پژوهش حسابداری
شماره ۱۰، پاییز ۱۳۹۲

امنیت و تهدیدات امنیتی در سیستم‌های اطلاعاتی حسابداری

سید علی واعظ
استاد یار گروه حسابداری دانشگاه شهید چمران اهواز
وریا احمدی[۱]
دانشجوی کارشناسی ارشد حسابداری دانشگاه شهید چمران اهواز

تاریخ دریافت : ۹۲/۰۶/۰۴
تاریخ پذیرش : ۹۲/ ۰۹/۱۵

چکیده

هدف این تحقیق که با بررسی تحقیق‌های پیشین به دست آمده است، بررسی امنیت در سیستم‌های اطلاعاتی حسابداری و تهدیدات مربوط به آن است. نتایج تحقیق نشان می‌دهد، تغییرات سریع در فناوری اطلاعات و بکارگیری سیستم‌ها و نرم افزارهای جدید سبب شده تا رایانه‌ها خیلی سریع‌تر و آسان‌تر از گذشته مورد استفاده قرار گیرند. از طرف دیگر این فناوری پیشرفته خطرات تازه و البته مهمی را در مورد نحوه‌ی تأمین امنیت و اطمینان از صحت اطلاعات حاصل از سیستم‌های اطلاعاتی حسابداری ایجاد کرده است. بنابراین لازم است که مدیران و حسابداران و حسابرسان با عوامل تهدید کننده سیستم‌های اطلاعاتی حسابداری آشنا باشند که توانایی اقدام به موقع جهت کاهش یا از بین بردن آثار این تهدیدات را داشته باشند.

واژه‌های کلیدی: سیستم‌های اطلاعاتی حسابداری، امنیت، تهدیدات امنیتی، فناوری اطلاعات.
طبقه‌بندی موضوعی: M49

۱ نویسنده مسئول: ahmadi. voria@yahoo. com

۱- مقدمه

امروزه یکی از شاخه‌های تخصصی حسابداری طراحی سیستم‌های اطلاعاتی حسابداری است و از طرفی مدیریت جهت تصمیم گیری راهبردی نیازمند اطلاعاتی است که عموما به وسیله‌ی سیستم‌های اطلاعاتی حسابداری فراهم می‌شود (پورحیدری، ۱۳۸۵). بنابر این در شرکت‌ها و سازمان‌هایی که امنیت سیستم‌های اطلاعاتی ضعیف است خطر نفوذ به سیستم و دست‌کاری اطلاعات بالا بوده و خسارت‌های وارده می‌تواند غیر قابل جبران باشد. نیاز به ایمنی اطلاعات ایجاب می‌کند که پیش‌بینی‌های لازم توسط مدیریت صورت گیردتا اطلاعات سیستم از ایمنی مناسبی برخوردار و اطلاعات آن قابل اتکاء باشد. با توجه به اهمیت روز افزون امنیت در سیستم-های اطلاعاتی به هنگام پردازش اطلاعات مالی، موضوع امنیت در سیستم‌های اطلاعاتی حسابداری و ایجاد آن در سازمان‌ها و شرکت‌ها جایگاه ویژه‌ای را در بین مدیران حسابداری و حسابرسان به وجود آورده است (ودیعی، ۱۳۸۹).

دیویس (۱۹۹۷) معتقد است که امروزه تغییرات فناوری اطلاعات در دامنه‌ی بزرگتری نسبت به گذشته صورت می‌گیرد و بسیاری از این تغییرات مطابق با سیستم‌های اطلاعاتی حسابداری سازمان‌ها می‌باشد. در کنار این سازگاری و تطبیق، پیشرفت‌های فناوری تهدیدات امنیتی جدیدی را برای سیستم‌های اطلاعاتی رایانه‌ای ایجاد کرده است. پارکر (۱۹۸۳) بر طبق یک قانون قدیمی معتقد است، اگر چیزی را با یک چکش مناسب و بزرگ بکوبیم مسلما خواهد شکست، در مورد رایانه‌ها، برنامه‌های رایانه‌ای، داده‌ها و کاربران نیازی نیست این چکش خیلی هم بزرگ باشد چون همه‌ی این اجزاء شکننده و آسیب پذیر بوده و خیلی زود صدمه می‌بینند.

۲- مبانی نظری

۲-۱- مفهوم سیستم

سیستم، مجموعه‌ی منظمی از عناصر به هم پیوسته است. که برای رسیدن به اهداف مشترکی با هم در تعاملند (سیستم حسابداری، سیستم بانک اطلاعاتی) و هر سیستم دارای ساختاری است که موارد زیر را در بر می‌گیرد:

۱- درون داده‌ها (اطلاعات ورودی)

۲- برون داده‌ها (نتایج به دست آمده از اطلاعات)

۳- فرایندها و تبدیل‌ها (تجزیه و تحلیل اطلاعات)

حسابداری نیز یک سیستم اطلاعاتی است که به وسیله‌ی آن اطلاعات مربوط به فعالیت‌های مالی شناسایی، ثبت، طبقه‌بندی و تلخیص می‌گردد تا امکان تصمیم‌گیری آگاهانه را برای استفاده‌کنندگان فراهم کند (ودیعی، ۱۳۸۹).

۲-۲- سیستم اطلاعات حسابداری

انجمن حسابداران امریکا از سیستم اطلاعاتی به عنوان پشتیبان تصمیم‌گیری مدیران حمایت نموده و بیان می‌دارد که " سیستم اطلاعاتی حسابداری بخشی از سیستم اطلاعاتی است که به جمع آوری، پردازش، طبقه‌بندی و تلخیص داده‌ها به منظور ارائه اطلاعات به تصمیم‌گیرندگان برون‌سازمانی می‌پردازد" (1974).

سیستم اطلاعاتی حسابداری مؤلفه و عنصری از شرکت است که به وسیله‌ی پردازش رویدادهای مالی، اطلاعات مالی و اطلاعات مبنای تصمیم‌گیری را در اختیار استفاده‌کنندگان قرار می‌دهد. سیستم اطلاعات حسابداری خوب ضمن ارائه گزارش‌ها و اطلاعات کارآمد، می‌تواند به عنوان بازوی توانمند مدیریت مورد توجه قرار گیرد (فاضلی و عدالت، ۱۳۸۹) از آنجا که سیستم اطلاعات حسابداری بر شناخت و درک چگونگی وظایف سیستم حسابداری شامل شیوه‌های گردآوری داده‌های مربوط به فعالیت‌ها و رویدادهای مالی سازمان‌ها، شیوه‌ی تبدیل داده به اطلاعاتی که مدیریت می‌تواند آنها را در سازمان مورد توجه قرار دهد و شیوه‌ی حصول اطمینان از قابلیت دسترسی و اتکاء به آن اطلاعات تأکید می‌کند، یکی از حیاتی‌ترین و اساسی‌ترین سیستمهای سازمان به شمار می‌رود (دیویس، ۱۹۹۷). همچنین این سیستم جهت پردازش رویدادهای مالی و به عنوان مبنایی برای تصمیم‌گیری مدیران و بیان وضعیت یک شخصیت تجاری این شرکت‌ها می‌باشد و این سیستم اطلاعاتی زمانی می‌تواند شرایط لازم برای مدیریت کارآمد را فراهم نماید که افراد کارشناس با اطلاعات تئوریک و تجربه لازم متصدی پردازش اطلاعات مالی باشند.

۲-۳- امنیت اطلاعات

در لغت امنیت به معنی رهایی از خطر، وجود ایمنی، رهایی از ترس یا نگرانی است. چوی بانک (۱۹۹۲) امنیت یک سیستم اطلاعاتی را به صورت " میزان اطمینان از این که تنها داده‌های مجاز و قانونی به یک سیستم وارد یا از آن خارج می‌شوند بدون اینکه اضافات و حذف‌ها، اصلاحات یا برگردان‌های غیرمجاز یا غیر قانونی در زمان بین ورود و دریافت مورد نظر اتفاق بیفتد" تعریف می‌کند.

مارو (۱۹۹۵) امنیت اطلاعات را " حفاظت از اختلال غیر مجاز، اصلاح، افشاسازی، یا استفاده از اطلاعات و منابع اطلاعاتی خواه تصادفی یا عمدا" تعریف می‌کند.

نبود امنیت باعث ایجاد نگرانی عمده برای سازمان‌ها و واحدهای تجاری و غیرتجاری شده است. بنابراین حسابداران و مدیران باید با انواع خطرات و تهدیدات امنیتی به منظور محافظت و نگه‌داری از برنامه‌های کاربردی و اطلاعات موجود در کامپیوترهای مورد استفاده آشنا باشند (دیلی، ۲۰۰۰). بدین منظور حسابداران و مدیران باید به طور صحیح با مدیران و طراحان سیستم در خصوص امنیت اطلاعات موجود در سیستم‌های کامپیوتری خود و مقابله با انواع خطرات و تهدیدات امنیتی مشاوره کنند زیرا انواع خطرات و تهدیدات برای سیستم‌های اطلاعاتی به موازات پیشرفت سریع فناوری اطلاعات در حال تغییر و تحول می‌باشد. به همین دلیل حسابرسان تأکید دارند که نیاز برای افزایش امنیت سیستم‌های اطلاعاتی حسابداری بر طبق آخرین تغییرات و پیشرفت‌های فناوری الزامی است(دیویس، ۱۹۹۷).

۲-٤- امنیت در سیستم‌های اطلاعاتی حسابداری

امنیت یکی از مهم‌ترین مسائل تکنولوژیکی است و اهمیت بالای آن ناشی از این است که امنیت ناکافی در یک سیستم از هر گونه قابلیت اطمینان هنگام گزارش اطلاعات مورد نیاز به افراد درون سازمانی یا برون سازمانی جلوگیری می‌کند و همچنین فرصت جعل، دستکاری و تقلب را افزایش می‌دهد (دیویس، ۱۹۹۷). اهمیت و میزان اتکاء پذیری اطلاعات مالی برای تصمیم‌گیری گروه‌های ذینفع در دنیای امروز برای همگان روشن است امروزه به جرأت می‌توان گفت که هر تصمیم مدیریتی آثار و نتایج مالی در پی دارد؛ به همین جهت، مدیریت برای هر تصمیم‌گیری به اطلاعات مالی قابل اتکاء نیازمند است (میر مجریان و شهشهانی، ۱۳۸۵).

ملیسا والتر (۲۰۰۷) بیان می‌کند که تخصص در سیستم‌های اطلاعاتی و حمایت تکنولوژی از آنها منجر به اصل صلاحیت برای حرفه‌ی حسابداری می‌شود؛ اما، متأسفانه برنامه‌های آموزشی تجاری بدنه‌ی اصلی امنیت سیستم‌های اطلاعاتی را شامل نمی‌شود و برای برطرف کردن آن موارد زیر را پیشنهاد می‌کند.

۱- فراهم کردن شرایط برای مشخص کردن اهمیت مکان‌یابی امنیت سیستم‌های اطلاعاتی به عنوان بخشی از یک آموزش حسابداری؛

۲-فراهم کردن تعدادی راهنمای علمی و کاربردی برای مدرسان سیستم‌های اطلاعاتی حسابداری که تمایل به توسعه و عرضه امنیت سیستم‌های اطلاعاتی دارند.

۲-۵- تخلفات امنیتی در سیستم‌های اطلاعاتی حسابداری

عوامل داخلی و خارجی بسیاری وجود دارد که سبب نقص امنیت سیستم می‌شود. با اهمیت‌ترین دلیل به کارکنان سازمان ارتباط پیدا می‌کند یعنی کسانی که به دارایی‌ها و سیستم‌های حسابداری سازمان دسترسی دارند. مشکلات سازمانی داخلی از قبیل کنترل‌های داخلی ضعیف، خط مشی‌های ضعیف کارکنان و نبود صداقت و درستی در سطوح بالای سازمان از عمده‌ترین دلایل تهدیدات امنیتی است.

طبق نظر هوژن و سیلین (۱۹۹۹) به دلایل زیادی ممکن است کارکنان جرایم رایانه‌ای انجام داده و اقدام به دزدی از کار نمایند. عمومی‌ترین این دلایل می‌تواند انتقام، کینه‌جویی، بدهی شخصی و فقدان کنترل‌های داخلی باشد. امروزه تجارت کار بسیار رقابتی است و کارکنان فشار و استرس زیادی را تحمل می‌کنند؛ در نتیجه، ممکن است احساس کنند بیش از توان از آنها کار خواسته می‌شود و کمتر از حد معمول دستمزد دریافت می‌کنند. حال اگر همزمان با مسائل شخصی جدی و با دشواری مسایل شغلی نیز مواجه باشند انگیزه‌ی آنها برای تقلب افزایش خواهد یافت، با همین شرایط اگر به این معادله کنترل‌های داخلی ضعیف و فناوری در دسترس رایانه‌ایی را نیز اضافه کنیم (که در انجام جرم کمک می‌کنند) آنگاه فرصت انجام تقلب جنبه‌ی واقعی و عینی پیدا می‌کند.

۲-٦- اهداف امنیت در سیستم‌های اطلاعاتی

کامل بودن اطلاعات: اطلاعات قابل اتکاء اطلاعاتی است که جامع، کامل و بدون خدشه باشد بنابراین اطلاعات نباید قابل دستکاری توسط افراد غیر مجاز باشد.

محرمانه بودن اطلاعات: اشخاص حقیقی یا حقوقی غیر مجاز نباید بتوانند اطلاعات را در اختیار گیرند.

استفاده مجاز از اطلاعات: هر کاربر مجاز است که اطلاعات را در حدی که مجاز است دریافت و برای کاربردهای خاص در اختیار گیرد.

در دسترس بودن اطلاعات: اطلاعات باید به موقع و به سرعت در اختیار کاربران مجاز قرار گیرد. کاربر مجاز باید بتواند در زمانی که به اطلاعات نیاز دارد به آن دسترسی داشته باشد (آریا، ۱۳۸۰)

۲-۷- تهدیدات امنیتی در سیستم‌های اطلاعاتی حسابداری

تهدیدات امنیتی بر حسب منبع ایجاد کننده‌ی آن و عامل ایجاد کننده‌ی آن و قصد و نیت فرد مرتکب شونده به سه دسته تقسیم می‌شوند (عرب مازار یزدی، ۱۳۸۹).

۱) تهدیدات درون سازمانی در مقابل تهدیدات برون سازمانی (بر حسب منبع ایجاد کننده)

کارمندان سازمان به عنوان مهم‌ترین منبع تهدیدات امنیتی داخلی هستند حال آنکه هکرها، بلایا و اتفاقات طبیعی به عنوان منبع عمده‌ی تهدیدات خارجی مد نظر قرار می‌گیرند. برخی معتقدند که کارکنان درون سازمانی به شکل بالقوه می‌توانند خطرناک‌ترین دشمنان سیستم باشند و در بیشتر موارد اشتباهات و دسترسی‌های غیرمجاز به اطلاعات ریشه‌ی اصلی مشکلات امنیتی در سیستم است.

۲) تهدیدات انسانی در مقابل تهدیدات غیر انسانی (بر حسب عامل ایجاد کننده)

تهدیدات امنیتی انسانی تهدیداتی هستند که از اعمال انسانی سرچشمه می‌گیرند و می‌توانند تصادفی و غیرعمدی یا عمدی باشند. دیویس (۱۹۹۷) معتقد است، خطاهای انسانی می‌توانند در

قالب خطاهای ناشی از غفلت و سهل‌انگاری و یا جرائم واقع شوند. خطای نوع اول وقتی رخ می‌دهد که فردی در انجام عمل درست و صحیح، ناتوان باشد و خطای نوع دوم زمانی اتفاق می‌افتد که فرد عملی را انجام دهد که نادرست بوده یا انجام آن ممنوع شده است و از سوی دیگر تهدیدات غیر انسانی عموما به تهدیدات فنی از قبیل نقص فنی سیستم یا سخت افزار یا مشکلات نرم‌افزاری سیستم مربوط می‌شود و یا ناشی از بلایای طبیعی از قبیل سیل و زلزله باشد. البته برخی از تهدیدات فنی ممکن است با اعمال انسانی در ارتباط باشد، از قبیل وارد کردن یک ویروس به سیستم از طریق نرم‌افزار آلوده.

۳) تهدیدات غیر عمدی (تصادفی) در مقابل تهدیدات عمدی (بر حسب قصد و نیت فرد مرتکب شونده)

تهدیدات غیر عمدی تهدیداتی هستند که از قصد و نیت کینه جویانه و بد خواهانه نشأت نگرفته‌اند. در حالی که تهدیدات عمدی تهدیداتی هستند که دارای قصد و نیت بدخواهانه مثل خرابکاری، تقلب رایانه‌ای و استفاده نادرست از دسترسی مجاز به سیستم می‌باشند. هوژن و سیلین (۱۹۹۹) معتقدند که اعمال غیر عمدی اگر چه هزینه‌ای را به سازمان تحمیل می‌کنند اما قابل اصلاح هستند و می‌توان از طریق آموزش و نظارت از وقوع آنها جلوگیری کرد. اما اعمال عمدی عموما منجر به جرائم رایانه‌ای شامل نابود کردن اجزاء سیستم، حذف کردن یا تغییر دادن ثبت‌ها و پرونده‌هاو.... به منظور از بین بردن اطلاعات یا تولید اطلاعات نادرست، می‌شوند.

۳-نتایج یافته‌های تحقیقات انجام شده در این زمینه امنیت سیستم‌های کامپیوتری

لاخ و همکاران (۱۹۹۲) در خصوص بحث امنیت در سیستم‌های اطلاعاتی بر اساس یک مدل چهار بعدی به این نتیجه رسیدند که تهدیدات امنیتی ممکن است مثل تهدیدات ناشی از اعمال کارکنان یا عیب و نقص سازمان داخلی باشند یا اینکه مثل اعمال هکرها یا بلایای طبیعی خارجی باشند. بر اساس این مدل بعد دیگر هر تهدید عامل ایجاد کننده می‌باشد؛ بعضی از تهدیدها ناشی از اعمال انسانی هستند حال آنکه برخی دیگر نتیجه‌ی رویدادهای طبیعی یا غیر انسانی می‌باشند و در نهایت، اعمال صرف نظر از منبع آن می‌تواند عمدی یا غیر عمدی باشد.

دیویس (۱۹۹۷) در مطالعاتی که انجام داد به این نتیجه رسید که حسابداران باید درباره‌ی عوامل تهدیدکننده امنیت اطلاعات آگاه باشند چون همان طوری که تکنولوژی به سرعت در حال تغییر است مخاطرات امنیتی اطلاعات نیز به همان سرعت در حال تغییرند و این مخاطرات یکی از نگرانی‌های بزرگ هر واحد اقتصادی است. هوژن و سیلین (۱۹۹۹) در تحقیقات خود به این نتیجه رسیدند که سازمان با استقرار سیستم و اعمال کنترل‌های داخلی مناسب شامل رویه‌های استخدامی خوب و برنامه‌های آموزشی مناسب در مقابل وقوع جرائم رایانه‌ای ایستادگی کرده و میزان زیان وارده را به حداقل ممکن رسانده است.

دیلی و همکاران (۲۰۰۰) در تحقیقات خود به این نتیجه رسیدند که اندازه‌گیری امنیت در سیستم‌های اطلاعاتی حسابداری جدید و در حال پیشرفت باید به عنوان اولین عامل کلیدی مد نظر قرار گرفته شود و اینکه قابلیت اندازه‌گیری امنیت به آگاهی و ثبات تنظیم‌کننده‌های سیستم بستگی دارد و اجزاء کلیدی امنیت اطلاعات شامل رمز عبور، پنهان کردن داده‌ها، مشارکت کارمندان و محافظت در برابر ویروس‌های کامپیوتری است.

دالکی و ویس (۲۰۰۱) در رابطه با سیستم‌های اطلاعاتی کامپیوتری به این نتیجه رسیدند که پیشرفت فناوری اطلاعات شرکت‌ها را قادر ساخت تا از کامپیوتر برای انتقال فعالیت‌های که قبلا به طور دستی اجراء می‌شدند استفاده کنند. جی و همکاران (۲۰۰۵) در تحقیقات خود به این نتیجه رسیدند که مشکلات مربوط به سیستم‌های اطلاعاتی تعدادی از شرکت‌ها را مجبور به افشاء ضعف‌های با اهمیت می‌کند. .

دبرابردو و جوزف ون (۲۰۰۷) به این نتیجه رسیدند که خطرهای موجود در سیستم‌های اطلاعاتی از منابع مختلفی سرچشمه می‌گیرد که اگر نادیده انگاشته شود می‌تواند مربوط بودن و اتکاء پذیری اطلاعات مالی را از بین ببرد و منجر به تصمیم‌گیری نادرست توسط ذینفعان مختلف شود. عرب‌مازار و خسروی (۱۳۸۹) به این نتیجه رسیدند که استفاده از سیستم‌ها با مخاطرات جدیدی نیز همراه است. مدیران باید مترصد شناسایی خطرات بالقوه ناشی از تهدیدات کنترل‌های داخلی موجود در سیستم‌های اطلاعاتی حسابداری مبتنی بر رایانه باشند و با استفاده از انواع مدل‌ها اثار این مخاطرات را ارزیابی کنند.

میهالاچ و ساموئل (۲۰۱۱) به این نتیجه رسیدند که بیشتر عملیات دفتری در تشکیلات اقتصادی امروزی بر عهده‌ی سیستم اطلاعات حسابداری است و از طرفی با توجه به این‌که

زنجیره‌ای از عوامل (جهانی شدن، دسترسی غیر مجاز و...) این سیستم‌ها را تهدید می‌کند بنابراین امنیت باید یکی از مهم‌ترین مسائل در برنامه‌ی کاری هر شرکت باشد.

کوز (۲۰۱۱) به این نتیجه رسید که ریسک را می‌توان از سه دیدگاه تجزیه و تحلیل کمی، کیفی و تجزیه و کامپیوتری بررسی کرد که این تجزیه و تحلیل‌ها بیشتر در سازمان‌های بزرگ و سازمان‌های متوسط انجام می‌شود اما در سازمان‌های کوچک بودجه لازم و کارمندان کافی برای انجام این تجزیه و تحلیل‌ها وجود ندارد اما حداقل باید ارزیابی‌های امنیتی را انجام دهند.

پاول و همکاران (۲۰۱۲) در تحقیق خود درباره‌ی ارتباط بین حسابرسی داخلی و امنیت اطلاعات به این نتیجه رسیدند که حسابرسی داخلی و بخش امنیت اطلاعات باید به طور گروهی با هم همکاری کنند زیرا کارمندان بخش امنیت اطلاعات ابزارها و شیوه‌های مختلف عملیاتی و تکنولوژیکی را برای حفاظت از منابع سازمان به کار می‌گیرند و حسابرسی داخلی یک بازخورد دوره‌ای درباره‌ی انواع فعالیت‌های که به بهبود امنیت اطلاعات کمک می‌کنند، فراهم می‌کند.

نتیجه‌گیری

سیستم‌های اطلاعاتی حسابداری مبنایی برای تصمیم‌گیری مدیران است و مدیران زمانی قادر به تصمیم‌گیری صحیح هستند که اطلاعات سیستمی در اختیار آنها علاوه بر ویژگی‌های مربوط بودن و به موقع بودن، امنیت نیز در آن تعبیه شده باشد که قابلیت اطلاعات مورد استفاده را تضمین کند. امروزه کمتر سازمانی را می‌توان یافت که از شبکه‌های رایانه‌ای استفاده نکند و اطلاعات با ارزشی را در آن ذخیره ننماید. تمامی این سازمان‌ها از ارتباطات پرسرعت و کم سرعت اینترنتی بهره می‌گیرند. از طرف دیگر، نفوذگران نیز مجهز به ابزارهای پرقدرت و ارزان قیمت نرم‌افزاری و سخت افزاری به منظور بهره‌گیری اقتصادی، ارضای کنجکاوی و اخلال در این شبکه‌ها هستند. بنابراین استقرار یک سیاست امنیتی موثر و پویا، وظیفه هر سازمان برای حفاظت از اطلاعات و وجهه خود است.

مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف امنیتی، بررسی موانع موجود برای رسیدن به این اهداف و ارائه راهکارهای لازم را بر عهده دارد. همچنین مدیریت امنیت وظیفه پیاده سازی و کنترل عملکرد سیستم امنیت سازمان را برعهده

داشته و در نهایت باید تلاش کند تا سیستم را همیشه به روز نگه دارد، بنابراین مدیران و حسابداران باید با انواع تهدیدها و روش‌های ایجاد امنیت در سیستم‌های اطلاعاتی آشنا باشند تا موفق به ایجاد امنیت در سیستم‌های اطلاعاتی خود شوند. البته تهدیدات را نمی‌توان به طور کامل از بین برد اما با انجام اقداماتی مشخص می‌توان تا حدودی ان را محدود کرد. برقراری امنیت قابل قبول در سیستم‌های اطلاعاتی حسابداری باعث افزایش قابلیت اتکاء و قابلیت اعتماد گزارش‌های مالی می‌شود که این امر منجر به مفید بودن اطلاعات مندرج در گزارش‌های مالی برای تصمیم‌گیری استفاده‌کنندگان درون سازمانی و برون سازمانی خواهد شد.

منابع

آریا، ناصر. دی ماه ۱۳۸۰. «حسابرسی شبکه‌های کامپیوتری» نشریه‌ی سازمان حسابرسی، شماره ۱۵۲

عدالت، احمد ؛ فاضلی، احمد. زمستان ۱۳۸۹. «سیستم اطلاعات حسابداری» نشریه حسابرس، شماره ۵۱، صص ۱۲۰-۱۲۴

ودیعی، محمد حسین ؛ محمدی، جمال. زمستان ۱۳۸۹ «امنیت در سیستم‌های اطلاعاتی حسابداری» نشریه حسابرس، شماره ۵۱، صص ۹۰-۹۴

عرب مازار یزدی، محمد ؛ خسروی، یاور. پاییز ۱۳۸۵. «ارزیابی خطر ناشی از تهدیدهای کنترل داخلی در سیستم‌های اطلاعاتی حسابداری مبتنی بر رایانه» ماهنامه حسابدار، شماره ۱۷۶، صص ۷۳-۸۵

میر مجرییان، حمید ؛ شهشهانی، سید محمد حسن. زمستان ۱۳۸۵. «کارایی تصمیم‌گیری در گزارشگری مالی در محیط شبکه گسترده جهانی». حسابرس. شماره ۳۵، صص ۳۷-۴۵

Charles e. davis. « an assessment of accounting information security». The cpa journals. Vol 67.

Haugen susanandj. Rogerselin (1999). « identifying and controlling computer crime and employe fraud». industrial management and data systems. Vol 99.

Loch,KarenD. Houston H. carrandMerill E. warkentin (1992) « threats to information system: today reality, yesterday understanding» MIS Quarterly. june.

Parker. DonnB (1983). «fighting computer crime». Charles scribners sons.

Riner , Kelly Rex, Charles A. Snyder and Houston H. carr (1991). «risk analysis for information technology» management information system. vol 8

Melissa walters (2007). «a draft of an information systems security and control course». Journals of information system. 5-34

Wang Ry, StrondD (1996). Beyond accuracy «what data quality means to data costomers» . journal management information system.

Deborah BeardandH. Josephwen (2007). « Reducing the thereate level for accounting information system , challenges for management , accoutingAuditorsandAcademicacians». CPA journals

Daily C. and lueblfing, M. (2000)« . Defending the security of the accounting system». The CPA Journals. 62-65

Blakley B, E. Mcdermott and D. Geer. « information security in information risk manamement, in proceeding of NSPW». Cloudcroft ,newmexico. USA, 2002

Paul johansteinbart, Robyhl. Raschke, graham gal, William N. Dilla« the relationship between internal audit an information security: An explorantory investigation». International journal of accounting information systems. 2012

Ge. W. andS. Mcvay. 2005. «the disclosure of material weeknessein internal control after the Sarbanes ». oxleyact. Accounting Horizons 19 (3): 137- 158

Mihalache D. Avsenie- samoil. (2011). « security of the Accounting information system infrastructure». 1339-1345

Ilhan. D, and veysi. n. t. 2001. Review of social , Economic &Bussiness studies locity , M. C. and L. P Willcocks (1998). « an empirical investigation of information technology sourcing ». lessons from experience MIS Quarterly 22 (3). 363-408

Ling-yu, chou, Charles. Du, timon, S. Vincent,lai, (2007). و continuous auditing whit amulti agent system». Decision support systems,No. 42. pp. 2274-2292