شناسایی چالش های امنیت فناوری اطلاعات در حسابرسی دیوان محاسبات کشور

محبوبه سلیمانی اصل*

چکیده:

موضوع بکارگیری فناوری اطلاعات در حسابرسی سالهاست که در دنیا مطرح شده و در سطح دیوان محاسبات نیز در این خصوص بحث می شود و آثار بکارگیری آن در بخش حرفه ی حسابرسی یا به تعبیر دیگر کاربرد فناوری اطلاعات در عملکرد دیوان محاسبات مورد توجه قرار گرفته است. با توجه به این موضوع هدف از پژوهش حاضر شناسایی چالش های امنیت فناوری اطلاعات در حسابرسی دیوان محاسبات کشور در سال ۱۳۹۱ می باشد. این تحقیق از نوع توصیفی-پیمایشی و کاربردی بوده و جامعه آماری آن شامل مدیران ، معاونین ، حسابرسان و مدیران فناوری اطلاعات دیوان محاسبات استانهای تهران، قم، مرکزی، سمنان، البرز، قزوین (به تعداد ۲۴۷ نفر) می باشد. روش نمونه گیری مورد استفاده ،روش نمونه گیری تصادفی ساده بوده که اندازه نمونه معادل ۱۲۷ نفر تعیین شده است .

با توجه به مصاحبه با افراد خبره عوامل چالش ها شناسایی گردید و برای گردآوری اطلاعات از پرسشنامه استفاده شده و اعتبار محتوای آن توسط اساتید راهنما و مشاور و چند نفر از افراد مطلع و متخصص تأیید گردیده و پایایی بر اساس آلفای کرونباخ اثبات شده است.

در این پژوهش پنج عامل ۱) عوامل مدیریتی و خط مشی سازمان ۲) عوامل فیزیکی ۳) کاربران وآموزش و فرهنگ امنیتی ۴) زیرساختهای امنیتی فناوری اطلاعات ۵) عوامل امنیتی سیستم های اطلاعاتی بعنوان چالش های فناوری اطلاعات شناسایی گردیده است.

با توجه به نتایج بدست امده عوامل زیرساختی فناوری اطلاعات در مرتبه اول ، عوامل مدیریتی و خط مشی سازمان و همچنین عوامل امنیتی سیستم های اطلاعاتی در مرتبه دوم و عوامل کاربران ، اموزش ، فرهنگ امنیتی در رتبه سوم و در نهایت عوامل فیزیکی در مرتبه آخر قرار گرفته اند.

واژگان کلیدی: امنیت فناوری اطلاعات ، امنیت فناوری اطلاعات در حسابرسی ، عوامل فیزیکی ، سیستم های اطلاعاتی ، مدیریت و ساختار سازمانی ، زیرساختهای امنیتی

* کارشناس ارشد حسابداری دانشگاه تهران ،دیوان محاسبات کشور m_soleimani@dmk.ir

۱- مقدمه:

حسابرسی در محیط فناوری اطلاعات فرآیند جمع آوری ، تجزیه وتحلیل اسناد ومدارک در محیط فنآوری اطلاعات می باشد. بنابراین الگو هاو روش های سنتی و دستی پاسخگو وبرآورد کننده انتظارات سازمان نمی باشند. دیوان محاسبات کشور در نظر دارد با استفاده از فناوری اطلاعات در انجام امور حسابرسی و پیاده‌سازی طرح سامانه نظارت الکترونیکی (سنا)ضمن کاهش مدت زمان گردآوری اطلاعات در حوزه حسابرسی، دقت و صحت اطلاعات مالی جمع‌آوری شده را افزایش داده و به نحوی محدوده نظارت مالی و بودجه‌ای خود را افزایش دهد.

دیوان محاسبات کشور در نظر دارد با استفاده از فناوری اطلاعات در انجام امور حسابرسی و پیاده‌سازی طرح سامانه نظارت الکترونیکی (سنا)ضمن کاهش مدت زمان گردآوری اطلاعات در حوزه حسابرسی، دقت و صحت اطلاعات مالی جمع‌آوری شده را افزایش داده و به نحوی محدوده نظارت مالی و بودجه‌ای خود را افزایش دهد.سامانه نظارت الکترونیکی سیستم و مکانیزمی است که کاربران و پرسنل دیوان محاسبات با استفاده از امکانات آن بتوانند در کمترین زمان با بیشترین میزان دقت و صحت قادر به دستیابی به اطلاعات مورد نیاز جهت انجام حسابرسی کلیه وزارتخانه ها و دستگاههای استفاده کننده از بودجه باشند لازم به ذکر است که از عمده اطلاعات قابل استفاده از این سیستم اطلاعات بودجه ای و مالی موسسات دستگاههای دولتی و همچنین کلیه قوانین و مقررات و مصوبات تصویب شده بصورت بروز می باشد.

لذا در این تحقیق بر روی شناسایی چالشهای امنیتی فناوری اطلاعات در سال ۱۳۹۱ تمرکز شده است چراکه سازمانهاو مؤسسات حسابرسی باید یک زیرساخت مناسب اطلاعاتی برای خود ایجاد کنند و در جهت سازماندهی اطلاعات در سازمان خود حرکت نمایند.برای این منظور باید ارزشیابی روی امنیت داراییهای سازمان(سخت افزار، نرم افزار ، اطلاعات ، ارتباطات و کاربر) صورت گیرد.تا با شناسایی موانع و چالش های امنیتی عوامل موثر در نابودی اطلاعات شناخته شود.در صورت عدم رفع این موانع حسابرسی با استفاده از فناوری اطلاعات از اعتبار لازم برخوردار نبوده و قابل اتکا نمی باشد و از محاسن آن نمی توان بهره گرفت .

۲- مبانی نظری

در اوایل دهه ۸۰ میلادی امنیت فقط با دیدگاه فنی مشاهده می شد و برقراری آن منوط به امنیت رایانه و دستگاه های جانبی می دانستند. اما با گذشت زمان متوجه شدند که بیشتر تجاوزات امنیتی از طریق مسائلی همچون ضعف های مدیریتی)از لحاظ امنیتی(و عوامل انسانی)به دلیل عدم آموزش(می باشد لذا از اواسط دهه ۸۰ میلادی تا اواسط دهه ۹۰ میلادی بحث مدیریت امنیت اطلاعات مطرح شد که آن را منوط به خط مشی امنیت اطلاعات و ساختارهای سازمانی ومؤلفه هایی چون استانداردهای امنیت اطلاعات، گواهی نامه های بین المللی، فرهنگ سازی امنیت اطلاعات در سازمان ، پیاده سازی معیارهای ارزیابی دائمی و پویایی امنیت اطلاعات دانستند (اسدی،۱۳۸۴)

امنیت اطلاعات به چهار مفهوم کلی قابل تقسیم است:

۱- محرمانگی۲- تمامیت ۳ - اعتبار و سندیت -۴ دسترسی پذیری.(حنفی زاده،۱۳۸۴)

هدف مدیریت امنیت اطلاعات در یک سازمان، حفظ سرمایه های)نرم افزاری، سخت افزاری، اطلاعاتی و ارتباطی و نیروی انسانی(سازمان در مقابل هر گونه تهدید) اعم از دسترسی غیرمجاز به اطلاعات، خطرات ناشی از محیط و سیستم و خطرات ایجاد شده از سوی کاربران(است .و برای رسیدن به این هدف نیاز به یک برنامه منسجم دارد.سیستم امنیت اطلاعات با تدوین استانداردها راهکاری برای رسیدن به این هدف می باشد. (رسولیان ،۱۳۹۰)استانداردهای امنیت به دو دسته اصلی تقسیم می گردد که دسته اول در رابطه با امنیت از لحاظ فنی و دسته دوم در رابطه با امنیت ازلحاظ مدیریتی است که قسمت های مختلف مدیریت سازمان را در بر می گیرند. (ویلسون،۲۰۰۵) استانداردهای ISMS در ۷ استاندارد تصویب گردید اندکه استاندار مدیریتی BS۷۷۹۹ موسسه استاندارد انگلیس،از برجسته ترین استانداردها و راهنماهای فنی که شامل ده گروه کنترلی می باشد. (خالقی،۱۳۸۶)

بر طبق نظر سادوسکای و همکاران،(۲۰۰۳) به طور کلی چالش های امنیتی را به ۴ دسته ذیل تقسیم می گردد:

۱- چالش های امنیتی رایانه ۲-چالش های امنیتی سیستم اطلاعاتی ۳-چالش های امنیتی در شبکه۴- چالش های امنیتی کاربران تقسیم می گردد. کنترل های فراهم کنندهٔ امنیت اطلاعات می توانند فیزیکی یا تکنیکی و مدیریتی باشد. کنترلهای فیزیکی شامل تهدیدات فیزیکی و ایمن سازی فیزیکی اطلاعات وکنترلهای مدیریتی در دو سطح کاربردی و مرکزی وشامل ایمن سازی مدیریتی و خط مشی سازمان بوده همچنین کنترلهای تکنیکی و تهدیدات آن در شبکه ،رایانه،کاربران و سیستمهای اطلاعاتی بوجود می آید (فارس،۱۳۸۷).

بر اساس استاندارد BS۷۷۹۹ نظام مدیریت امنیت اطلاعات ISMS باید شامل روش های ارزیابی، محافظت، مستندسازی و بازنگری باشد، که این مراحل در قالب یک چرخه PDCA تحقق پذیر است. حسابرس سامانه اطلاعاتی بایستی به ارزیابی مناسب بودن فناوری و رمزگذاری ،اعتبار و صحت دریافتها و پرداختها ،کفایت کنترلها در انتقال داده های اولیه در بین فرایندها،کفایت کنترلها به منظور جلوگیری از تغییر و مخدوش کردن داده ها به صورت سهوی و عمدی و کفایت کنترل بر داده های بایگانی شده بپردازد. (سعیدی،۱۳۸۸) بر اساس بخش ۴۰۱ استاندارد بین المللی حسابرسی با عنوان "حسابرسی در محیط سامانه اطلاعاتی " به منظور برنامه ریزی ،هدایت،سرپرستی و مرور کارهای انجام شده لازم است حسابرس از دانش کافی به منظور ارزیابی جنبه های مختلفی چون رمزگذاری ،شیوه های امنیت شبکه و فناوری های امنیتی همچون سامانه امنیتی ، حفاظت در مقابل ویروس ، ردیابی تلاشهای تعدّی گرانه مورد نیاز است از این رو حسابرس سامانه اطلاعاتی برای حفظ صلاحیت فنی خود بایستی بطور مستمر تحت آموزش حرفه ای قرار گیرد.

۳- پیشینه پژوهش

دیلون و ترک زاده (۲۰۰۶)به بررسی امنیت سیستم اطلاعات (IS)[1] و تداوم آن به عنوان چالشی برای مدیران و متخصصان پرداخته و با استفاده از روش تفکر متمرکز بر ارزش به شناسایی اهداف "اصلی" امنیت IS و راه های دستیابی به این اهداف می پردازد. نتایج حاصل از آن ،۸۶ هدف اصلی که در زمینه مدیریت امنیت IS ضروری هستند را مشخص می سازد.

کاردناس و همکارانش (۲۰۰۸)تلاش نمودند چالش های امنیت سیستم های کنترلی را شناسایی نموده به دو پرسش پاسخ داده شود: (۱) چرا باید به دنبال امنیت سیستم های کنترل باشیم؟ و (۲) شرایط مختلف و مشکلات اساسی امنیت سیستم های کنترل چه هستند؟ و نتایج خود را بصورت یک چارچوب جدید ریاضی برای تجزیه و تحلیل حملات علیه سیستم های کنترل ارائه می نماید.

در پژوهشی دیگر اسمیت و جامسون (۲۰۰۶)به بررسی محرک هاو فاکتورهای کلیدی در امنیت سیستم های اطلاعاتی در دولت الکترونیکی و و موانع مهم امنیت سیستم اطلاعاتی و تداوم مدیریت تجاری در دولت الکترونیکی می پردازد. نتایج حاصل از این تحقیق نشان می دهد که مسائل اصلی اجرا و پیاده سازی امنیت عبارتند از آگاهی، حمایت از مدیریت فعال، آموزش، و بودجه مناسب.

یکی از مباحث امنیتی نفوذ به اطلاعات می باشد آندرو مور (۲۰۰۱) مدل سازی حمله و نفوذ به اطلاعات و بقاو تداوم اطلاعات را مورد بررسی قرار داده است .نتیجه این پژوهش نشان می دهد که چگونه می توان الگوهای عمومی نفوذ را مستند سازی و سازماندهی کرد و چگونه می توان از آنها مجدداً برای تسهیل ساخت و ساز فرایند استفاده کرد. همچنین توسعه روش هایی برای استخراج شرایط و طراحی سیستم های سازمانی و عملیاتی است که در مقابل حملات مخرب بیشتر و بهتر دوام می آورند.

چاو (۲۰۰۳) نظریه سیستم مجموعه مدیریت امنیت اطلاعات را مورد توجه قرار داده و نتیجه حاصله در این پژوهش نشان می دهد یکی از چالش های امنیتی، فقدان نظریه مدیریت امنیت اطلاعات می باشد. بنابراین به بیان استراتژی امنیت اطلاعات و چگونگی رفتار سازمانی با توجه به مدیریت امنیت اطلاعات پرداخته است.نوشته ها و دیدگاه های مختلف مجموعه درباره خط مشی امنیت، مدیریت ریسک، کنترل و حسابرسی، سیستم های مدیریتی را می سازد که می تواند پایه و اساس محکمی برای مطالعات تجربی بیشتر باشد.

موروتیدیس (۲۰۰۳)در پژوهشی به یکپارچه سازی امنیت و سیستم های مهندسی از طریق مدل سازی سیستم های اطلاعاتی ایمن پرداخته اند . وبه این نتیجه رسیده است که معرفی یک فرایند است که با استفاده از مفاهیم و نمادهای یکسان، امنیت و سیستم های مهندسی در کل فرایند توسعه سیستم ادغام می کند. این فرآیند با وسیله پنج ایده کلیدی مشخص می شود.

ماندول و ورما (۲۰۰۴) در تحقیقی به مباحث حسابرسی برخط و چالش های امنیتی اطلاعات حسابرسی می پردازد وبه این نتیجه رسیده اند که حسابرس هنگام حسابرسی برخط باید مطمئن شود که کنتر لهای لازم برای حفظ محرمانگی، صحت و دردسترس بودن داده ها و اطلاعات در حال پردازش وجود دارد .

1- Information system

ژیو در سال (۲۰۰۹)را ه حل امنیتی به کار گرفته شده در حسابرسی برخط در کشور چین را بررسی نموده و در خصوص مسائل امنیتی بر خط ۵ راهکار کاربردی را که بطور ایمن تیم حسابرسان می توانند از ان بهره ببرند مطرح نموده است.

محمود زاده و راد رجبی(۱۳۸۵) شناسایی و سنجش تأثیر عواملی است که سیستمهای اطلاعاتی سازمانها را با خطر سرقت، نابودی و یا تغییر اطلاعات مواجه میسازند را در تحقیق خود مورد بررسی قرار داده و دریافتند که مؤلفه عدم آگاهی کاربران بالاترین تهدید و پس از آن امنیت نیروی انسانی دومین تهدید برای امنیت اطلاعات سیستمهای رایانه ای می باشد. مؤلفه های امنیت فیزیکی و امنیت اطلاعات به ترتیب در رتبه های بعدی قرار دارند.

الهی و همکارانش(۱۳۸۸) در راستای الگوی بر "امنیت اطلاعات رفتاری" تمرکز داردر این راستا فاکتور های مؤثر بر اثربخشی امنیت سیستم های اطلاعاتی معرفی می شوندمحقق دراین پژوهش به این نتیجه رسیده که عوامل انسانی نسبت به عوامل فنی و تاکتیکی دارای تأثیر و ارزش بیشتری بر اثربخشی ISS[1] دارند.

امیر خوانی (۱۳۸۸) در پایان نامه خود به ارائه مدلی جهت شناسایی عوامل مؤثر بر اثر بخشی سیستم مدیریت امنیت اطلاعات در سازمانهای دولتی پرداخته و در نتایج حاصل از آن عوامل مؤثر در سیستم مدیریت امنیت اطلاعات در سازمانهای دولتی شناسایی گردیده است.

در دیماه سال (۱۳۸۶) ترک لادانی، وهمکاران تلاش نموداند در تحقیقی با تأمل بر فعالیتهای انجام شده در زمینه ISMS، دیدگاه روشنی از وضعیت موجود، چالشها و راهکارهای مناسب برای ادامه این روند ارائه نمایند.پژوهشگران دریافتند چالشهای استقرار ISMS در سازمانهای دولتی را می توان در عوامل موثر بر پیاده سازی امنیت و عوامل شکست پروژه ISMS از سوی سازمان و پیمانکار و ممیزان طبقه بندی نموده است.

عرب مازار و محمدی (۱۳۸۵) در مقاله ای به تهدیدات امنیتی سیستم های اطلاعاتی رایانه ای از دیدگاه صاحب نظران، طبقه بندی گوناگون تهدیدات امنیتی و دلایل این تهدیدات پرداخته و در نتیجه تقلبات رایانه ای را در قالب تهدیدات مربوط به داده های ورودی سیستم، فرآیند پردازش سیستم، خروجی های سیستم طبقه بندی گردیده است.

رضایی (۱۳۸۷)در یکی از جدید ترین پژوهشهای انجام شده بین المللی به بررسی اثر فرهنگ سازمانی بر اثر بخشی سیاست های مدیریت امنیت اطلاعات می پردازد و دریافت از آنجائیکه ،کاربر نهایی هر سامانه امنیتی انسان است ،هیچ سامانه اطلاعاتی بدون مدیریت کاربران آن ،کارآمد نخواهد بود.بنابراین اجرای اثربخش و مناسب مدیریت امنیت اطلاعات ،نیازمند ترکیبی از فرهنگ سازمانی مطلوب ،فناوری امنیتی متناسب و نگرش پشتیبانی گرای مدیریت است.

هادی نیا (۱۳۸۸)شناسایی موانع اجرایی شدن حسابرسی الکترونیک در دیوان محاسبات کشور مورد بررسی قرار داده با توجه به نتایج به دست آمده مشخص گردیده که مواردی مثل آموزش، زیرساخت های امنیتی و قانونی، زیرساخت های فناوری اطلاعات و عوامل مدیریتی اجرایی شدن حسابرسی الکترونیکی می شود.

1- Information system security

عبداللهی‌ازگمی (۱۳۷۵) طراحی و پیاده‌سازی سرویس‌های امن برای شبکه‌های کامپیوتری موضوع کار خود قرار داده است و نایج ان ارائه مطالبی در خصوص مبنای امنیت سیستم‌های کامپیوتری و تهدیدهای امنیتی شبکه‌ها و سرویسهای آن، مدل‌های امنیتی و ارزیابی امنیت نیز بررسی و متغیرهای اولیه‌ای نیز برای ارزیابی سرویسهای امن می باشد.

فلاح و همکارش (۱۳۸۱) در خصوص امنیت شبکه کامپیوتری به توصیف شکلی قابلیت دسترسی و از کار اندازی سرویس در شبکه های کامپیوتری پرداخته و دریافت است که در خصوص حملات از کاراندازی سرویس تاکنون یک روش مناسب برای تحلیل حمله ها یا روشی برای ارزیابی کارایی راه حلهای ارائه شده به منظور غلبه بر این حمله ها فراهم نکرده اند.

اسدی(۱۳۸۴) فناوری های امنیت اطلاعات: با یک دیدگاه طبقه بندی ،فناوری اطلاعات را از لحاظ امنیتی و بر اساس زمان به دو گروه تقسیم نموده و دریافت مرحلهٔ خاصی از زمان که در هنگام تعامل فناوری با اطلاعات، عکس العمل لازم در برابر یک مشکل امنیتی، ممکن است کنشی یا واکنشی باشد.

حسن آقای (۱۳۸۳) در پژوهش خود در زمینه بررسی تاثیر فناوری اطلاعات بر ویژگیهای کیفی ازاطلاعات حسابداری و قابلیت اعتماد به اطلاعات انجام داده است. نتایج حاصله در این تحقیق نشان می دهد که استفاده از فناوری اطلاعات، تغییرات قابل توجهی درکیفیت گزارش گری مالی ایجاد کرده است، به ویژه افزایش در کیفیت مربوط بودن اطلاعات حسابداری که به طور عمده از به موقع بودن اطلاعات ناشی می شود. لیکن با وجود مزایا ی بسیار فناوری اطلاعات برای گزارش گری مالی، قابلیت اعتماد اطلاعات کاهش می یابد.

ضمنا تا قبل از این هیچگونه پژوهشی در ایران در خصوص شناسایی امنیتی فناوری اطلاعات در حسابرسی انجام نگردیده است و تحقیق حاضر اولین پژوهش در این زمینه می باشد.

۴- اهداف و فرضیه پژوهش

به منظور دستیابی به پاسخی مناسب جهت سوال اصلی این پژوهش که: چالشهای امنیت فناوری اطلاعات در حسابرسی دیوان محاسبات کشور کدامند؟ فرضیه این تحقیق طراحی شد که در قالب آن مواردی از چالشهای امنیت فناوری اطلاعات در حسابرسی دیوان محاسبات مشخص گردید.

۵- روش شناسایی پژوهش

۵-۱- روش پژوهش

این پژوهش از لحاظ روش توصیفی- پیمایشی است و از حیث هدف با توجه به ابعاد عملکردی موضوع کاربردی است. به منظور جمع آوری داده ها در پژوهش حاضر از روش کتابخانه ای، مطالعات میدانی، پرسشنامه و مصاحبه استفاده شده است. در نتیجه کتاب ها، مقالات، اسناد، دستورالعملها و مبانی مربوطه و

استانداردهای امنیتی مربوط به موضوع پژوهش مورد بررسی و با توجه به ان و از طریق مصاحبه به شناسایی موانع پرداخته شده و سپس با استفاده از پرسشنامه مطلب مورد نظر در خصوص تاثیر عوامل امنیتی ، جمع آوری و بصورت توصیفی مورد تحلیل قرار گرفت تا چالشهای امنیتی فناوری اطلاعات در حسابرسی دیوان محاسبات مشخص گردد. در این پژوهش از روش پیش آزمون استفاده گردیده که با استفاده از ۱۰ پرسشنامه میزان آلفای کرونباخ برابر ۰/۹۱۸۰ بدست آمد که نشانگر پایائی بالای پرسشنامه مورد استفاده می‌باشد. سوالات پرسشنامه بر مبنای طیف ۵ گزینه ای لیکرت حاوی ۵۲ پرسش در ۵ قسمت اصلی است مطرح شده اند و ارزش آن نشانگر میزان تاثیر آنها می باشد . سپس تعداد ۱۲۷ پرسشنامه در جامعه اماری توزیع و از پرسشنامه وصول شده در تجزیه و تحلیل اماری پژوهش استفاده شدند.

۲-۵-جامعه آماری و قلمرو پژوهش

در تحقیق حاضر، جامعه آماری شامل مدیران، معاونین، حسابرسان و مسئولان و کارشناسان فناوری اطلاعات دیوان محاسبات کشور است با توجه به این مطلب حجم جامعه آماری در سطح کشور ۱۲۰۰ نفر می‌باشد.با توجه به وجود ۳۲ استان و نیز وجود تعداد کارکنان نسبتاً زیادی که در هریک از استانها هستند، از شیوه نمونه‌گیری تصادفی استفاده گردید. داده‌های این پژوهش آخرین وضعیت امنیت در فناوری اطلاعات در این جامعه اماری در بازه زمانی خرداد لغایت مرداد ۱۳۹۱ گردآوری شده است.

جدول شماره(۱)

ردیف	نام استان	تعداد افراد جامعه	حجم نمونه	درصد
۱	تهران	۷۵	۳۹	۷/۸۷
۲	البرز	۲۰	۱۰	۳۰/۷۱
۳	سمنان	۳۴	۱۸	۱۴/۱۷
۴	مرکزی	۴۴	۲۳	۱۲/۶۰
۵	قزوین	۳۰	۱۶	۱۶/۵۴
۶	قم	۴۰	۲۱	۱۸/۱۱
	جمع	۲۴۳	n = ۱۲۷	۱۰۰

۳-۵)روش های آماری به کار رفته در پژوهش

روش های آماری مورد استفاده در پژوهش حاضر آمار توصیفی و استنباطی است. علیرغم محدودیت های فوق با جمع آوری پرسش نامه ، داده های خام تلخیص شدند و با استفاده از نرم افزارهای مربوطه که مشهورترین آنها SPSS می باشد کار تجزیه و تحلیل داده ها به اتمام رسید.برای

آزمون فرضیه های این تحقیق و تجزیه و تحلیل آنها از روش‌های آزمون t تک نمونه‌ای، آزمون رتبه بندی فریدمن و آزمون های تکمیلی ویلککسون استفاده شده است.

۶- روش نمونه گیری و حجم نمونه

با توجه به وجود ۳۲ استان و نیز وجود تعداد کارکنان نسبتاً زیادی که در هریک از استانها هستند، از شیوه نمونه‌گیری تصادفی استفاده گردید.در دیوان محاسبات کشور ۳۲ استان به شش منطقه تقسیم گردیده است که منطقه یک بدلیل اهمیت بعنوان جامعه نمونه آماری انتخاب شده و استانهای تشکیل دهنده ان ۶ استان : تهران، البرز، مرکزی، قزوین، سمنان و قم می باشند و سپس از کارکنان هریک از استانهای مذکور نمونه گیری انجام گردید.

با توجه به محدود بودن جامعه، برای تعیین اندازه نمونه از فرمول زیر استفاده شد :

$$n = \frac{N z^2_{\frac{\alpha}{2}} \sigma_x^2}{\varepsilon^2 (N-1) + z^2_{\frac{\alpha}{2}} \sigma_x^2}$$

که در این پژوهش از روش پیش آزمون استفاده گردیده که با استفاده از ۱۰ پرسشنامه اولیه واریانس مؤلفه‌ها بدست آمد.سوالات پرسشنامه بر مبنای طیف لیکرت مطرح شده اند .لذا نسبت به هرسوال میانگین مشخص می شود هر چقدر میزان واریانس بیشتر باشد پراکندگی داده ها بیشتر و نظرات متفاوت تر خواهد بود و اندازه نمونه آماری بزرگتر می باشدلذا از حد بالای واریانس استفاده می نماییم تا بزرگترین اندازه نمونه بدست آید و تمامی اندازه نمونه مولفه های دیگر را پوشش دهد. از آنجا که هرقدر واریانس منظور شده بزرگتر باشد حجم نمونه افزایش می‌یابد؛ بیشترین واریانس بدست آمده به میزان ۰/۳۶۹ (مربوط به مؤلفه «عوامل مدیریتی و خط مشی سازمان») به عنوان برآورد واریانس جامعه منظور شد. لذا با توجه به محدود بودن جامعه، برای تعیین اندازه نمونه با توجه به فرمول بالا تعداد نمونه معادل ۱۲۷ نفر تعیین گردیدکه بدین صورت مقادیر پارامترهای مربوطه به شرح ذیل مورد استفاده قرار گرفت :

جدول شماره(۲)

ردیف	عنوان	شرح	مقدار
۱	N	حجم جامعه	۱۲۰۰
۲	α	سطح خطا	۰/۰۵
۳	$z_{\frac{\alpha}{2}}$	مقدار آماره z	۱/۹۶
۴	S_x^2	برآورد واریانس جامعه δ_x^2	۰/۳۶۹
۵	ε	میزان دقت	۰/۱۰
6	**n**	**اندازه نمونه**	**۱۲۷**

برای جمع آوری اطلاعات ۱۲۷ پرسشنامه توزیع شد که پس از تکمیل و وصول آن، در تجزیه و تحلیل آماری پژوهش مورد استفاده واقع شده است.

۷- تحلیل داده های پژوهش

۱-۷-تجزیه و تحلیل توصیفی داده‌ها

در این بخش با استفاده از جدولها به تحلیل توصیفی داده‌ها پرداخته شده است.. ابتدا ویژگی‌های جمعیتی پاسخ‌دهندگان توصیف می‌شود این ویژگی‌های شامل : استان محل خدمت و سمت سازمانی افراد پاسخ‌دهنده می‌باشد. در بخش دوم به مقایسه نظرات پاسخ‌دهندگان با ویژگی‌های جمعیتی متفاوت در خصوص مؤلفه‌های تحقیق پرداخته شده است.

طبق نتایج آمار توصیفی، افراد در نظر گرفته شده در نمونه آماری دارای میانگین سنی ۳۵ سال، میانگین ۱۰ سال تجربه کاری تحصیلکرده و دارای دانش کافی در زمینه فناوری در حسابرسی بودند.

جدول شماره(۳):توزیع فراوانی پاسخ‌دهندگان برحسب استان محل خدمت

ردیف	استان محل خدمت	فراوانی	درصد
۱	البرز	۱۰	۷/۸۷
۲	تهران	۳۹	۳۰/۷۱
۳	سمنان	۱۸	۱۴/۱۷
۴	قزوین	۱۶	۱۲/۶۰
۵	قم	۲۱	۱۶/۵۴
۶	مرکزی	۲۳	۱۸/۱۱
جمع		۱۲۷	۱۰۰

جدول شماره(۴):توزیع فراوانی پاسخ‌دهندگان برحسب سمت

دیف	سمت سازمانی	فراوانی	درصد
۱	مدیران و معاونین	۲	۱/۵۷
۲	حسابرسان	۱۰۲	۸۰/۳۱
۳	مسئولین و کارشناسان IT	۱۴	۱۱/۰۲
۴	نامشخص	۹	۷/۰۹
جمع		۱۲۷	۱۰۰

جدول شماره(۵):میانگین مولفه های تحقیق به تفکیک استان محل خدمت

ردیف	مولفه	مرکزی	البرز	سمنان	تهران	قزوین	قم
۱	عوامل مدیریتی و خط مشی سازمان	۲/۶۹	۲/۴۸	۲/۴۶	۲/۲۱	۱/۷۶	۲/۵۵
۲	عوامل کاربران و آموزش و فرهنگ امنیتی	۲/۷۰	۳/۳۵	۲/۳۹	۲/۷۰	۲/۲۴	۲/۳۱
۳	عوامل فیزیکی	۲/۹۱	۲/۶۴	۲/۴۴	۳/۱۷	۲/۵۰	۲/۶۱
۴	عوامل زیرساختی فناوری	۱/۹۶	۱/۹۳	۲/۱۸	۲/۶۶	۱/۴۹	۲/۴۶
۵	عوامل امنیتی سیستمهای اطلاعاتی	۳/۱۹	۲/۳۱	۲/۰۴	۲/۴۶	۱/۸۰	۲/۲۱

جدول شماره(۶):میانگین مولفه های تحقیق به تفکیک سمت پاسخ دهندگان

ردیف	مولفه	حسابرسان		سایر کارکنان	
		میانگین	میانه	میانگین	میانه
۱	عوامل مدیریتی و خط مشی سازمان	۲/۳۵	۲/۲۷	۲/۴۲	۲/۴۰
۲	عوامل کاربران و آموزش و فرهنگ امنیتی	۲/۶۰	۲/۵۵	۲/۵۸	۲/۴۵
۳	عوامل فیزیکی	۲/۷۸	۲/۷۵	۲/۸۵	۲/۶۹
۴	عوامل زیرساختی فناوری	۲/۱۹	۲/۲۰	۲/۳۱	۲/۲۰
۵	عوامل امنیتی سیستم های اطلاعاتی	۲/۴۰	۲/۳۸	۲/۵۳	۲/۳۱

جدول شماره(۷):میانگین مولفه های تحقیق به تفکیک سن پاسخ دهندگان

ردیف	مولفه	سی و پنج سال و کمتر		بیش از سی و پنج سال	
		میانگین	میانه	میانگین	میانه
۱	عوامل مدیریتی و خط مشی سازمان	۲/۵۷	۲/۴۷	۲/۶۷	۲/۶۷
۲	عوامل کاربران و آموزش و فرهنگ امنیتی	۲/۵۸	۲/۷۳	۲/۶۶	۲/۵۵
۳	عوامل فیزیکی	۲/۸۰	۲/۷۵	۲/۸۰	۲/۶۳
۴	عوامل زیرساختی فناوری	۲/۲۰	۲/۲۰	۲/۲۴	۲/۲۰
۵	عوامل امنیتی سیستم های اطلاعاتی	۲/۴۹	۲/۵۰	۲/۶۳	۲/۷۵

جدول شماره(۸):میانگین مولفه های تحقیق به تفکیک سابقه کار پاسخ دهندگان

ردیف	مولفه	ده سال و کمتر		بیش از ده سال	
		میانگین	میانه	میانگین	میانه
۱	عوامل مدیریتی و خط مشی سازمان	۲/۶۰	۲/۶۰	۲/۶۵	۲/۵۳
۲	عوامل کاربران و آموزش و فرهنگ امنیتی	۲/۶۹	۲/۷۳	۲/۵۸	۲/۵۵
۳	عوامل فیزیکی	۲/۸۱	۲/۶۹	۲/۷۶	۲/۶۹
۴	عوامل زیرساختی فناوری	۲/۲۲	۲/۲۰	۲/۱۹	۲/۲۰
۵	عوامل امنیتی سیستم های اطلاعاتی	۲/۶۵	۲/۷۵	۲/۵۶	۲/۶۳

۲-۷-تجزیه و تحلیل آماری داده‌ها

در تحقیق حاضر برای تعیین معنی‌داری اختلاف بین میانگین یک متغیر با یک مقدار ثابت از آزمون t یک نمونه‌ای استفاده گردید که با توجه به طیف درنظر گرفته شده در پاسخ‌ها، مقدار آزمون برابر ۳ در نظر گرفته شده است. چنانچه میانگین پاسخ‌ها در هر یک از متغیرها از عدد ۳ بیشتر باشد وضعیت آن در جامعه مساعد خواهد بود در غیر این صورت از نظر جامعه مورد آزمون، متغیر بررسی شده وضعیت مساعدی نداشته و چالشی جهت امنیت فناوری اطلاعات خواهد بود.

در آزمون مورد نظر فرض‌های H_0 و H_1 برای بررسی وضعیت میانگین نظرات جامعه با استفاده از نمونه گرفته شده؛ بصورت زیر بیان می‌شوند.

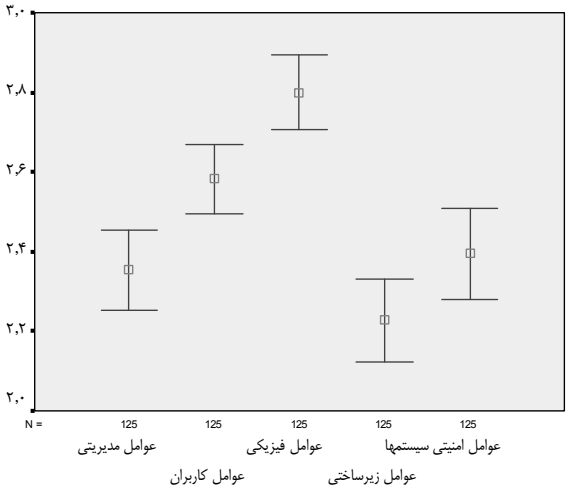
$$\begin{cases} H_0 : \mu_0 \leq \mu_x \\ H_1 : \mu_0 > \mu_x \end{cases}$$

که با توجه به موارد ذکر شده $\mu_0 = ۳$ می‌باشد.

در انجام این آزمون، با توجه به مؤلفه p ـ مقدار (P-Value) ارائه شده تصمیم‌گیری خواهد شد. چنانچه مقدار آن کمتر از سطح آزمون(α) باشد و کرانهای فاصله اطمینان «اختلاف میانگین با مقدار آزمون» مثبت باشد فرض H_0 رد می شود و گرنه دلیلی بر رد فرض H_0 وجود ندارد. سطح آزمون در این بررسی ۰/۰۵ در نظر گرفته شده است.

جدول شماره(۹):بررسی های فرضیه های تحقیق از طریق آزمون t تک نمونه‌ای انجام و نتایج آن به شرح جدول ذیل می باشد. (p<۵٪)

عنوان	آماره t	p- مقدار	اختلاف میانگین و مقدار آزمون	فاصله اطمینان ۹۵٪ اختلاف میانگین و مقدار آزمون		نتیجه آزمون	وضعیت
				کران پایین	کران بالا		
عوامل مدیریتی و خط مشی سازمان	-۱۲/۸۴	۰/۰۰۰	-۰/۶۵	-۰/۷۵	-۰/۵۵	تأیید H_0	وجود چالش
عوامل کاربران و آموزش و فرهنگ امنیتی	-۹/۶۸	۰/۰۰۰	-۰/۴۲	-۰/۵۰	-۰/۳۳	تأیید H_0	وجود چالش
عوامل فیزیکی	-۴/۳۳	۰/۰۰۰	-۰/۲۰	-۰/۳۰	-۰/۱۱	تأیید H_0	وجود چالش
عوامل زیرساختی فناوری	-۱۵/۰۳	۰/۰۰۰	-۰/۷۷	-۰/۸۸	-۰/۶۷	تأیید H_0	وجود چالش
عوامل امنیتی سیستمهای اطلاعاتی	-۱۰/۶۴	۰/۰۰۰	-۰/۶۰	-۰/۷۲	-۰/۴۹	تأیید H_0	وجود چالش



چنانکه در جدول فوق نشان داده شده است، فواصل اطمینان مربوط به میانگین تمامی مؤلفه‌ها، پایین تر از عدد ۳ (متوسط) می‌باشد.کران پایین فاصله اطمینان مربوط به میانگین «عوامل زیرساختی فناوری» پایین‌تر از سایر مؤلفه ها بوده و بالای فاصله اطمینان میانگین «عوامل فیزیکی» بالاتر از مؤلفه‌های دیگر است. نتایج بدست آمده در آزمون های مربوط به تمامی متغیرها بیانگر تأیید فرض صفر و چالشی بودن وضعیت متغیرها در جامعه می‌باشد.

۸- رتبه بندی عوامل امنیتی فناوری اطلاعات

همانطور که میدانیم در آزمون فریدمن که یک آزمون ناپارامتری میباشد، امتیازات در هر سوال را مستقل از دیگر سوالات بخش رتبهبندی میکند و برای مقایسه و رتبه بندی مؤلفه‌های تحقیق و میزان اهمیت هریک از چالش های امنیتی فناوری اطلاعات در دیوان محاسبات کشور از آزمون فریدمن استفاده شده است.

فرض H_0 : میانه تمامی متغیرها برابرند.

فرض H_1 : حداقل دو متغیر وجود دارد که میانه آنها نابرابر است.

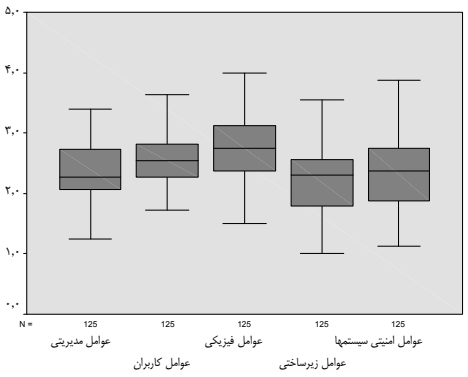
جدول شماره(۱۰):میانگین رتبه مؤلفه‌ها در آزمون فریدمن

ردیف	متغیر	میانگین رتبه
۱	عوامل مدیریتی و خط مشی سازمان	۲/۷۱
۲	عوامل کاربران و آموزش و فرهنگ امنیتی	۳/۳۵
۳	عوامل فیزیکی	۳/۹۲
۴	عوامل زیرساختی فناوری	۲/۲۸
۵	عوامل امنیتی سیستمهای اطلاعاتی	۲/۷۴

جدول شماره(۱۱):نتایج آزمون فریدمن

تعداد	درجه آزادی	مقدار آماره x^2	P- مقدار
125	4	83/36	0/000

. P- مقدار بدست آمده بسیار کوچکتر از سطح خطای ۰/۰۵ = α می‌باشد . پس فرض H۰ رد شده یعنی تفاوت معنی‌داری بین میانه‌های حداقل دو مؤلفه وجود دارد.با توجه به رد فرض صفر مبنی بر برابری میانه تمامی متغیرها، جهت شناسایی اختلاف موجود بین متغیرها از آزمون های ویلکاکسون استفاده می‌کنیم.



جدول شماره(۱۲):نتایج آزمون های تکمیلی ویلکاکسون

ردیف	مؤلفه‌های مورد آزمون		تعداد رتبه‌ها			P – مقدار
	مؤلفه ۱	مؤلفه ۲	بزرگتر	کوچکتر	همرتبه	
۱	عوامل مدیریتی و خط مشی سازمان	عوامل کاربران و آموزش وفرهنگ امنیتی	۳۹	۸۷	۰	۰/۰۰۰۰
۲	عوامل مدیریتی و خط مشی سازمان	عوامل فیزیکی	۳۸	۸۸	۰	۰/۰۰۰۰
۳	عوامل مدیریتی و خط مشی سازمان	عوامل زیرساختی فناوری	۷۵	۴۶	۶	۰/۰۰۹۶
۴	عوامل مدیریتی و خط مشی سازمان	عوامل امنیتی سیستمهای اطلاعاتی	۵۹	۶۵	۳	۰/۳۴۴۶
۵	عوامل کاربران و آموزش و فرهنگ امنیتی	عوامل فیزیکی	۳۷	۸۷	۱	۰/۰۰۰۰
۶	عوامل کاربران و آموزش و فرهنگ امنیتی	عوامل زیرساختی فناوری	۹۰	۳۶	۰	۰/۰۰۰۰

۷	عوامل کاربران و آموزش و فرهنگ امنیتی	عوامل امنیتی سیستمهای اطلاعاتی	۸۲	۴۴	۰	۰/۰۰۱۶
۸	عوامل فیزیکی	عوامل زیرساختی فناوری	۱۰۳	۱۹	۴	۰/۰۰۰۰
۹	عوامل فیزیکی	عوامل امنیتی سیستمهای اطلاعاتی	۸۴	۳۶	۶	۰/۰۰۰۰
۱۰	عوامل زیرساختی فناوری	عوامل امنیتی سیستمهای اطلاعاتی	۵۳	۶۹	۵	۰/۰۰۵۴

چنانکه در جدول فوق نشان داده شده است، فرض برابری میانه‌ها در مورد زوج متغیر: «عوامل مدیریتی و خط مشی سازمان» و «عوامل امنیتی سیستم های اطلاعاتی» در سطح خطای α = ۰/۰۰۵ تأیید می‌شود و می‌توان گفت میانه این زوج متغیرها در جامعه تفاوت معنی داری نداشته و وضعیت آنها در جامعه یکسان است.در سایر مقایسات دو بدو فرض صفر رد شده و با توجه به نتایج آزمون های تکمیلی می‌توان متغیرهای مورد بررسی را بدینصورت رتبه بندی نمود:

جدول شماره(۱۳):رتبه بندی مؤلفه‌های تحقیق

متغیر	رتبه
عوامل فیزیکی	۱
عوامل کاربران و آموزش و فرهنگ امنیتی	۲
عوامل مدیریتی و خط مشی سازمان و عوامل امنیتی سیستم های اطلاعاتی	۳
عوامل زیرساختی فناوری	۴

با توجه به نتایج بدست آمده می توان دید که عوامل فیزیکی بالاترین رتبه را داشته و کمترین چالش را در امنیت فناوری اطلاعات در دیوان محاسبات داراست . عوامل کاربران و آموزش و فرهنگ امنیتی در رتبه دوم قرار داشته و چالش جدی تری است. پس از آن عوامل مدیریتی و خط مشی سازمان و عوامل امنیتی سیستم های اطلاعاتی در رتبه بعد بود و نسبت به دو مولفه قبلی چالش های مهمتری هستند. مهمترین چالش امنیتی فناوری اطلاعات در دیوان محاسبات کشور نیز عوامل زیرساختی فناوری می باشد.

۹- نتیجه گیری

در این پژوهش به شناسایی موانع و چالش های امنیتی فناوری اطلاعات در حسابرسی دیوان محاسبات پرداخته و عوامل شناسایی شده را به ۵ گروه تقسیم نموده بصورت پرسشنامه در معرض نظرسنجی حسابرسان ،مدیران و معاونین و مدیران فناوری اطلاعات جامعه اماری قرار داده شده است.برای تجزیه و تحلیل داده های در نرم افزار spss، از روش های آمار توصیفی و استنباطی استفاده شد.

افراد در نظر گرفته شده در نمونه آماری دارای میانگین سنی ۳۵ سال، میانگین ۱۰ سال تجربه کاری و دارای دانش کافی در زمینه امنیت فناوری اطلاعات بودند.

پس از تجزیه و تحلیل داده ها، مشخص گردید که هر پنج بخش اصلی این پژوهش که مورد آزمون قرار گرفتند، چالشهای امنیت فناوری اطلاعات در حسابرسی دیوان محاسبات کشور به شمار می روند ، نکته قابل تامل یکسان نبودن عوامل مورد پژوهش است که بیانگر وجود تفاوت در اهمیت هر یک از این عوامل نزد پاسخگویان است.و در نهایت ۵ عامل رتبه بندی گردید و مشخص شد از لحاظ میزان چالش نسبت به یکدیگر در چه رتبه ای قرار دارند.که عوامل زیرساختی بیشترین چالش و عوامل فیزیکی کمترین چالش را دارا می باشند.

۱۰- محدودیت های پژوهش

هر محققی در انجام پژوهش های خود با محدودیت های خاصی مواجه است که برحسب موضوع پژوهش، روش پژوهش، جامعه آماری آن و ابزار گردآوری داده ها این محدودیت ها می توانند در پژوهش های مختلف متفاوت باشند. بنابراین پژوهش حاضر نیز از محدودیت های فوق الذکر مصون نبوده است. محدودیت هایی که در این پژوهش وجود داشته عبارت است از:

- عمده ترین محدودیت پژوهش هایی که ابزار گردآوری داده های آن ها پرسشنامه می باشد علی رغم اینکه از پاسخ دهندگان خواسته می شود تا نظرات واقعی خود را ارائه نمایند. لیکن در برخی موارد ممکن است پاسخ دهندگان نظرات غیر واقعی ارائه نمایند.
- با عنایت به آنکه جامعه اولیه تحقیق ، تمامی سازمانهای دیوان محاسبات در کل استانهای کشور بوده لیکن به سبب عدم امکان بررسی تمامی استانها تنها ۶ استان به عنوان نماد کار موضوع پژوهش انتخاب گردید .

۱۱- پیشنهادهای پژوهش

با توجه به یافته های سایر پژوهشها و نتایج پژوهش حاضر و همچنین بنابر اطلاعات حاصل از مصاحبه با افراد حرفه ای در این حوزه به اهمیت امنیت فناوری اطلاعات پیشنهاداتی جهت ارتقاء حفظ امنیت اطلاعات ارائه می گردد.

الف)مسائل امنیتی در مدیریت و خط مشی سازمان

در پاسخ به سوال اول که آیا عوامل مدیریتی و خط مشی سازمان چالشی جهت امنیت فناوری اطلاعات می باشد، آزمون آماری اثبات کرد با توجه به مقدار میانگین که کمتر از مقدار آزمون بوده ، این عامل دارای بحران و چالش می باشد که در آن شاخصهای چون توجه مدیران ارشد به مباحث امنیتی ،تشکیل جلسات شورای راهبری،تدوین برنامه جامع برای پیاده سازی مسائل امنیتی ،وجود استراتژی پیاده سازی امنیت و ارزیابی ارزش اطلاعات ،استفاده از مشاوران طرح سیستم مدیریت امنیت اطلاعات و تخصیص بودجه لازم مورد پرسش قرار گرفته است.لذا پیشنهادات ذیل جهت کاهش این چالش مطرح می گردد:

۱) اتخاذ سیاستهای امنیتی مناسب و اجرای صحیح آنها خطر از دست دادن ناگهانی اطلاعات را کاهش میدهد، ورود غیرمجاز به سیستم را بسیار مشکلتر میکند و ابزار امنیتی برای شناسایی حملات و اصلاح رخنه های امنیتی را فراهم میسازد. برای حفظ اطلاعات محرمانه و کمک به یکپارچگی برنامه ها و اطلاعات ذخیره شده باید تلفیقی از سیاستگذاری ها و پیاده سازی آن انجام شود.

۲) مدیران برای نیل به اهداف تعیین شده باید بر سیاستهای امنیت اطلاعات توجه موکد داشته باشند. همچنین درک هزینه های پیاده سازی سیاست های امنیتی کارآ از اهمیت زیادی برخوردار است. فناوری ها روالهای امنیتی نوعی سرمایه گذاری به حساب می آیند و باید با توجه به هزینه های ضایعات محتمل،مورد ارزیابی قرار گیرند.

۳) نه تنها حمایت امنیت اطلاعات ،بلکه حمایت از پدیده آوران و گسترش دهندگان سیستم مدیریت امنیت اطلاعات امری مهم است زیرا وجود این متخصصین باعث ایجاد و پیشرفت مدیریت امنیت اطلاعات می شود.

ب)مسائل امنیتی کاربران، آموزش،فرهنگسازی امنیتی

در پاسخ به سوال دوم که آیا عوامل کاربران و آموزش و فرهنگ امنیتی چالشی جهت امنیت فناوری اطلاعات می باشد، آزمون آماری اثبات کرد با توجه به مقدار میانگین که کمتر از مقدار آزمون بوده ، این عامل دارای بحران و چالش می باشد در این عامل شاخصهای چون آموزش پرسنل ،اطلاع رسانی مباحث امنیتی به پرسنل،سطح دسترسی افراد ،اتکا به مستندات الکترونیکی ،تخریب اطلاعات توسط کاربران ،فرهنگسازی سطوح مختلف سازمان ،افشا اطلاعات ، پیچیدگی در رمز گذاری مورد پرسش قرار گرفته است.برطبق آزمون آماری این عامل در رتبه دوم نسبت به عوامل دیگر دارای چالش می باشد و نشانگر آن است که عدم آگاهی کاربران برای سازمانها ایجاد چالش بیشتری می نماید و نقش موثرتری در امنیت اطلاعات دارند لذا پیشنهاد

می گردد :

۴) سازمان ها باید در اقدامی نوآورانه با ترکیبی از عملیات امنیتی فناوری اطلاعات و شخص تلاش کنند تا در جریان فعالیتهای کارکنان خود قرار گیرند.

۵) ایجاد دوره های آموزش برای مدیران و کارکنان،

۶) ایجاد آموزش کافی در زمینه فناوری نوین اطلاعات برای متخصصین و مدیران فناوری اطلاعات

ج)مسائل امنیتی فیزیکی

در پاسخ به سوال سوم که آیا عوامل فیزیکی چالشی جهت امنیت فناوری اطلاعات می باشد، آزمون آماری اثبات کرد با توجه به مقدار میانگین که کمتر از مقدار آزمون بوده ، این عامل دارای بحران و چالش می باشد پرسشهای این عامل شاخصهای چون پیاده سازی استانداردهای مکانی حفاظت از اطلاعات ،کنترل تردد افراد بصورت الکترونیکی به مکان حفاظت اطلاعات،کنترل ورود سیستمهای الکترونیکی جهت سرقت اطلاعات،امنیت فیزیکی سیستمهای کامپیوتری می باشد.بر طبق آزمون ویلکاکسون عوامل فیزیکی بالاترین رتبه را در چالشهای امنیتی دارا می باشد و این مطلب حاکی از آن است که پیاده سازی استانداردها در خصوص مکان فیزیکی و محیط نگهداری اطلاعات توجه کمی به آن شده است و از ضعف بیشتری برخوردار است.می توان این موارد را جهت کاهش آن پیشنهاد نمود:

۷) پیاده سازی استانداردهای امنیتی مکان نگهداری اطلاعات

۸) ایجاد فضای مناسب برای نگهداری اطلاعات

۹) کنترل و تعیین سطح دستری افراد به این مکان و کنترل تردد افراد بوسیله سیستم های الکترونیکی

۱۰) خرید محصولات امنیتی مانند فایروال و برنامه های ضدویروس، و به کارگیری آنها در سیستمهای کامپیوتری سازمان ها و استفاده از روالهای استاندارد در به کارگیری و کنترل سیستمهای امنیتی و به روزسانی مداوم این سیستم ها

۱۱)طراحی محیط فیزیکی محل نگهداری اطلاعات منطبق با استانداردهای مرکز اطلاعات

د)مسائل زیر ساختهای امنیتی

در پاسخ به سوال چهارم که آیا عوامل زیر ساختی فناوری اطلاعات چالشی جهت امنیت فناوری اطلاعات می باشد، آزمون آماری اثبات کرد با توجه به مقدار میانگین که کمتر از مقدار آزمون بوده ، این عامل دارای بحران و چالش می باشد پرسش این عامل شاخصهای چون ساختار شبکه داخلی سازمان،سیستم پشتیبان گیری از اطلاعات ،امنیت زیرساختی شبکه داخلی جهت تبادل اطلاعات در حسابرسی ،امنیت شبکه دولت،امنیت در مقابل نفوذگرها اشاره گردیده است.طبق نتیجه آزمون آماری این عامل از درجه رتبه کمتری برخوردار است بعبارت دیگر نسبت به عوامل دیگر چالش کمتری دارا می باشد و سازمان در مقابل این عامل از وضعیت بهتری نسبت به سایر عوامل برخوردار است.

۱۲)ایجاد شبکه های ملی امن با پهنای باند مناسب،جهت تبادل اطلاعات بین سازمان دیوان محاسبات و سایر

۱۳)برای محافظت از اطلاعات سازمان- نسخه های پشتیبان تهیه نمایید..چنانچه فایل اصلی به هر دلیلی از بین برود یا پاک شود میتوان از نسخه پشتیبان استفاده کرد. مهمترین نکته در مورد نسخه های پشتیبان این است که تهیه پشتیبان باید در فواصل زمانی منظم صورت بگیرد.

۱۴)سازمانها باید ارتباط میان بخش خصوصی و بخش عمومی را افزایش داده و از تخصص بخش خصوصی در حفظ امنیت اطلاعات بهره گیرد.

ه)مسائل امنیتی سیستمهای اطلاعاتی

در پاسخ به سوال پنجم که آیا عوامل امنیتی سیستمهای اطلاعاتی چالشی جهت امنیت فناوری اطلاعات می باشد، آزمون آماری اثبات کرد با توجه به مقدار میانگین که کمتر از مقدار آزمون بوده ، این عامل دارای بحران و چالش می باشد در پرسش این عامل به شاخصهای چون ثبت اطلاعات محرمانه،دسترسی افراد به سیستمهای اطلاعاتی ،استاندار سازی سیستم اطلاعاتی،هویت افراد بهره بردار از سیستمهای اطلاعاتی ،امنیت تبادل اطلاعات در سیستمهای اطلاعاتی اشاره گردیده است. طبق نظر آزمون ویلکاکسون رتبه این عامل همتراز عوامل مدیریتی و خط مشی سازمان می باشد و در رتبه سوم قرار دارد و چالش آن از عوامل فیزیکی و کاربران و فرهنگ سازی در این سازمان کمتر می باشد.

۱۵) ایجاد مرکز امداد برای حملات،

۱۶)سند امنیت فضای تبادل اطلاعات دیوان محاسبات کشور به مفهوم مرکز اشتراک و تبادل اطلاعات مالی سازمانهای دولتی

۱۷) خرید محصولات امنیتی مانند فایروال و برنامه های ضدویروس، و به کارگیری آنها در سیستمهای کامپیوتری سازمان ها و استفاده از روالهای استاندارد در به کارگیری و کنترل سیستمهای امنیتی و به روزسانی مداوم این سیستمها

۱۸)طراحی محیط فیزیکی محل نگهداری اطلاعات منطبق با استانداردهای مرکز اطلاعات

۱۲- پیشنهاداتی برای پژوهش آینده

به نظر محقق دامنه پژوهش در زمینه امنیت فناوری اطلاعات بسیار گسترده بوده و پژوهش در ابعاد گوناگون می تواند انجام گیرد پیشنهاداتی برای انجام پژوهش آتی ارائه می گردد:

- انجام پژوهش در سایر سازمانها دیوان محاسبات کشور در استانهای دیگر
- تحلیل تاثیر آموزش عالی امنیت اطلاعات بر روی عملکرد کارکنان و متخصصان سازمان
- تحلیل نقش فرهنگ سازی در پیاده سازی امنیت اطلاعات در سازمان
- تحلیل نقش امنیت اطلاعات در عملکرد سازمان
- تحلیل چگونگی پیاده سازی امنیت فناوری اطلاعات با توجه به چالش های موجود در سازمان

- تحلیل عوامل موثر دیگر بر امنیت اطلاعات در سازمان
- تحلیل نقش قانون اساسی دولت در تحقق سیستم مدیریت امنیت اطلاعات در سازمان

۱۳- منابع

۱) اسدی، مریم،(۱۳۸۴) ،"فناوری های امنیت اطلاعات: با یک دیدگاه طبقه بندی"، مجله علوم اطلاع رسانی، دوره ۲۰ ، شماره ۳و۴ ص ۱-۱۶

۲)امیرخانی،علی،(۱۳۸۸)،"ارائه مدلی از عوامل موثر در اثربخشی سیستم مدیریت امنیت اطلاعات در سازمانهای دولتی"،پایان نامه کارشناسی ارشد: دانشگاه مدیریت تهران

۳)ترک لادانی، شیخ زینالدین ،موزرانی ، میرعلایی،(۱۳۸۶)،"تاملی بر چالشهای استقرار *Isms* در سازمانهای دولتی ایران" ،مجله تکفا،سال پنجم،شماره ۷و۸

۴)حسن آقای، کامران ،(۱۳۸۳)، "بررسی تاثیر فناوری اطلاعات بر ویژگی کیفی اطلاعات حسابداری"، پایان نامه کارشناسی ارشد حسابداری :دانشگاه تربیت مدرس

۵)خالقی،محمود،(۱۳۸۶)،" راهنمای پیاده سازی سیستم مدیریت امنیت اطلاعات استاندارد "BS۷۷۹۹،تهران، انتشارات شورای عالی فضای امنیت تبادل اطلاعات کشور

۶)رضایی،امیرحامد،(۱۳۸۷)،" نقش فرهنگ سازمانی در مدیریت امنیت اطلاعات"،مجله عصرفناوری اطلاعات،شماره۳۶،ص ۵۶-۵۷

۷)سلیمان فلاح، مهران ،(۱۳۸۱)، "توصیف شکلی قابلیت دسترسی و از کار اندازی سرویس در شبکه های کامپیوتری"، پایان نامه کارشناس ارشد کامپیوتر: دانشگاه تربیت مدرس

۸)سعیدی،علی، و افسانه سروش نیا،(۱۳۸۸)،مجله حسابرس، سال یازدهم، شماره ۴۴و۴۵، ص ۴۵

۹)شعبان،الهی،طاهری،مهدی،حسن زاده،علیرضا،(۱۳۸۸)،ارائه چارچوبی برای عوامل انسانی مرتبط در امنیت سیستم های اطلاعاتی،فصلنامه مدرس علوم انسانی،دوره ۱۳،شماره ۶۱،ص ۱

۱۰) صالح هادی نیا ،(۱۳۸۸)، شناسایی موانع اجرایی شدن حسابرسی الکترونیکی در دیوان محاسبات کشور،پایان نامه کارشناسی ارشد حسابداری: دانشگاه آزاد ارومیه

۱۱)عرب مازار یزدی،محمدی ،نازنین،(۱۳۸۵)، تهدیدات امنیتی در سیستم های اطلاعاتی حسابداری رایانه ای ،ماهنامه حسابدار ،سال ۲۱ ،شماره ۱۷۹،ص ۲۲

۱۲)عبداللهی ازگمی، محمد ،(۱۳۷۵)،طراحی و پیاده‌سازی سرویس‌های امن برای شبکه‌های کامپیوتری،پایان نامه کارشناس ارشد کامپیوتر: دانشگاه صنعت شریف

۱۳)فارس،(۱۳۸۷)،گامهای پیاده سازی سیستم امنیت اطلاعات ،مجله پردازشگر، سال هفتم ،شماره ۶۰۰ ، ص۷۴-۷۵

۱۴) هاتف،مهدی،(۱۳۸۸)،چالشها و چشم اندازهای امنیت در فضای مجازی ، ماهنامه توسعه انسانی پلیسی شماره ۲۲،ص ۹۳

1- Alvaro A.Dardenas,saurabh amin,Shankar Sastry,(2008), Research Challenges for Security of Contol Systems,

2- Andrew P.Moore,Robert J.Ellison,Richard C.linger,(2001), Attack Modeling for information Security and Survivability,Software Engineering institute,no 001,pp1-20

3- George Sadowsky; James X. Dempsey; Alan Greenberg; Barbara J. Mack;Alan Schwartz,(2003), *IT Security Handbook*, infoDev, Worldbank.
4- Haralambos Mouratidis ,Paolo Giorgini,Gordon Manson,(2003), Integrating Security and Systems Engineering: Towards the Modelling of Secure Information Systems. In:Eder, J. Missikoff, M. (Eds) CAiSE 2003, LNCS 2681, pp 63-78
5- Louis R.Chao,Jil-Hsing Tang,Yen-ping Chi,Kwo-shing Hong,(2003), An integrated system thory of information security management,information management & computer security ,no 11-5,pp 243-248
6- Mark Wilson, Joan Hash, (2005),NIST Special publication: Building an information technology security awareness and training program".
7- Stephen Smith,Rodger Hamieson,(2006), Determining Key Factors In E-overment information system security,Journal,spring2006,pp 23-32.
8- WaMandol, Puja and Monica verma, (2004), On Line Auditing, II International Seminar on IT Audit, Nanjing, china.
9-Wang Zhiyu,(2009) ,Security Solution Used In On Line Auditing In China, Intoit NO28