نیرنگهای کامپیوتری

ترجمه و تلخیص:

عباسعلی طوسیان شاندیز

گسترش تکنولوژیهای کامپیوتری موجب بروز شگفتی در جوامع بشری شده و روزبروز بر میزان وابستگی جوامع به امواج بزرگ و کوچک کامپیوتری، این انقلاب صنعتی جدید، که توسط "آلوین تافلر" موج سوم نامیده شده، افزوده می‌شود. یکی از شگفتیهای مهم جوامع بشری، نیرنگهای کامپیوتری می‌باشد. براساس تحقیقات "پارکر"[1] تخصص در امنیت کامپیوتری، دومورد در دهه ۱۹۵۰، ۶۳ مورد در دهه ۱۹۶۰، ۵۶۹ مورد طی سالهای ۷۸–۱۹۷۰، کلاهبرداری کامپیوتری کشف گردید که دارای نرخ افزایش گیج‌کننده‌ای معادل ۱۹۰۰ درصد در هر دهه از ۷۰–۱۹۵۰ بوده است.

براساس نتایج تحقیقات Brandt Allen، متوسط خسارات ۱۵۰ فقره کلاهبرداری کامپیوتری مبلغی معادل ۱/۳ میلیون دلار در ازای هر کلاهبرداری بوده است. طی سالهای اخیر زیانهای ناشی از کلاهبرداریهای کامپیوتری خیره‌کننده می‌باشد. بعنوان مثال در سال ۱۹۷۳ Equity Funding ۲۷/۲۵ میلیون دلار، در سال ۱۹۷۸ Security Pacific ۱۰/۳ میلیون دلار و در سال ۱۹۷۹، Wells Fargo مبلغی معادل ۲۱/۳ میلیون دلار کلاهبرداری نموده‌اند. اقدامات حسابرسان مستقل می‌تواند میزان این کلاهبرداریها را کاهش دهد.

اهداف این مقاله عبارتند از:

۱– مرور جنبه‌های تاریخی مسئولیت حسابرسان در افشای نیرنگها.

۲– شناسایی مبداء کلاهبرداریهای کامپیوتری.

۳– شناسایی روشهای جلوگیری از کلاهبرداریهای کامپیوتری.

1- Parker

مسئولیت حسابرسان در افشای نیرنگها

نیرنگ بمعنی انجام عملی جهت منحرف نمودن حقیقت، انعکاس غیرواقعی رویدادها یا هر روش دیگر بمنظور اغفال افراد موردنظر می‌باشد. نیرنگ می‌تواند یک جرم، یک جنایت، یا فعالیتهایی مانند سرقت، جعل اسناد یا امضاء، اختلاس و بزهکاری باشد.

تاکنون اصطلاح مشخصی جهت تشریح نیرنگهای کامپیوتری بکار گرفته نشده است اما از اصطلاحات مختلفی مانند: کلاهبرداری کامپیوتری[۲]، سوءاستفاده کامپیوتری[۳]، جنایت کامپیوتری[۴]، اختلاس کامپیوتری[۵]، سرقت کامپیوتری[۶] و حماقت کامپیوتری[۷] در مقالات و مطالب مربوط به کامپیوتر و حسابداری استفاده شده است.

از آنجایی که اصطلاح "کلاهبرداری" دارای اشاره ضمنی وسیعتری ازلحاظ قانونی است، در این‌مبحث کلاهبرداری کامپیوتری را مورد استفاده قرار می‌دهیم.

کلمه کامپیوتر بعنوان یک صفت در اصطلاح کامپیوتری مورد استعمال قرارگرفته است. "پارکر" کلاهبرداری را در ۴ نوع زیر طبقه‌بندی نموده است:

۱) کامپیوتر هدف کلاهبرداری است.

۲) کامپیوتر ایجادکننده محیطی غیرعادی است که در آن کلاهبرداری انجام می‌شود.

۳) کامپیوتر وسیله انجام کلاهبرداری است.

۴) کامپیوتر بعنوان سمبل تحریف و فریب است.

نوع اول مربوط به دشمنان علم و صنعت[۸] می‌باشد، نوع دوم بوسیله سارقین اطلاعات یا برنامه‌ها انجام می‌گیرد. نوع سوم مربوط به مسائل صرفا "مالی یا سرقت با استفاده از کامپیوتر بعنوان وسیله می‌باشد و آخرین آنها اختصاصا" مربوط به استفاده از کامپیوتر جهت تحریف یا فریب است(صورتحسابهای جعلی یا بیمه‌نامه‌های صوری از این‌جمله هستند). بنابراین ممکن است نقش کامپیوتر در کلاهبرداری را بصورت زیر تعریف کنیم:

2-Computer fraud
3-Computer abuse
4-Computer crime
5-Computer embezzlement
6-Computer theft
7-Computer capes
8-Vandialism

۱) بصورت یک هدف[9]
۲) بصورت یک محیط[10]
۳) بعنوان یک وسیله[11]
۴) بعنوان یک سمبل[12]

جنبه‌های تاریخی وظایف حسابرسان در افشای کلاهبرداریها

علت اصلی حسابرسی از بابل قدیم در قرون وسطی تا انقلاب صنعتی قرن نوزدهم، کشف کلاهبرداری بوده است. قبل از انقلاب صنعتی حسابرسی شامل استنطاق آشکار از مسئولان دولتی بوسیله نمایندگان مردم بود که به شکل زیر به دوره انقلاب صنعتی در انگلیس منتقل گردید:

با افول ورشکستگیها و بحرانهایی که در سالهای ۱۸۴۴، ۱۸۵۵ و ۱۸۶۲ برای شرکتهای فعال بوجود آمده بود، مسئولیتهای حسابداری و حسابرسی مشخصی مستقیما" توسط قوانین اعمال گردید که یکی از آنها محافظت از موجودی درمقابل کلاهبردار است، حال آنکه مسئولیت دیگر، کنترل مستقیم وظایف فیزیکی مدیران و روءسا بوده که عمدتا" موجب به‌حداقل رساندن کلاهبرداریها گردیده بود.

در سه‌دهه اول قرن، متخصصین حسابرسی در آمریکا، اصولی را که در بریتانیا وجود داشت، قبول و تصویب نمودند، لذا عرفا" وظایف حسابرسان در این‌دوره کشف کلاهبرداریها بود. طی بحران بزرگ ۱۹۳۰، حسابداری تاکید زیادی‌روی مفهوم "بررسی داخلی"[13] می‌نمود که بسرعت به "کنترلهای داخلی"[14] تغییر پیدا کرد و کشف و ردیابی کلاهبرداریها بصورت یک وظیفه اصلی درآمد. فلسفه وجودی حسابرسی این بود که حسابرسان مستقل بایستی کنترلهای داخلی مشتری را جهت تعیین روشهای حسابرسی ارزیابی نموده و درمورد صحت ارائه صورتهای مالی مشتری اظهارنظر نمایند. فلسفه وجودی اینگونه حسابرسی می‌تواند "ضامن اسناد"[15] سال ۱۹۳۳ باشد که در یک گزارش ویژه توسط" انجمن حسابداران امریکا"[16] (بنیانگزاران AICPA ــ انجمن حسابداران

9-Object
10-Environment
11-Instrument
12-Symbol
13-Internal check
14-Internal control
15-Securities Act
16-American Institute of Accontant

خبره امریکا[17]) در سال ۱۹۴۹ کنترلهای داخلی نامیده شد.

استفاده از روشهای کنترلهای داخلی مناسب امکان ارائه صورتهای مالی صحیح را افزایش می‌دهد بنابراین به منظورارائه اظهارنظر درمورد صحت صورتهای مالی مشتری، حسابرس باید سیستم کنترلهای داخلی مشتری را مطالعه و ارزیابی نماید. این باور وجود دارد که کنترلهای داخلی مناسب می‌تواند امکان کلاهبرداریها را کاهش دهد اما هیچ تعهدی درمورد ریشه‌کن کردن آن وجود ندارد. از سال ۱۹۵۰ که انجمن حسابداران خبره امریکا باتوجه به مسئولیت حسابرسان در برنامه‌ریزی حسابرسی بمنظور کشف کلاهبرداریها از آنها حمایت کرد، نظر خود را درمورد مسئولیت حسابرسان، در استانداردهای ۱۶ حسابرسی (SAS-16)[18] بیان کرده است:

هدف حسابرسان مستقل از بررسی صورتهای مالی، کنترل درانطباق بودنشان با اصول استانداردهای پذیرفته‌شده حسابرسی و اظهارنظر نسبت به منطبق بودن صورتهای مالی بر اصول پذیرفته‌شده حسابداری و رعایت ثبات رویه می‌باشد. نتیجتا" تحت استانداردهای پذیرفته‌شده حسابرسی، حسابرسان مستقل مسئولیت دارند که درقلمرو روشهای حسابرسی خود ..... بمنظور تهیه برنامه حسابرسی ..... جهت کشف اشتباهات ویا سوءجریاناتی که اثرات عمده‌ای روی صورتهای مالی دارند و بمنظور بکارگیری مهارت لازم جهت هدایت این بررسیها، برنامه‌ریزی کنند. بررسی اشتباهات یا سوءجریانات عمده معمولا" ازطریق روشهای حسابرسی جهت ارائه اظهارنظر مناسبی درمورد صورتهای مالی انجام می‌گیرد. توجه داشته باشید که استانداردهای حسابرسی ۱۶، نمی‌گوید که ارائه صحیح صورتهای مالی به‌معنی عاری از تقلب بودن آن است، بلکه استانداردهای مزبور حسابرسان مستقل را مسئول بررسی و کشف اشتباهات و سوءجریانات درحین رعایت محدودیت‌های ذاتی عملیات حسابرسی می‌داند و به این‌معناست که نمونه‌گیریهای حسابرسان براساس روش انتخابی اطلاعات بوده و شامل ریسک زیادی نیز می‌باشد. لذا ممکن است اشتباهات یا سوءجریاناتی وجود داشته باشد ولی کشف نگردد. همانطور که قبلا" اشاره شد، باور یا فرض عموم بر این است که حسابرسی، بمنظور دستگیری سارقین انجام می‌گیرد ولی وضعیتی که توسط حسابرسان مستقل تایید می‌شود با آنچه که در باور عموم است تفاوت دارد.

17-American Institute of Certified Public Accountant

18-Statement or Auditing Standards

در این‌باره انجمن "حسابرسان داخلی امریکا" (IIA)[19] نیز مانند انجمن حسابداران خبره امریکا وضعیتهای زیادی را درنظر گرفته است، در این استاندارد بمنظور اعمال حرفه‌ای حسابرسان داخلی اظهار می‌دارد که :

در رعایت دقت حرفه‌ای، حسابرسان داخلی باید مراقب احتمال وقوع اشتباهات عمدی و غیرعمد، حذف، عدم کارآیی و تضاد منافع باشند، همچنین باید مراقب شرایط و فعالیتهایی باشند که احتمال وقوع سوءاستفاده‌های بیشتری در آنها وجود دارد. حسابرسان داخلی نمی‌توانند کاملا" مطمئن باشند که کار غیراصولی یا سوءجریان وجود ندارد. خلاصه اینکه متخصصین حسابداری نباید ادعا کنند که کشف کلاهبرداریها هدف اصلی حسابرسی است. انجمن حسابداران خبره امریکا و انجمن حسابرسان داخلی امریکا رسما" اعلام کرده‌اند که حسابرسان باید مراقب وجود کلاهبرداریها درحین بررسیهایشان باشند، اما این اطمینان وجود ندارد که اگر کلاهبرداریهایی به‌وقوع پیوست، حتما" کشف خواهد شد. در این‌باره سازمان "حسابداری عمومی امریکا ـ دیوان محاسبات ـ GAO "[20]، با انتشار مجموعه وظایف خاص، بصورت یک قانون، تااندازه‌ای از انجام کلاهبرداریهای مستقیم در موءسسات دولتی فدرال جلوگیری نمود.

روش شناسایی کلاهبرداریهای کامپیوتری

چگونه کامپیوتر جهت ارتکاب به کلاهبرداری مورداستفاده قرار می‌گیرد؟ اصول این‌عمل به ۴ صورت انجام می‌شود : ۱) دستکاری ورودیها ، ۲) دستکاری فایلها ، ۳) دستکاری برنامه‌ها ، ۴) دستکاری عملیات. براساس تحقیقات "آلن" ، تعدادی موارد کلاهبرداری را می‌توان بصورت زیر دسته‌بندی نمود (توجه داشته باشید که چند مورد در بیش از یک طبقه تقسیم‌بندی شده‌اند) :

دستکاری ورودیها (معاملات)	**۱۰۹ مورد**
دستکاری فایلها	**۱۳ مورد**
دستکاری برنامه‌ها	**۱۴ مورد**
دستکاری عملیات	**۵ مورد**
متفرقه	**۱۷**
جمع	**۱۵۸ مورد**

19-Institute of Internal of Auditors
20-General Accounting office

دستکاری ورودیها برجسته‌ترین روشی است که معمولا" جهت انجام کلاهبرداری مورد استفاده قرار می‌گیرد و در بررسیهای "آلن" حدود ۱۷۰ را شامل شده است . ورودیها یا معاملات بایستی به یکی از سه‌طریق زیر دستکاری شوند : ۱ـ اضافه کردن معاملات موهوم ، ۲ـ تغییر معاملات ، و ۳ـ حذف معاملات . اضافه کردن معاملات غیرمجاز ، مثل سیاست بیمه‌ای غلط (ساختگی) در شرکتهای بیمه‌ای و پس‌انداز ساختگی در چند بانک می‌باشد که سه روش فوق بیشتر مورداستفاده قرار می‌گیرد . تغییر معاملات معمولا" شامل انتقال معاملات به حسابهای غیرصحیح می‌باشد . به‌عنوان مثال شماره حساب پس‌انداز مشتری تغییر داده می‌شود تا وجوه پس از واریز به حساب مشخصی جهت دستبرد انتقال یابد . حذف معاملات بدین‌صورت است که به کامپیوتر دستور داده می‌شود تا معاملات معینی را از پردازش حذف کند . به‌عنوان مثال در یک‌مورد موجودی کالایی از فایل موجودیها حذف می‌شود تا کالا از انبار خارج شود .

دستکاری فایل‌ها مربوط به دستکاری مستقیم فایلهای اصلی در زمان تعمیر و نگهداری برنامه ، و دستکاری مستقیم ترمینال ورودی همزمان با تعمیر و نگهداری فایل می‌باشد ، که جهت کلاهبرداری صورت می‌گیرد . یک‌مثال از این‌نوع مربوط به تحلیلگر برنامه‌ریز سیستمی بود که درست قبل از تهیه صورتحساب ، قیمتهای کالاهای خریداری را در فایل اصلی تغییر داده و پس از اخذ صورتحساب ، قیمتها را در فایل اصلی تصحیح می‌نمود .

علاوه بر اینها براساس تحقیقات فوق ، تقلبات کامپیوتری درنتیجه دستکاری برنامه‌ها تقریبا" به‌وسعت دستکاری در فایلها بود. دستکاری در برنامه‌ها به‌معنی تغییرات غیرمجاز برنامه جهت کلاهبرداری است . به‌عنوان مثال در یک‌مورد یک برنامه‌نویس حقوق و دستمزد برنامه را بصورتی تغییر داده بود که سنتهای خرده در محاسبه کسور مالیاتی برای هر کارگر به حساب کسور مالیاتی برنامه‌نویس منتقل می‌شد که درنتیجه مالیات متعلقه به برنامه‌نویس از این‌طریق تامین می‌شده است . . . در موردی دیگر برنامه‌نویس یک موسسه ، برنامه پس‌انداز و وام را بصورتی تغییر داده بود که سنتهای خورده در محاسبه بهره به حساب خودش منتقل و پس‌انداز می‌شد .

کلاهبرداری ازطریق عملیات غیرمتعارف کامپیوتری تقریبا" همیشه محدود به پرداختهای نقدی می‌باشد که در آن کامپیوتر بصورت غیرمجاز جهت پرداختهای اضافی بکار گرفته می‌شود . در یک‌مورد ، مدیر مرکز پردازش اطلاعات یک مرکز بورس اوراق بهادار بسادگی ازطریق داد ن یک برنامه مشابه موجب صدور چکی بنام شخصی موهوم شده و سپس ترتیب پرداخت آن را می‌دهد . بعضی از کلاهبرداریهای کامپیوتری ازطریق دستکاری

ورودیها، فایلها، ویا استفاده از عملیات، انجام نمی‌گیرد. مثالهایی از این‌نوع: خرابکاری، استراق سمع، یا جاسوسی صنعت، جهت سود بردن در رقابتها می‌باشد و سرقت و فروش اطلاعات، برنامه‌ها و زمان کامپیوتر جهت سود شخصی نیز جزء کلاهبرداریها محسوب می‌گردد. از میان این‌گونه کلاهبرداریهای متفرقه که بدلیل استفاده از ترمینالها و کامپیوترهای خانگی همه‌جا گسترش یافته و نیز بعلت استفاده بانکهای کشورها از سیستم انتقال الکترونیکی وجوه، استراق سمع بیشتر جلب توجه می‌نماید. بدترین قسمت در استراق سمع این است که هیچ شرکت بیمه‌ای اقدام به بیمه برنامه‌های کامپیوتری درقبال اینگونه کلاهبرداری نمی‌نماید.

چگونگی مبادرت به کلاهبرداری:

از مطالعه جداول الف و ب چنین بنظر می‌رسد، شخصی که به سیستمهای کامپیوتری دسترسی داشته باشد حتی یک بیگانه با سازمان، می‌تواند مرتکب کلاهبرداری کامپیوتری شود. طبق جداول فوق، افرادی که قادر به کلاهبرداری هستند عبارتند از: اول: مسئول اطلاعات ورودی ترمینال، برنامه‌نویس، منشی، و مدیر دفتر کامپیوتر که هرروزه مستقیما" به سیستم کامپیوتری دسترسی دارند. این افراد نسبت به سایرین بیشتر مرتکب کلاهبرداری شده‌اند. دوم: اضافه کردن معاملات موهوم بیشتر تکرار شده. سوم: حتی افراد خارج از سیستم نیز می‌توانند مرتکب کلاهبرداریهای کامپیوتری شوند زیرا آنها با استفاده از کامپیوترهای خانگی یا ترمینالهای خارجی می‌توانند به سیستم نفوذ نمایند. چهارم: بیشتر کلاهبرداریهای کامپیوتری بوسیله یک شخص انجام می‌گیرد. این شاید دلیلی باشد بر اینکه چرا اکثر کلاهبرداریهای کامپیوتری بصورت اتفاقی کشف می‌شوند. پنجم: پایین‌ترین وضعیت ارتکاب بالاترین احتمال تبانی را داراست و بالعکس. ششم: اگر مرتکب به‌تنهایی اقدام به تقلب کند معمولا" دزد بزرگی خواهد بود ــ مدیر یا متصدیان شرکتهای بزرگ ــ که بطور متوسط در ۱۸ مورد از بررسیها، هر مورد ۲۷۴۰۰۰ کلاهبرداری نموده‌اند. درنهایت در تجزیه و تحلیل کلی، کلاهبرداریهای خارج از موسسه بالاترین زیان مالی را در سه مورد از بررسیها به میزان ۲/۴ میلیون دلار (بطور متوسط) وارد کرده‌اند. در این‌میان خارجیانی که مسئول اطلاعات ورودی / ترمینال بوده‌اند بطور متوسط در هرمورد از ۱۵ مورد حدود ۷۲۷ هزار دلار اختلاس نموده‌اند. علاوه بر آن گروه دیگری از مرتکبین، اپراتورهای کامپیوتر بوده‌اند که بطور متوسط در هرمورد ۶۹۶ هزار دلار کلاهبرداری نموده‌اند، یعنی تقریبا" به اندازه مسئولان اطلاعات ورودی /

ترمینال .

جدول الف چگونگی مبادرت مرتکبین ــ روشهای دستکاری

موقعیت شغلی	اضافه‌کردن معامله	تغییر معامله	حذف معامله	تغییرات فایلها	تغییر برنامه	عملیات نامناسب	موارد متفرقه
۱ــمسئول اطلاعات ورودی/ترمینال	۹	۴	—	۱	—	—	۱
۲ ــ منشی	۹	۶	—	۱	—	—	—
۳ ــ برنامه‌نویس	—	—	—	—	۱۴	—	۱
۴ــ مدیر متصدی	۸	۴	۳	۱	۳	۱	۱
۵ــاپراتورکامپیوتر	۱	۴	—	۱	—	۳	—
۶ ــ سایر پرسنل	۱	—	۱	۱	—	—	۲
۷ ــ افراد خارج از موٴسسه	۳	۱	—	—	—	—	۱
۸ ــ نامعلوم	—	۱	—	۲	—	—	—

جدول ب متوسط زیان ــ چگونگی مبادرت مرتکبین ــ شامل موارد انفرادی

موقعیت شغلی مرتکب اصلی	مرتکبین انفرادی	مرتکبین جمعی	داخل موٴسسه ۱	داخل موٴسسه ۲	داخل موٴسسه ۲ <	خارج از موٴسسه ۱	خارج از موٴسسه ۲	خارج از موٴسسه ۲ <	متوسط زیان (هزار) انفرادی	متوسط زیان (هزار) جمعی
۱ــمسئول اطلاعات ورودی/ترمینال	۴	۱۵	۵	۱	۳	۱	—	۵	۸ دلار	۷۲۷دلار
۲ ــ منشی	۱۱	۱۶	۳	۱	۱	۲	—	۱	۳۷	۵۸
۳ــبرنامه‌نویس	۱۰	۱۵	۴	۱	—	۳	—	۱	۲۰	۵۳
۴ــمدیرمتصدی	۱۸	۲۱	—	۳	—	—	—	۱	۲۷۴	۳۱۴
۵ــاپراتورکامپیوتر	۵	۹	—	۲	۱	—	۱	۱	۳۳	۳۷
۶ ــ سایرپرسنل	۴	۵	—	۱	—	—	—	—	۴۸	۹۲
۷ــاپراتورکامپیوتر	۳	۵	—	—	—	—	—	—	—	۶۹۶
۸ ــ نامعلوم	—	۳	—	—	—	—	—	—	—	۲۴۰۰

سیستم جلوگیری از کلاهبرداریها

با علم به اینکه مردم چگونه مرتکب کلاهبرداری می‌شوند می‌خواهیم بدانیم که چگونه از این اعمال جلوگیری نماییم. همچنانکه Allen اشاره نموده" از بیشتر کلاهبرداریهای کامپیوتری با بازبینی ساخت سازمانی شرکت جلوگیری می‌شود" و "شاید غیرممکن است که نیمی از موارد کلاهبرداری. . . از حوزه مسئولیت افرادی که اطلاعات را مورد پردازش قرار می‌دهند جدا شود".

عملیات اجرایی فساد خارجی[21] در سال ۱۹۷۷ مدیران را واداشت تا از یک سیستم مناسب کنترل داخلی جهت حفاظت از داراییها استفاده نمایند. چگونگی ایجاد و ابقای یک سیستم مناسب کنترل داخلی کاملا" مربوط به مدیران بوده و حسابرسان مستقل باید جهت ایجاد و ابقای چنین سیستمی مشتریان را یاری نمایند.

یک روش سیستماتیک که "روش گردش سیستمها "[22] نامیده می‌شود می‌تواند یک سیستم مناسب کنترل داخلی را ایجاد نموده و آن را ادامه دهد. اصول زیربنایی روش این است که سیستم براساس کنترلهای "سیستمهای اطلاعاتی حسابداری" می‌باشد بنابراین می‌تواند بطور موثری از نقطه‌نظر گردش سیستمی گسترش پیدا نماید.

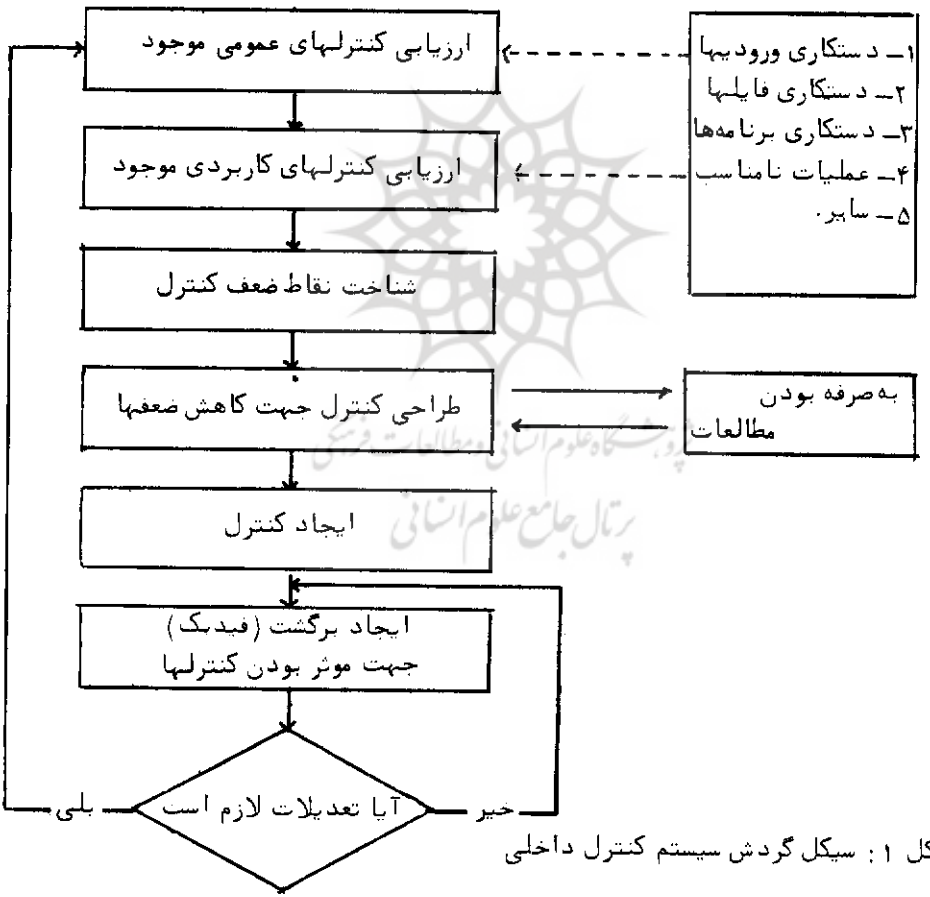
گردش سیستم کنترل داخلی[23]

گردش سیستم کنترل داخلی در شکل ۱ نشان داده شده. گردش با ارزیابی کنترلهای عمومی و کاربردی وضعیت موجود شروع می‌شود. درطی ارزیابی به ۴ نوع دستکاری کامپیوتر که منجر به کلاهبرداری می‌گردند باید توجه خاصی مبذول داشت، بخصوص بمنظور ارزیابی کنترلی در سیستم اطلاعاتی حسابداری باید به سئوالات زیر پاسخ داد: آیا ترکیب کنترلهای عمومی و کاربردی، کنترل مناسبی بمنظور جلوگیری از دستکاری ورودیها، فایلها، برنامه‌ها و عملیات نامناسب[24] اعمال می‌نمایند؟ در جواب به این سئوالات به سومین مرحله گردش می‌رسیم که شناخت نقاط ضعف کنترلی است. چهارمین مرحله از دو مرحله کوچکتر شامل طرح تدابیر کنترلی و توجیه اقتصادی آنها تشکیل

---

21 Foreign Corruption Practices Act
22 System life cycle approach
23 Life Cycle of The System of internal control
24 Improper Operation

می‌شود . هر طرح کنترلی که درنظر گرفته می‌شود باید دارای هزینه مطالعاتی به‌صرفه باشد . از آنجایی که رسیدن به کنترل مطلق ازنظر اقتصادی غیرمعقول است، باید مطالعات براساس به‌صرفه بودن هزینه‌ها باشند، کنترل مطلق به‌معنی وضعیتی بدون ریسک می‌باشد ــ وضعیتی که رسیدن به آن بسیار گران خواهد بود ــ. پنجمین مرحله تعدیلات اقتصادی این تدابیر کنترلی جهت ایجاد کنترلها می‌باشد . مرحله ششم سنجش کنترل داخلی اجراشده و برگشت اطلاعات به مدیریت است ، این مرحله عموما" تحت کنترل حسابرسان داخلی یا گروه کنترلی دایره EDP است . برگشت اطلاعات درمورد اجرای سیستم کنترل داخلی شامل کفایت یا عدم کفایت سیستم کنترل داخلی است . اگر سیستم کنترل داخلی مناسب تشخیص داده شود برگشت اطلاعات بایستی تازمانی که تعدیلاتی بیشتر در سیستم کنترل داخلی لازم تشخیص داده می‌شود ، ادامه یابد .



شکل ۱ : سیکل گردش سیستم کنترل داخلی

نقش حسابرسان مستقل در سیکل :

سیکل گردش سیستم کنترل داخلی که در بالا شرح داده شد به حسابرس مستقل درمورد مطالعه و ارزیابی کنترل داخلی ، مشتری کمک می‌کند . سیکل می‌تواند به‌عنوان پروسه انجام مسئولیت حسابرس درقبال مشتریان موردنظر قرار گیرد . حسابرسان مستقل باید اول کنترلهای عمومی را ارزیابی نموده ، سپس مطالعه و ارزیابی درمورد کنترلهای کاربردی را در هریک از کاربردهای عمده کامپیوتر بعمل آورند . در اینجاست که باید حسابرس مستقل احتمال وقوع دستکاری ورودیها ، فایلها ، برنامه‌ها و عملیات نامناسب در هر سیستم اطلاعاتی حسابداری را درنظر بگیرد . در ارزیابی کنترلهای داخلی ، حسابرس مستقل ممکن است بررسیهای اولیه (مقدماتی) ، بررسیهای تفضیلی ، و تستهای تطبیق جهت برآورد کنترلهای داخلی مشتری ، اجرا نماید . هر ضعفی که در سیستم کنترل داخلی مشتری مشاهده شد باید به نظر مدیران موسسه رسیده و روشهایی جهت ازبین بردن ضعفهای مشاهده‌شده ارائه گردد . حسابرس‌مستقل باید چگونگی انجام پیشنهاد ارائه‌شده به مشتری را پیگیری نماید . این پیگیری ممکن است چندماه پس‌از حسابرسی یا درحین حسابرسی سالانه انجام گیرد و بستگی به توافقهای موجود بین مشتری و حسابرسان دارد .

خلاصه اینکه حسابرسان مستقل در کمک به مشتری جهت دوام سیستم کنترل داخلی بخصوص در شرکتهایی که فاقد حسابرس داخلی هستند ، دارای نقش حساسی می‌باشند . بمنظور پیشگیری و کشف کلاهبرداریهای کامپیوتری حسابرسان مستقل باید باتوجه به احتمال دستکاری ورودیها ، فایلها ، برنامه‌ها ، وعملیات نامناسب سیستمهای اطلاعاتی حسابداری را مطالعه و ارزیابی نمایند .

پیشگیری از دستکاری ورودیها

باتوجه به نتایج بدست‌آمده از تحقیقات Allen ، حدود ۷۰% کلاهبرداریها ازطریق ورودیها انجام می‌گیرد . در اینجا ما روشهای کنترلی مورداستفاده جهت جلوگیری از دستکاری ورودیها را بررسی می‌نماییم .

معاملات می‌توانند در دو مرحله از عملیات ورودیها اضافه ، کسر ویا تغییر یابند . مرحله انجام معامله و مرحله ثبت معامله . این‌دو مرحله با ایجاد اسناد اصلی شروع و درست قبل از تبدیل به زبان قابل‌فهم کامپیوتر تمام می‌شوند . بعد از تغییر اطلاعات به زبان قابل‌فهم کامپیوتر ، ورودیها توسط کامپیوتر تهیه می‌شوند و پس از آن اطلاعات

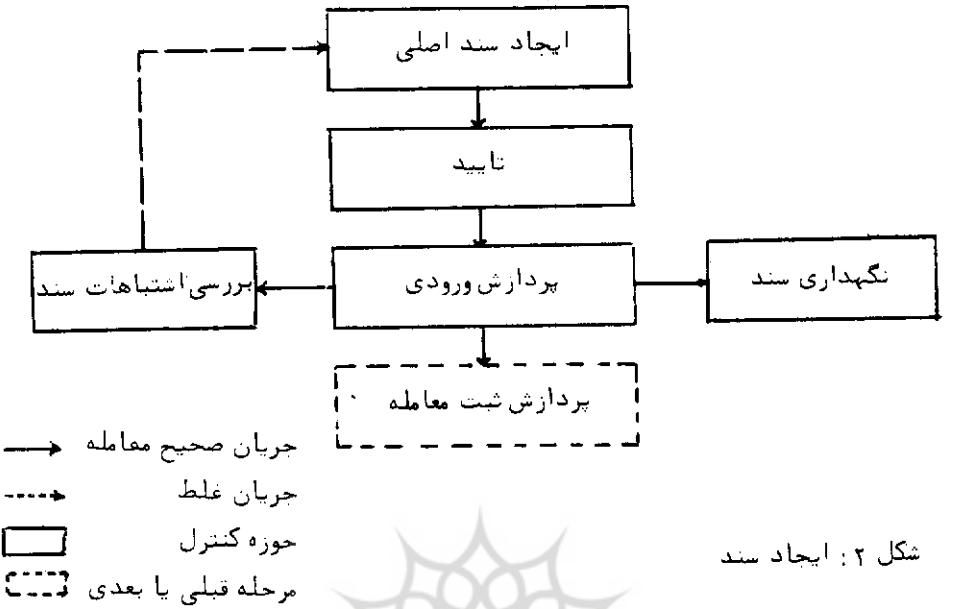
برای فایل اصلی (مسترفایل) پردازش می‌گردد . این‌دو مرحله در زیر موردبحث قرار گرفته است :

ایجاد معامله و کنترلهای آن . شکل ۲ نشان می‌دهد که مرحله ایجاد معامله شامل : ۱) ایجاد سند اصلی ، ۲) تایید معامله (مجاز بودن معامله) ، ۳) تهیه ورودیها ، ۴) نگهداری (بایگانی) سند ، ۵- بررسی اشتباهات سند می‌باشد . ایجاد اسناد مربوط به نقطه‌ای است که در آن اسناد اصلی معاملات بوجود می‌آیند . تایید معامله مرحله‌ای است که در آن معامله بوسیله یک‌نفر که صلاحیت دارد مورد تایید (تصویب) قرار می‌گیرد . بعد از ایجاد و تایید اسناد اصلی اطلاعات معامله قبل از اینکه به زبان قابل فهم کامپیوتر تبدیل شوند ، باید تهیه گردند . تهیه ورودیها شامل : بررسی اطلاعات سند ، آماده کردن جمعها ، و رونویسی اطلاعات از اسناد اصلی به فرم ازقبل‌طراحی‌شده می‌باشد . همزمان با تهیه ورودیها ، ممکن است اشتباهات اطلاعات بوجود آید که نتیجتا " روشهای بررسی اشتباهات موردعمل قرار می‌گیرند . بعد از اینکه ورودیها تهیه شدند اسناد اصلی بایگانی شده و بصورتی مناسب نگهداری می‌شوند .

جهت جلوگیری از دستکاری ورودیها باید کنترلهایی در هریک از مراحل انجام معامله اعمال شود . برای کنترل ایجاد اسناد اصلی باید روشهایی جهت ایجاد و حفاظت از فرمهای معاملات نوشته شود . در فرمها باید محدودیتهای اختیارات ، جمع ناخالص ، جمع خالص ، مانده‌گیری ، ته‌جمع ها ، ضبط تاریخ ، و شماره سریال موردتوجه قرار گیرند و بایستی فقط‌منحصر به فرمهای موجودی کالا باشند . برای اعمال کنترل در اختیارات باید جزئیات اختیارات سرپرستان در تایید معاملات ، بصورت مدون باشد . بطوریکه معمول است پرسنل پردازش اطلاعات نباید مجاز به انجام و تصویب معامله باشند و بایستی تفکیک وظایف بین دایره EDP [۲۵] و دوایر استفاده‌کننده وجود داشته باشد . تایید معاملات باید به‌استناد مدارک کتبی انجام شود . کنترلهای تهیه ورودیها شامل اطلاعات معاملات ، بررسی استفاده‌کنندگان ورودیها ، جمعهای دسته‌ای ، صورت عملیات اسناد ، و حفاظت فیزیکی اسناد می‌باشد . در رابطه با کنترلهای حفاظتی اسناد اصلی ، باید از آنها بصورتی سیستماتیک و فیزیکی حفاظت شود و دسترسی به اسناد فایلها محدود به افراد مجاز باشد . درمورد بررسی اشتباهات اسناد اصلی باید روشهای مدونی جهت : بررسی اشتباهات کشف‌شده ، تصحیح اشتباهات ، تعویض (جایگزینی) اطلاعات تصحیح‌شده ، و همچنین تفکیک وظایف بین افراد تهیه‌کننده یا تصویب‌کننده اسناد اصلی و افرادی که بررسی‌کننده

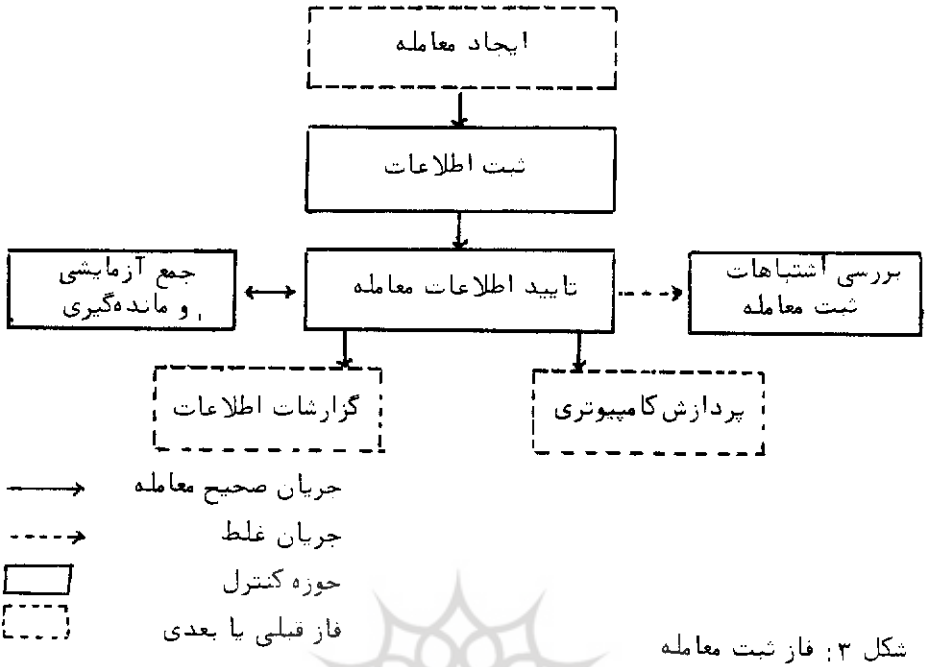
25 Earning Data Process

اشتباهات می‌باشند ، وجود داشته باشد .



شکل ۲ : ایجاد سند

مرحله ثبت معامله و کنترلهای آن : کنترل ثبت معاملات از نقطه‌ای که اطلاعات تغییر پیدا می‌کنند شروع می‌شود که این تبدیل اطلاعات می‌توانند در فرمهای کارت پانچ ، یا بصورت ثبت اطلاعات بوسیله یک خط ارتباطی ازطریق ترمینال انجام گیرند . در هریک از دو فرم ، باید اطلاعات تایید و بررسی شوند تا بدون اشتباه باشند . تایید اطلاعات معامله ازطریق روشهای بررسی اشتباهات ثبت معامله انجام می‌گیرد . کنترلهای ثبت معامله بابت جلوگیری از کلاهبرداریهای کامپیوتری ازطریق اضافه نمودن معاملات غیرمجاز اختصاصاً" دارای وضعیتی بحرانی می‌باشند. نقاط کنترلی در مرحله ثبت معاملات در شکل ۳ نشان داده شده است .



شکل ۳: فاز ثبت معامله

کنترلهای ثبت معاملات، کنترلهای کاربردی می‌باشند که جهت اطمینان از ورود اطلاعات مجاز بصورت کامل و صحیح به سیستم کامپیوتری، مورد استفاده قرار می‌گیرند. در نقطه تبدیل اطلاعات باید روشهای مدونی شامل موارد زیر باشد: الف و ب، در چه موقع و توسط چه‌کسی تبدیل اطلاعات انجام شود؟ ج: استفاده از "توقف کار برای رسیدگی" د: جمع آزمایشی. سخت‌افزارهای تبدیل اطلاعات همچون ترمینالها، وسایل کلید به نوار[۲۶]، و ماشینهای کارت پانچ باید بصورتی فیزیکی حفاظت شوند و مطمئن شویم که افراد غیرمجاز نمی‌توانند به آنها دسترسی داشته باشند و افراد مجاز هم بعد از ساعات کار اداری نتوانند وارد اطاق ترمینال شوند. یادآوری این نکته ضروری است که سیستم کلمه رمز می‌تواند اطمینان دهد که دسترسی به ترمینال فقط بصورت مجاز امکانپذیر است و بایستی صورت عملیات ترمینال به اندازه کافی بررسی شود تا هرگونه دسترسی غیرمجاز به ترمینال آشکار گردد. علاوه بر اینها باید به تقسیم کار بصورتی مناسب وجود داشته باشد که اشخاص ثبت‌کننده اطلاعات همان افراد بررسی‌کننده صورت عملیات ترمینال یا اپراتورهای کامپیوتر یا نویسندگان برنامه‌های کاربردی نباشند.

---

26 Key-to-Tape

کنترلهای تایید اطلاعات معامله مربوط به بررسی رونوشتها و تنظیم برنامه می‌باشند. اگر اطلاعات روی کارت پانچ واردشده از این اطلاعات باید بصورتی دستی یا غیردستی بررسی شوند، اگر اطلاعات به ترمینال وارد می‌شوند، دستورالعمل مدونی باید صحت اطلاعات در ترمینال را تایید نماید. وقتی که اطلاعات به فرم قابل‌فهم کامپیوتر در آن ذخیره شد یک برنامه اجرا می‌گردد تا اعتبار و کامل بودن اطلاعات معامله را آزمایش نماید. در برنامه تنظیمی موارد زیر باید رعایت شود: الف: چه‌کسی معامله را انجام داده، ب: چه‌کسی آن را تایید نموده، ج: جمع آزمایشی گرفته شده و با جمعهای دستی مقایسه گردد.

بعد از اینکه اشتباهات اطلاعات معلوم شد باید مطابق روشهای بررسی اشتباهات که قبلا" تشریح شد بررسی و تصحیح گردند. کنترلهای بررسی اشتباهات جهت اطمینان از اینکه در کشف اطلاعات اشتباه، پیگیری مناسبی وجود دارد، موردنیاز می‌باشند. روشهای مدون بررسی اشتباهات شرحی است از: ۱ـ افرادی که مسئول بررسی اشتباهات و تصحیح آنها می‌باشند و ۲ـ افرادی که مجاز به تایید اطلاعات تصحیح‌شده در هر سیستم اطلاعاتی حسابداری می‌باشند. لازم به یادآوری است که افراد ایجادکننده، تصویب‌کننده، یا تهیه‌کنندگان ورودیهای معاملات یا افراد بررسی‌کننده ثبت معاملات نباید همان افرادی باشند که اشتباهات را بررسی می‌نمایند. همچنین دسترسی غیرمجاز باید فورا" به اطلاع حسابرسان داخلی یا مدیران سطوح بالا جهت تکمیل نمودن بررسیهایشان برسد.

بطور خلاصه اگر کنترل ورودیها بدقت برنامه‌ریزی شده و اجرا گردند از کلاهبرداریهای کامپیوتری درسطح وسیعی جلوگیری خواهد شد. کنترلهای ورودیها شامل کنترلهای ایجاد معامله و کنترلهای ثبت معامله می‌باشند. قسمت اول شامل: کنترلهای ایجاد اسناد اصلی، کنترلهای مجاز بودن، کنترلهای تهیه ورودیها، کنترلهای بررسی اشتباهات اسناد، و کنترلهای نگهداری (بایگانی) اسناد می‌باشند. قسمت دوم شامل: کنترلهای ثبت اطلاعات، کنترلهای صحت اطلاعات معامله، کنترلهای مانده‌ها و جمعها، و کنترلهای بررسی اشتباهات ثبت معاملات می‌باشند.

نتیجه:

کلاهبرداریهای کامپیوتری یکی از خطرات جانبی تکنولوژیهای کامپیوتری در قرن حاضر می‌باشند. این عمل می‌تواند بعنوان یک هدف، یک محیط، و یک سمبل، مورد

استفاده قرار گیرد.

پیشتر نظر عموم بر این بود که حسابرس مستقل طی بررسیهایش باید کلاهبرداریها را کشف نماید اما حسابداران حرفه‌ای معتقدند که کشف کلاهبرداریها مسئولیت اصلی حسابرسان مستقل نمی‌باشد، درحالی که اگر کلاهبرداریهایی وجود داشته باشد ممکن است طی مطالعه و ارزیابی کنترلهای داخلی مشتری توسط حسابرس مستقل کشف گردد. باید اشاره نمود که از زمان بابل قدیم (در قرون وسطی) تا دهه ۱۹۳۰ همیشه فرض بر این بود که مسئولیت اصلی حسابرسان کشف کلاهبرداریها بوده است.

کلاهبرداریهای کامپیوتری به ۴ صورت ممکن است انجام گیرند: ۱ـ دستکاری ورودیها، ۲ـ دستکاری فایلها، ۳ـ دستکاری برنامه‌ها، و ۴ـ دستکاری عملیات. دستکاری ورودیها عمده‌ترین روشی است که جهت کلاهبرداریها مورداستفاده قرار می‌گیرد. بنابراین بایستی کنترلهای مناسبی روی دستکاری ورودیها، طراحی و ایجاد شود که درآن دو مرحله ایجاد و ثبت معامله موردتوجه قرار گیرد. طی مرحله ایجاد معامله کنترلهایی روی: ۱ـ ایجاد سند اصلی، ۲ـ تایید معامله (مجاز بودن معامله)، ۳ـ تهیه ورودیها، ۴ـ بایگانی سند، و ۵ـ بررسی اشتباهات سند، اعمال می‌گردند. کنترلها در مرحله ثبت معامله عبارتند از: ۱ـ تایید اطلاعات، ۲ـ بررسی اشتباهات معامله، ۳ـ اعمال روشهای مدون روی: بررسی اشتباهات معامله، تبدیل اطلاعات از سند اصلی به زبان قابل‌فهم کامپیوتر، و سایر عملیات ورودیها، ۴ـ حفاظت فیزیکی از وسایل ورودی، ۵ـ کاربرد و حفظ سیستم استفاده از کلمه رمز، و ۶ـ تفکیک وظایف بصورتی مناسب در پردازش ورودیها.

جهت ایجاد یک سیستم مناسب کنترل داخلی که بتواند از کلاهبرداریهای کامپیوتری جلوگیری نماید می‌توان از روش "گردش سیستمها" استفاده نمود. مراحل متوالی گردش، سیستم کنترل داخلی را ازلحاظ نقاط قوت و ضعف بررسی کرده و ایجادکننده طرحهای کنترلی مجاز اقتصادی جهت ازبین بردن نقاط ضعف در سیستم کنترل داخلی است. گردش سیستم کنترل داخلی شامل موارد زیر می‌باشد: ۱ـ ارزیابی کنترلهای عمومی موجود، ۲ـ ارزیابی کنترلهای کاربردی، ۳ـ شناخت نقاط ضعف کنترل، ۴ـ طراحی طرحهای کنترلی مقرون بصرفه ازنظر هزینه مطالعات، ۵ـ ایجاد طرحهای کنترلی، و ۶ـ ایجاد برگشت اطلاعات درمورد موثر بودن کنترل داخلی.

◆◆◆