب و کار مورد بررسی قرار گیرد[۲۶]. کاهش ریسک امنیت اطلاعات دارای تاثیر مثبت بر قیمت سهم و موقعیت بازار شرکت‌های کسب وکار می‌باشد، به‌طوری که باید با آن به عنوان یک مسئله کسب و کار برخورد شود[۱۳]. حفاظت از داده‌ها و اطلاعات به عنوان یک مزیت رقابتی، باید بخشی از استراتژی کسب وکار باشد. شکست و یا عدم تمرکز بر امنیت اطلاعات یک عدم موفقیت مدیریت می‌باشد[۹]. ویتمن [1](۲۰۰۴). بنابراین، مدیریت باید یک رویکرد گسترده‌تر را نسبت به امنیت اطلاعات اتخاذ کند، و حاکمیت شرکتی باید در مسائل امنیت اطلاعات دخالت داشته باشند.

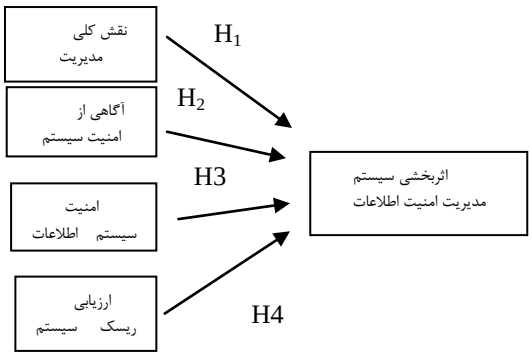
بنابراین فرضیه سوم تحقیق عبارت است از: امینت سیستم اطلاعات کسب وکار بر اثربخشی سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک تاثیر مثبت دارد.

۲-۵- ارزیابی ریسک سیستم امنیت اطلاعات

ارزیابی ریسک امنیت اطلاعات بخش مهمی از اثربخشی ISMS است، که شامل ارزیابی ریسک با استفاده از روش‌های کمی و کیفی و ترکیب ابزارها برای مقابله با این آسیب‌پذیری‌ها می‌باشد[۴۰ و ۳۸]. راه‌حل‌های تکنولوژیکی مختلفی برای امنیت اطلاعات توسعه داده شده است و در حال پیشرفت هستند و در عین حال مسائل امنیت اطلاعات یک چالش بزرگ برای بسیاری از سازمان‌ها می‌باشد (بودین، گوردون، و لوئب، ۲۰۰۸). راه‌حل‌های تکنولوژیکی نیز به سیاست امنیت اطلاعات و استراتژی‌های سازمانی بستگی دارد، پس در جنبه‌های گسترده‌تر، باید از دیدگاه مدیریتی به آن پرداخته شود[۱۸]. اما تمامی راه‌حل‌های تکنولوژیکی دارای ریسک هستند که باید ریسک آنها به منظور افزایش اثربخشی یک ISMS مدنظر باشد[۲۲].

بنابر این فرضیه چهارم عبارت است از: ارزیابی ریسک سیستم امنیت اطلاعات بر مدیریت سیستم امنیت اطلاعات در شرکت خدمات انفورماتیک تاثیر مثبت دارد.

با توجه به فرضیات پژوهش، مدل مفهومی پژوهش به شکل زیر خواهد بود:



شکل (۱): مدل مفهومی پژوهش

۳-روش‌شناسی پژوهش

با توجه به اینکه پژوهش حاضر درصدد شناسایی عوامل موثر بر اثربخشی مدیریت سیستم امنیت اطلاعات است به لحاظ هدف یک پژوهش کاربردی، به لحاظ شیوه گردآوری داده‌ها یک پژوهش توصیفی و با توجه به اینکه به بررسی روابط بین متغیرها می‌پردازد از نوع همبستگی است. برای بررسی پیشینه پژوهش و مبانی تئوریک از روش مطالعات کتابخانه‌ای و منابع اینترنتی استفاده شد.

به منظور گردآوری داده‌ها برای آزمون و ارزیابی فرضیات و مدل از ابزار پرسشنامه استفاده شد. پرسشنامه در این پژوهش پرسشنامه محقق

[1] Vitman

ساخته است که شامل شامل دو بخش است. بخش اول شامل مشخصات فردی پاسخ‌دهنده شامل جنسیت، سن، تحصیلات و سابقه کاری و بخش دوم شامل سوالات مربوط به متغیرها بود که از طیف ۵ گزینه‌ای لیکرت برخوردار بوده و شامل ۲۵ سوال می-باشد. برای طراحی پرسشنامه ابتدا با توجه به متغیرها سوالات اولیهٔ پرسشنامه تهیه شد و پس از بررسی توسط خبرگان و نیز اعمال اصلاحات لازم، پرسشنامهٔ نهایی تدوین شد. جهت سنجش روایی محتوایی ابزار از نظرات خبرگان و شاخص لاوشه به طور همزمان استفاده شد. در بررسی کیفی محتوا، متخصصان بازخورد لازم را در ارتباط با ابزار ارائه میدهند که براساس آن موارد اصلاح شدند. برای بررسی روایی محتوایی به شکل کمی، ازدو ضریب نسبی روایی محتوا و شاخص روایی محتوا استفاده شد. شاخص روایی محتوی بصورت تجمیع امتیازات موافق برای هرآیتم که امتیاز "مرتبط اما نیاز به بازبینی" و "کاملاً مرتبط" را کسب کرده‌اند تقسیم بر تعداد کل متخصصان محاسبه شد. برای تعیین ضریب نسبی روایی محتوی از متخصصان درخواست شد تا هرآیتم را براساس طیف سه قسمتی «ضروری است»، «مفید است ولی ضرورتی ندارد» و «ضرورتی ندارد» بررسی نماید. با توجه به اینکه پانل خبرگان ۵ نفر بودند حداقل مقدار روایی برای ۵ نفر برابر ۰/۹۹ است. نتایج روایی محتوا در جدول (۱) آمده است. به منظور تعیین تعداد نمونه آماری مناسب در این پژوهش از فرمول کوکران در جوامع نامحدود استفاده گردید. بر این اساس با در نظر گرفتن سطح خطای نمونه‌گیری ۱۰ درصد اندازه نمونه آماری این پژوهش از طریق فرمول زیر ۹۶ نفر درنظر گرفته شده است.

$$n = \frac{Z^2_{1-a/2}\ pq}{d^2}$$

در فرمول فوق با در نظر گرفتن ضریب اطمینان ۰/۹۵، مقدار $Z^2_{1-a/2}$ برابر ۱/۹۶ تعیین می‌شود. همچنین در صورتی‌که مقدار احتمال p=1-q را برابر بیشترین مقدار خود یعنی ۰/۵ در نظر بگیریم، با در نظر گرفتن خطای ۱۰ درصد مقدار حجم نمونه برابر با ۹۶ خواهد بود.

مقدار آلفا برابر با ۰/۸۷ به دست آمد که رقم پایایی بالای پرسشنامه را نشان می‌دهد. همچنین (۲) مقادیر آلفای کرونباخ را به تفکیک متغیرهای پژوهش نشان می‌دهد.

جدول (۱): نتایج CVR و CVI

متغیر	سوالات	CVR	CVI	بازه CVR	بازه CVI	نتیجه روایی
نقش کلی مدیریت	یک شرکت باید یک ساختار مدیریت جامع و شیوه‌هایی برای امنیت اطلاعات داشته باشد	۰/۷	۰/۸	>۰/۶۲	>۰/۷۹	تایید
آگاهی امنیت سیستم اطلاعات و انطباق با آموزش	حمایت مدیریت ارشد مهم‌ترین موضوع یک برنامه امنیت اطلاعات است	۰/۷۳	۰/۸	>۰/۶۲	>۰/۷۹	تایید
	علاقه مدیریت ارشد و مشارکت برای بهبود مداوم در سیستم‌های امنیت اطلاعات حیاتی است	۰/۷	۰/۸	>۰/۶۲	>۰/۷۹	تایید
	از نقش‌های ضروری مدیریت امنیت اطلاعات می باشد	۰/۴۶	۰/۲	>۰/۶۲	>۰/۷۹	مردود
	مدیریت باید به همترازی فناوری کسب وکار و مسائل امنیتی بپردازد	۰/۷۴	۰/۸	>۰/۶۲	>۰/۷۹	تایید
	مدیریت باید زیر ساخت اطلاعات را توسعه دهد	۰/۴۶	۰/۲	>۰/۶۲	>۰/۷۹	مردود
	پیروی از سیاست امنیت اطلاعات یک رویکرد برای پذیرش رفتار مثبت کارکنان است	۰/۴۶	۰/۶	>۰/۶۲	>۰/۷۹	مردود
	آموزش امنیت اطلاعات احتمالا مهم‌ترین اقدام برای اثربخشی آن می باشد، چون آن آگاهی و درک را افزایش می‌دهد	۰/۷۳	۰/۸	>۰/۶۲	>۰/۷۹	تایید
	مشارکت کارکنان و خلق دانش تغییرات مثبت نسبت به آگاهی و رفتار امنیت اطلاعات ایجاد می‌کند	۰/۷۳	۰/۸	>۰/۶۲	>۰/۷۹	تایید
	یک تهدید داخلی عمده برای امنیت اطلاعات نقض سیاست‌های دسترسی با نیت بدخواهانه می‌باشد	۰/۷	۰/۸	>۰/۶۲	>۰/۷۹	تایید
	انطباق کارکنان با سیاست امنیت اطلاعات یکی از ابعاد آگاهی امنیت	۰/۴۶	۰/۶	>۰/۶۲	>۰/۷۹	مردود

	اطلاعات می‌باشد					
امنیت سیستم اطلاعات کسب و کار	حاکمیت امنیت اطلاعات یک مسئولیت در سطح هیئت مدیره است، همانطور که اثر کاهش دهنده خطر بر قیمت سهم و موقعیت بازار دارد	۰/۷	۰/۸	>۰/۶۲	>۰/۷۹	تایید
	باید به امنیت اطلاعات توسط مدیریت ارشد به عنوان یک مسئله امنیت کسب وکار پرداخته شود	۰/۷۳	۰/۸	>۰/۶۲	>۰/۷۹	تایید
	مسائل امنیت سایبری باید در اتاق هیئت مدیره و جلسات اجرایی در محل اتاق سرور بحث شود	۰/٤٦	۰/٦	>۰/۶۲	>۰/۷۹	مردود
	مدیریت ارشد و عوامل اجرایی امنیت اطلاعات باید با امنیت اطلاعات به عنوان یک مسئله کسب وکار به جای یک مسئله فنی برخورد نمایند.	۰/۷	۰/۸	>۰/۶۲	>۰/۷۹	تایید
ارزیابی ریسک امنیت سیستم اطلاعات	مدیریت باید به توسعه استراتژی ها برای مقابله با آسیب‌پذیری، از طریق ابزارهای فنی و اجتماعی بپردازد	۰/٦	۰/٦	>۰/۶۲	>۰/۷۹	مردود
	تصمیم‌گیری‌های دیریت در مورد کنترل دسترسی، سیاست امنیت، امنیت سخت‌افزار، تامین مالی، آگاهی امنیتی، آموزش و مدیریت منابع انسانی تاثیر مهم بر اثربخشی اقدامات دارد	۰/٦	۰/٦	>۰/۶۲	>۰/۷۹	مردود
	مدیریت امنیت وظیفه پیاده‌سازی و کنترل عملکرد سیستم امنیت سازمان را بر عهده دارد	۰/۷۳	۰/۸	>۰/۶۲	>۰/۷۹	تایید
	مدیریت امنیت باید سیستم را همیشه به روزنگه دارد	۰/۷	۰/۸	>۰/۶۲	>۰/۷۹	تایید
	هدف امنیت اطلاعات در یک سازمان حفظ سرمایه های (نرم‌افزاری ، سخت‌افزاری،اطلاعاتی و ارتباطی و نیروی انسانی) در مقابل هرگونه تهدید اعم از دسترسی غیر مجاز به اطلاعات ، خطر ناشی از محیط و خطرات ایجاد شده از سوی کاربران است	۰/۷۳	۰/۸	>۰/۶۲	>۰/۷۹	تایید
اثربخشی سیستم مدیریت امنیت اطلاعات	مدیریت امنیت در ارزیابی برنامه‌های کلی سیستم دخالت دارد	۰/۷۸	۰/۸	>۰/٦٦	>۰/۷۹	تایید
	مدیریت امنیت در ارزیابی عملکرد واحد کاری نقش مهمی دارد	۰/۸	۰/۸	>۰/٦٥	>۰/۸	تایید
	مدیریت در انجام کارهای تیمی از هماهنگی و انسجام برخوردار است	۰/۷٥	۰/۸٤	>۰/۷	>۰/۷۹	تایید
	مدیریت قادر به جذب نیروی انسانی کارآمد است	۰/٤۳	۰/۲	>۰/٦٥	>۰/۷٥	مردود
	مدیریت بر بهبود کیفیت و اثربخشی سیستم توجه دارد	۰/۸	۰/۸	>۰/٦۹	>۰/۷۹	تایید

جدول (۲): مقادیر آلفای کرونباخ متغیرهای تحقیق

متغیر	مقدار آلفای کرونباخ
نقش کلی مدیریت	۰/۸۷
آگاهی امنیت سیستم اطلاعات و انطباق با آموزش	۰/۷۱
امنیت سیستم اطلاعات کسب و کار	۰/۸
ارزیابی ریسک امنیت سیستم اطلاعات	۰/۷٤
ارزیابی اثر بخشی سیستم مدیریت امنیت اطلاعات	۰/۸۷

برای بررسی نرمال بودن یا نبودن توزیع داده‌ها از آزمون کلموگراف-اسمیرنوف استفاده شد که نتایج نشان می‌دهند که داده‌ها دارای توزیع نرمال نیز هستند. در نتیجه برای بررسی رابطه ی بین متغیرها از ضریب

همبستگی پیرسون استفاده شد.(جدول ۴)

٤-یافته‌های پژوهش

به منظور ارزیابی اثربخشی سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک پس از تعیین معیارهای اصلی، تجزیه و تحلیل اطلاعات انجام شد. ابتدا جدول (۳)، به نمایش یافته‌های جمعیت شناختی می‌پردازد و سپس در ادامه یافته‌های استنباطی ارائه می‌شوند.

جدول (۳): توصیف یافته‌های جمعیت‌شناختی آزمودنیهای تحقیق

متغیر		فراوانی	درصد فراوانی
سن	۳۰-۲٦	۲	۲
	۳۵-۳۱	٤۰	۳۸
	٤۰-۳٦	٤٤	٤۲
	٤۱سال به بالا	۱٤	۱٤
سطح تحصیلات	دیپلم و پایین‌تر	۱	۱
	فوق دیپلم	٤	٤
	لیسانس	۵۷	۵۹
	فوق لیسانس و بالاتر	۳٤	۳٦
سابقه کاری	۱۰سال و کمتر	۲۳	۱
	۲۰_۱۱	۳۹	٤
	۳۰_۲۱	۲۵	۵۹
	۳۱سال به بالا	۹	۳٦
جنسیت	زن	۲۰	۲۱
	مرد	۷٦	۷۹

جدول (٤):نتایج آزمون کولموگروف اسمیرنف

متغیر	تعداد	میانگین	انحراف معیار	کولموگروف اسمیرنف	سطح معنی داری	نرمال یا غیر نرمال
نقش کلی مدیریت	۹٦	۳/٤۱	۰/۰۱	۱/۱۵۱	۰/۱٤۲	نرمال
آگاهی امنیت سیستم اطلاعات و انطباق با آموزش	۹٦	۳/۵۵	۰/۹۰۱	۱/۱۷۸	۰/۱۲۵	نرمال
امنیت سیستم اطلاعات کسب و کار	۹٦	۳/۵۲	۰/۸۷	۱/۰۱٤	۰/۲۵۲	نرمال
ارزیابی ریسک امنیت سیستم اطلاعات	۱	٤ ۸ / ۳	۸ ۱ / ۰	۱۱ /۳ ۱	۱٦ /۸ ۰	نرمال

با توجه به نتایج بدست آمده از جدول (۴) از آنجایی که سطح معناداری متغیرها بزرگتر از ۰/۰۵ می‌باشد فرض نرمال بودن این داده‌ها تأیید می‌گردد و داده‌ها نرمال می‌باشند. در ادامه جداول ۵ الی ۸ به بررسی فرضیه‌های پژوهش می‌پردازد.

جدول (۵):نتایج آزمون همبستگی پیرسون برای فرضیه اول

		مدیریت سیستم امنیت اطلاعات
نقش کلی مدیریت	ضریب پیرسون	۰/۷۰۸
	سطح معنی‌داری	۰/۰۰۰
	تعداد	۹۶

با توجه به نتایج جدول ۵ مقدار p آزمون بیشتر از سطح معناداری ۰/۰۰۰ می باشد و فرض صفر رد نمی‌گردد؛ بنابراین اطلاعات نقش کلی مدیریت بر سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک تاثیرگذار است.

جدول (۶) به گزارش نتایج فرضیه دوم می‌پردازد.

جدول (٦): نتایج آزمون همبستگی پیرسون فرضیه دوم

		مدیریت سیستم امنیت اطلاعات
امنیت سیستم اطلاعات کسب وکار	ضریب پیرسون	۰/۷۳٦
	سطح معنی‌داری	۰/۰۰۰
	تعداد	۹٦

با توجه به نتایج جدول (۶) مقدار p آزمون بیشتر از سطح معناداری ۰/۰۵ می‌باشد فرض صفر رد نمی‌گردد؛ و امینت سیستم اطلاعات کسب وکار بر سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک تاثیرگذار است.

نتایج حاصل از فرضیه چهارم تحقیق در جدول (۷) گزارش شده است.

جدول (۷): نتایج آزمون همبستگی پیرسون فرضیه چهارم

		مدیریت سیستم امنیت اطلاعات
ریسک امنیت سیستم اطلاعات	ضریب پیرسون	۰/۷۵۳
	سطح معنی داری	۰/۰۰۰
	تعداد	۹٦

با توجه به نتایج جدول ۷مقدار p آزمون بیشتر از سطح معناداری ۰/۰۵ می‌باشد فرض صفر رد نمی‌گردد؛ و ارزیابی ریسک امنیت سیستم اطلاعات بر سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک تاثیرگذار است.

جدول (۸) به جمع‌بندی نتایج فرضیات تحقیق می‌پردازد.

جدول (۸): نتایج فرضیات تحقیق

فرضیه تحقیق	نتیجه
سیاست امنیت سیستم اطلاعات بر مدیریت سیستم امنیت اطلاعات در شرکت شرکت خدمات انفورماتیک تاثیرگذار است.	تأیید
امینت سیستم اطلاعات کسب وکار بر سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک تاثیرگذار است.	تأیید
شاخص آگاهی امنیت سیستم اطلاعات و انطباق با آموزش بر سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک تاثیرگذار است.	تأیید
نقش کلی مدیریت برای سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک ضروری است.	تأیید

آزمون رگرسیون

در تحقیق برای بررسی تأثیرگذاری از رگرسیون استفاده می‌شود. در این حالت مقادیر یک متغیر (متغیر وابسته y) از روی مقادیر دو یا چند متغیر دیگر متغیرهای مستقل $x_1,x_2,...,x_p$ برآورد می‌شود. این کار از طریق ساختن یک معادله خطی به شکل عمومی زیر انجام می‌شود:

$$y=b_0+b_1(x_1)+b_2(x_2)+...+b_p(x_p)$$

در این معادله پارامترهای $b_1,b_2,...,b_p$ ضرایب رگرسیون جزئی هستند و b_0 مقدار ثابت رگرسیون است.

در معادله رگرسیون چندگانه، ضرایب مستقل به عنوان ضرایب رگرسیون جزئی شناخته می‌شوند که معنی آن این است که این ضرایب میزان افزایش متغیر وابسته را به ازای یک واحد افزایش متغیر مستقل مورد نظر نشان می‌دهد.

شرایط حاکم بر رگرسیون خطی چندگانه عبارتند از:

- هر متغیر به صورت جداگانه توزیع نرمال دارد.
- متغیرها در جامعه، به صورت چندمتغیره توزیع نرمال دارند.
- نمودار پراکندگی برای تک تک متغیرهای مستقل با متغیر وابسته جهت بررسی رابطه خطی رسم گردد.

جدول (۹): ضرایب معادله رگرسیون برای مولفه‌های موثر بر امنیت اطلاعات و مدیریت سیستم امنیت اطلاعات

مدل	ضرایب استاندارد نشده		ضرایب استاندارد شده	آماره t	سطح معنی-داری
	B	خطای استاندارد	بتا		
(ثابت)	۰/۰۵۷	۰/۳۲۱		۰/۱۷۸	۰/۰۰۱
نقش کلی مدیریت	۰/۰۳۵	۰/۰۸۷	۰/۰۵	۰/٤۰۸	۰/۰۲۱
آگاهی سیستم امنیت اطلاعات و انطباق با آموزش	۰/۳۵۸	۰/۱۲٤	۰/۳۱۲	۲/۸۷۹	۰/۰۰۵
امنیت سیستم اطلاعات کسب وکار	۰/۳۵٦	۰/۱۲۲	۰/۳۸۸	۲/۹۱۵	۰/۰۰٤
ارزیابی ریسک امنیت سیستم اطلاعات	۰/۱۹۷	۰/۱۲۵	۰/۲۱۷	۱/۵۷۱	۰/۰۰۲

در خروجی جدول شماره (۹) و در ستون B به ترتیب مقدار ثابت و ضریب متغیر مستقل در معامله رگرسیون ارائه شده است و این معادله به صورت زیر می‌باشد :

$$y=0.05x_1+ 0.312x_2+0.388x_3+0.217x_4$$

طبق خروجی جدول شماره (۹)، بقیه ستون های این نگاره شامل معیار ضرایب ستون B، آماره t و sig است که جهت آزمون فرض تساوی هر یک از ضرایب ستون B با عدد صفر به کار می‌رود. حال اگر β و α به ترتیب مقدار ثابت و شیب خط رگرسیون جامعه باشد، آزمون فرض‌ها را برای این دو مقدار می‌توان به صورت زیر نوشت :

$$\begin{cases} H_0 : \alpha = 0 \\ H_1 : \alpha \neq 0 \end{cases}$$

$$\begin{cases} H_0 : \beta = 0 \\ H_1 : \beta \neq 0 \end{cases}$$

از آن‌جایی‌که در این خروجی از آن‌جایی‌که سطح معناداری کلیه متغیرها کوچکتر از ۰/۰۵می‌باشد می‌توان اینگونه نتیجه گرفت که ضریب این متغیر در برازش مدل رگرسیون قابل قبول می‌باشد بنابراین نباید از آن‌ها را از معادله رگرسیون حذف کرد .

۵- نتیجه گیری

هدف از پژوهش حاضر شناسایی عوامل تعیین‌کننده اثربخشی سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک بود. طبق نتایج حاصل از تحقیق؛ ۲۰ درصد افراد زن و ۷۹ درصد مرد؛ ۲درصد از پاسخ‌دهندگان بین ۲۶ تا ۳۰ سال، ۴۰درصد بین ۳۱ تا ۳۵ سال، ۴۴ درصد بین ۳۶ تا ۴۰ سال و ۱۴ درصد بالای ۴۱ سال؛ ۱درصد پاسخ‌دهندگان دارای مدرک دیپلم و پایین‌تر ، ۴درصد فوق دیپلم، ۵۹ درصد پاسخ‌دهندگان لیسانس، ۳۶ درصد فوق لیسانس و بالاتر ؛ ۲۴ درصد کمتر از ۱۰ سال ،۴۱ درصد بین ۱۱ تا ۲۰ سال، ۲۶درصد بین ۲۱ تا ۳۰ سال و ۹ درصد بیشتر از ۳۱ سال سابقه کاری بودند.

با توجه به نتایج بدست آمده از آزمون کلیه فرضیه ها با اطمینان بالایی پذیرفته شدند.

- نقش کلی مدیریت بر اثربخشی سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک تأثیرگذار است.

عوامل سازمانی، مانند توسعه سیاست امنیتی، آگاهی، انطباق و اجرای بهترین شیوه‌ها، اندازه‌گیری‌های اولیه برای امنیت اطلاعات می‌باشد. تمام این فعالیت‌ها، مسئولیت مدیریت یک شرکت هستند. شیوه‌های مدیریتی مرتبط با فن‌آوری اطلاعات محرک اثربخشی فناوری اطلاعات می‌باشند[۱۶]. پس نه تنها کنترل شیوه‌ها، بلکه همه شیوه‌های بهتر مدیریتی مربوط به امنیت اطلاعات آن را موثرتر و همتراز با اهداف کسب وکار می‌کند. بنابراین، مدیران امنیت اطلاعات باید یک رویکرد جامع‌تر برای شیوه‌های مدیریتی بهتر جهت مدیریت موثر امنیت اطلاعات اتخاذ نمایند. نتایج تحقیق حاضر با یافته‌های چابینسکی (۲۰۱۵)، کالکینز و همکاران (۲۰۱۴) و بوراس و همکاران (۲۰۱۴) همسو می‌باشد.

- شاخص آگاهی امنیت سیستم اطلاعات و انطباق با آموزش بر اثربخشی سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک تاثیرگذار است.

آموزش نه تنها آگاهی درباره امنیت اطلاعات را ایجاد می‌کند بلکه همچنین می‌تواند رفتار کارکنان برای جلوگیری از نقض سیاست دسترسی برانگیزد. نقض سیاست‌های دسترسی با قصد بدخواهانه، تهدید عمده داخلی برای امنیت اطلاعات است[۳۲]، چرا که کارمندان می‌توانند به حساس‌ترین اطلاعات دسترسی داشته باشند. نتایج تحقیق با یافته‌های [۱۰، ۵] همراستاست. آنها اعتقاد داشتند آموزش‌های انطباق اثرات متعدد و قابل توجه بر امنیت اطلاعات در هر سازمان دارد.

- امینت سیستم اطلاعات کسب وکار بر اثربخشی سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک تاثیرگذار است.

کاهش ریسک امنیت اطلاعات دارای تاثیر مثبت بر قیمت سهم و موقعیت بازار شرکت‌های کسب وکار می‌باشد. امنیت اطلاعات، اگر در جلسات با سطح بالاتر مورد بحث قرار گیرد، با برنامه‌ریزی و سیاست‌های کلی کسب وکار هم راستا می‌شود، و اثربخشی آن را تضمین می‌کند[۳۵]. نتایج تحقیقات علاالدینی، ۲۰۱۴ نیز سودمندی بررسی امنیت اطلاعات در یک چارچوب گسترده تر و به عنوان یک مسئله امنیت کسب وکار پیشنهاد می‌کند.

- ارزیابی ریسک امنیت سیستم اطلاعات بر اثربخشی سیستم مدیریت امنیت اطلاعات در شرکت خدمات انفورماتیک تاثیرگذار است.

مدیریت برای توسعه و یا اتخاذ هر دو روش یا یک روش ترکیب شده و تعدیل کردن از نظر زیرساخت‌های اطلاعات مسئولیت بیشتری دارد. مدیریت همچنین باید به توسعه استراتژی‌ها برای مقابله با آسیب‌پذیری در سیستم، از طریق ابزارهای فنی و اجتماعی بپردازد. طبق نتایج[۲۷ ، ۳۳] در نظر گرفتن پیچیدگی‌های کسب وکار باید در زمان ارزیابی ریسک امنیت اطلاعات استفاده شوند. امنیت اطلاعات باید به عنوان امنیت کسب و کار بجای یک موضوع فنی مورد بررسی قرار گیرد[۱۱]. همچنین طبق نتایج نظری (۲۰۱۵)، حفاظت از داده‌ها و اطلاعات از تهدیدات بالقوه باید بخشی از استراتژی کسب وکار باشد.

بدیهی است که رفع محدودیت‌ها و موانع پیش روی هر پژوهش میدانی، زیربنای پژوهش‌های بعدی قرار می‌گیرد. تحقیق حاضر نیز با محدودیت‌هایی مواجه بوده است. یکی از محدودیت‌های این پژوهش عدم دسته‌بندی متغیرهای موثر بر اثربخشی سیستم مدیریت امنیت اطلاعات می‌باشد، لذا پیشنهاد می‌شود با توجه به شناسایی نوع متغیرها، دسته‌بندی متناسب با آنها انجام پذیرد. با توجه به اینکه تعدادی از متغیرهای ابتدایی بعد از بررسی روایی محتوای با استفاده از ضریب لاوشه تایید نشدند، پیشنهاد می‌شود این متغیرها که شامل متغیرهای امنیت اطلاعات، میزان پایداری سیستم، تعداد دفعات داده‌های از دست رفته، سیاست امنیت اطلاعات و همچنین دیگر متغیر ها نیز برای تحقیقات آتی مورد بررسی قرار گیرند.

منابع وماخذ

[۱] پورمند، علی، (۱۳۸۷)، **استانداردی برای مدیریت امنیت اطلاعات**، تدبیر، شماره ۱۷، صفحات ۱۷۸-۱۸۳.

[۲] تاج فر، احمد؛ محمودی میمند، محمد؛ رضاسلطانی، فرامرز؛ رضا سلطانی، پدرام،(۱۳۹۳)، **رتبه‌بندی موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات و بررسی میزان آمادگی مدیریت اکتشاف**، مدیریت فناوری اطلاعات، شماره ٦ ، جلد ٤، صفحات ٥٥١-٥٦٦.

[۳] میوالد، آدرین، (۱۳۸۳)، **(امنیت شبکه کامپیوتر)**، احمد صفایی، نشر دانش پرور. تهران، چاپ اول.

[4] Abd Rahman, S., Haslinda, A., (2014), **Relationship between Organizational Characteristics and Information Security Knowledge Management Implementation**, Procedia - Social and Behavioral Sciences, 123, 433-443.

[5] Alaedini, M., Salekfard, S., (2014**), Investigating the role of an enterprise architecture project in the business-IT alignment**, Information systems frantiers, 15(1), 67-88.

[6] Al-Awadi, M., Renaud, K., (2007), **Success factors in information security implementation in organizations**, Paper presented at the IADIS International Conference e-Society . Available in: http://www.dcs.gla.ac.uk /~karen/ Papers/sucessFactors2.pdf.

[7] Alfawaz, S., (2011), **Information security management: a case study of an information security culture**, Phd thesis, Queensland University of technology, faculty of science and technology.

[8] Atif, A., (2015**), A case analysis of information systems and security incident responses**, International Journal of Information Management, 35, 717-723.

[9] Atkins, B., (2014), **Board focus on cyber security**, corporate government, 43(3), 308-321.

[10] Bellone, J., (2008), **A practiced approach to information security management system implementation**, Information Management & Computer Security, 16 (1): 49-57.

[11] Blasch, E., Al-Nashif, Y, Hariri, S., (2014), **Design and Implementation An integrated management system for protect and transmission of secure information**.

[12] Bouras, C., Kokkinos, V., Tseliou, G., (2014), **Methodology for public administrators for selecting between open source and proprietary software**, Telematics and informatics, 30(2), 100-110.

[13] Caulkins, J., (2014), **When to make proprietary software open source**, Journal of economic dynamics and control. 37(6), 1182-1194.

[14] Chabinsky, S., (2015), **The business nessecity of cybersecurity: it is not an IT issue**, Security, solutions for enterprise security leaders, 51(3), 56.

[15] Chang, S. E., Ho, C. B., (2006**), Organizational factors to the effectiveness of implementing information security management**, Industrial Management & Data Systems, 106(3), 345–361.

[16] Choi, N., Kim, D., Goo, J., (2008), **Knowing is doing an empirical validation of the relationship between managerial information security awareness and action**, Information Management & Computer Security, 16 (5): 484-485.

[17] Erick, A., (2015), **Major accident prevention and management of information systems security in technology-based work processes**, Journal of Loss Prevention in the Process Industries, 36, 84-91.

[18] Ernest-Jones, T., (2006), **Pinning down a security policy for mobile data, Network Security**, 2006 (6): 8-13.

[19] Fomin, V., DeVries, H., Barlette, Y., (2008**), ISO/IEC 27001 Information systems security management standards: Exploring the reasons for low adoption**. RSM Erasmus University, Netherland.

[20] Honan, B., (2006), **IT security-commoditized, badly Info security today**, and 3 (5): 41.

[21] Kakkar, A., Punhani, R., Madan, S., (2012**), Implementation of ISMS and its Practical Shortcomings**, International Refereed Research Journal ISSN 1839-6518, Vol. 02, No. 01, www.irj.iars.info.

[22] Kazemi, M., Khajouei, H., Nasrabadi, H., (2012), **Evaluation of information security management system success factors: Case study of Municipal organization**, African Journal of Business Management, 6(14): 4982-4989.

[23] Khorasani Rad, A., Hossein Abadi, H., Amirzadeh, R., (1996), **Standard ISO / IEC 27001**, Partner Company Tuff Iran (Member of TUV Nord), Tehran.

[24] Knapp, K. J., Marshall, T. E., Rainer, R. K., Morrow, D. W., (2004), **Top Ranked Information Security Issues: The 2004 International Information Systems Security Certification Consortium (ISC) Survey Results**, Auburn University, Auburn, AL.

[25] Kotonya, G., Sommerville, I., (1998), **Requirements Engineering Process and Techniques**, Hardcover, ISBN: 978-0-471-97208-2,http://eu.wiley.com/ WileyCDA/WileyTitle/productCd-0471972088.html#instructor.

[26] Kwok, L., Longley, D., (1999), **Information security management and modeling**, Information Management & Computer Security, 7 (1): 30-40.

[27] Li, S. H., Yen, D. C., Chen, S. C., Chen, P. S., Lu, W. H., Cho, C.C., (2015), **Effects of virtualization on information security**, Computer Standards & Interfaces, 42, 1-8.

[28] Mohseni, M., (2013), **Has your organization compliance with ISMS? A case study in an Iranian Bank**, ArXiv preprint arXiv: 1303.0468. ftp/arxiv/papers/1303/1303.0468.pdf.

[29] Nazareth, D., Choi, J., (2015), **A system dynamics model for information security management, information and management**, 52, 123-134.

[30] Phillips, B., (2013), **Information technology management practice**, Journal of organizational & end user computing. 25(4), 50-75.

[31] Ring, T., (2013), **A breach too far? Computer Fraud & Security**, 6:5-9.

[32] Ryan, J., (2012), **A comparison of information security trends between formal and informal environments**.,A Dissertation for the Degree of Doctor of Philosophy the Graduate, Faculty of Auburn University Alabama.

[33] Singh, A. N., (2013), **ISM practices**, Global journal of flexible systems management, 14(4), 225-239.

[34] Siponen, M., Willison, R., (2009), **Information security management standards: Problems and solutions**, Information & Management, 46 (5): 267-270.
[35] Soomro, Z., Shah, M., Ahmed, J., (2016), **Information security management needs more holisticapproach: A literature review**, International journal of management, 36: 215-225.
[36] Vermeulen, C., Von Solms, R., (2002), **The information security management toolbox taking the pain out of security management**, Information management & computer security, 10 (3): 119-125.
[37] Young, R., Windsor, J., (2014), **Empirical evaluation of information security planning and integration**, Communications of the association for information systems, 26(1), 245-266.
[38] Zang, W.I., (2014), **Research of information security quantitative evaluation method**, applied mechanics, 513, 369-372.
[39] Zuccato, A., (2007), **Holistic security management framework applied in electronic commerce**, Computer and Security, 26 (3): 256-265.
[40] Houa, Y., Gaob, P., Nicholsonc, B., (2018), **Holistic security management framework applied in electronic commerce**, Computer Technological Forecasting and Social Change and Security, 126 (1): 64-75.
[41] Wei, Y., Wu, W-Ch., Chu, Ya-Chi., (2018**), Performance evaluation of the recommendation mechanism of information security risk identification Neurocomputing**, 279(1):48-53.