اولین کنفرانس بین المللی جهش علوم مدیریت اقتصاد و حسابداری
1st international conference on the mutation of management science, economics and accounting
www.mmea.ir
موسسه آموزش عالی ادیب مازندران
ISC کد اختصاصی: ۰۰۲۰۱-۹۱۰۴۶

**عنوان:** شناخت تقلب رایانه ای در سیستم های اطلاعاتی حسابداری وارائه راهکار های پیشگیری

**علی امیری**[۱]
**ماهرخ دارابی**[۲]

## چکیده :

دلیل اهمیت سیستم اطلاعاتی حسابداری برای متخلفان و مجرمان رایانه‌ای، نقش سیستم های اطلاعاتی حسابداری در کنترل منابع مالی است همچنین با توجه به اهمیت این سیستم ها برای مدیریت عملیات سازمان، ممکن است در معرض سوء استفاده فرصت طلبان و افراد که دارای تضاد منافع با سازمان هستند، قرار گیرد. لذا پژوهش حاضر با بررسی جرایم رایانه ای در شاخه ی اطلاعات حسابداری و مقوله بندی آن به منظورآگاه سازی حسابداران و حسابر سان و سایر ذینفعان اطلاعات مالی میتواند راهکارهای نوینی برای جلوگیری از اعمال مجرمانه ارائه نماید. همچنین مقوله بندی های انجام شده ابزاری(تهیه پرسشنامه) برای نگارش پژوهش های تجربی آینده است . این پژوهش از منظرهدف توصیفی -تطبیقی می باشد، که به شیوه کتابخانه ای تحلیل محتوا گردیده است .نتایج حاصل از پژوهش ، شامل سه بخش است که نخست مقوله بندی انواع تقلب رایانه ای شامل ۱- تقلب اطلاعات۲_ پرداز شگر۳_ داده های ورودی۴- د ستورهای رایانه‌ای۵_ ستاده ها ا ست،، سپس راه های پی شگیری و ک شف تقلب های رایانه‌ای شامل تحلیل و تفکیک جزئیات ۴ مقوله به شرح،کاهش احتمال وقوع تقلب ، عوامل افزایش دشواری و سختی ارتکاب به تقلب ، عوامل بهبود شیوه های کشف و شناسایی تقلب و ارائه ی راهکار های پی شگیری از تقلب رایانه ای و شنا سایی شیوه های کاهش زیان نا شی از آن در اطلاعات ح سابداری مقوله بندی شدودرنهایت طبقه بندی ا ستفاده از رویه ها و مقررات منا سب برای ا ستخدام و اخراج کارکنان به شیوه ی کیفی مورد بررسی و تحلیل محتوا قرار گرفت

کلید واژه ها:
تقلب رایانه ای[۳] جرایم رایانه ای[۴] سیستم اطلاعاتی حسابداری[۵] پیشگیری از تقلب[۶]

## ۱- مقدمه:

[۱] استادیار، گروه حسابداری و مدیریت مالی، دانشکده علوم انسانی، دانشگاه آزاد اسلامی واحد بندرعباس، بندرعباس، ایران.
Amiri.study@gmail.com
[۲] دانشجوی دکتری، گروه حسابداری و مدیریت مالی، دانشکده علوم انسانی ،دانشگاه آزاد اسلامی واحد بندرعباس، بندرعباس، ایران
m.darabi412@gmail.com

[3] Computer fraud
[4] cyber crime,
[5] accounting information system,
[6] Fraud prevention

عدم وجود آمارهای دقیق از جرایم رایانه‌ای از اهمیت موضوع و سوء استفاده از سیستمهای اطلاعاتی حسابداری نمی‌کاهد، حسابداران مسئول طراحی و انتخاب و تکمیل و کنترل فرایند هایی هستند که سیستم های اطلاعاتی حسابداری را ایجاد می کند. زیرا اطلاعات حسابداری منتشر شده می تواند، سرمایه گذاران، بستانکاران و تحلیلگران مالی وسایر ذینفعان را گمراه سازد همچنین با توجه به اهمیت این اطلاعات، دستیابی غیر مجاز یا سوء استفاده از آنها می تواند خسارات جبران ناپذیری را برای سازمان ها در بر داشته باشد.

سیستم اطلاعاتی حسابداری شامل افراد، روش ها و شیوه های فن آوری اطلاعاتی[۷]است که در یک سازمان وظایفی به شرح زیر دارد :

۱-گردآوری وذخیره داده های مربوط به فعالیت هاورویدادهابطورکلی که یک بنگاه تجاری بتواندآنچه را رخ داده است بررسی کند.

۲-پردازش وتبدیل دادهابه اطلاعات مفیدبرای تصمیم گیری به نحوی که مدیریت برمبنای این اطلاعات قادربه برنامه ریزی, اجراوکنترل فعالیت های شرکت باشد.

۳-طراحی کنترل های داخلی[۸]کافی بمنظورحفاظت ازداراییهاازجمله مدارک واطلاعات بنگاه.(مقدسی ۱۳۸۶)

با گسترش و به کارگیری فناوری‌های جدید پدیده جرایم مرتبط با این فناوری ها با سرعت و به صورت تصادفی افزایش یافته است، هم اکنون مجرمان به ویژه در کشورهای بسیار پیشرفته قادرند از خانه خود و با کمی امکانات، پول بانک‌ها و شرکت‌ها را از نقطه ای به نقطه دیگر جهان انتقال دهند و این در حالی است که سعی می‌کنند با اقدامات پیچیده ردپایی از خود به جای نگذارند این مجرمان افراد متخصصی هستندکه به رمز و راز های تخصصی و فنی امور رایانه آشنایی دارند و همین دلیل است که متولیان مقابله با این جرایم به سختی و پس از گذشت زمان نسبتاً زیادی آنها را کشف می‌کنند.(مقدسی ۱۳۸۶)، ( مرادی و بیات ۱۳۹۴)

بین دو واژه ی جرایم رایانه ای و سوء استفاده رایانه ای تفاوت بسیار ظریفی وجود دارد، در جرایم رایانه ای افراد زمانی مرتکب جرم رایانه‌ای می‌شوند که منافع مالی غیرمشروع به دست آورده اند، اما سوء استفاده کنندگان رایانه با انگیزه انتقام و چالش، به سازمان خسارت وارد می‌کنند. با توجه به تمایزی که بین این دو کلمه وجود دارد به نظر می رسد استفاده از واژه تقلب رایانه‌ای بتواند به نوعی ویژگی های هر دو واژه را پوشش دهد به عبارت دیگر هر گونه اقدام عمدی و فریبکارانه که توسط مدیران یا اشخاص ثالث برای بدست آوردن مزیتی ناروا و غیرقانونی اعم از مالی و غیرمالی انجام می‌شود را تقلب گویند.( مرادی و بیات ۱۳۹۴) ، (محمودی ۱۳۹۱)،

بنابراین حفاظت اطلاعات تنها در صورتی موثر است که مدیریت سازمان تقلب ها و جرایم رایانه ای را جدی بگیرد و سیاست‌های کنترلی دقیقی را به منظور پیشگیری و یا حداقل کردن خسارت این تهدیدها اجرا کندهمچنین مدیریت ، پیش از آنکه منابع اش را برای ایمن سازی به کار گیرد باید بداند که کدام یک از دارایی ها نیاز به

---

[۷] Information technology practices
[۸] Internal controls

حفاظت دارند و هر یک تا چه اندازه آ سیب پذیرند، ارزیابی خطر، موثرترین مجموعه کنترل‌ها را برای حفاظت از دارایی‌ها تعیین می کند، ارزیابی خطر فرآیندی تکراری و پویا برای شنا سایی حوادثی ا ست که د ستیابی به اهداف مو سسه را تهدید می کند و با این ارزیابی، می توان تهدیدها را مدیریت کرد و ازتکرار ارتکاب به جرایم رایانه ای پیشگیری نمود.

مدیران، حسابداران و سرمایه گذاران از اطلاعات رایانه‌ای[9] برای کنترل منابع ارز شمند خود ا ستفاده می کند بنابراین می توان گفت که اطلاعات مالی رایانه ای سرمایه ارزشمندی است که می باید از آن محافظت کرد، هرچه مدیران و حسابداران بیشتر راجع به تقلب ها و جرایم رایانه‌ای آگاهی داشته باشند، بهتر می توانند ریسک و کنترل های ریسک پذیر را در سیستم های اطلاعاتی رایانه‌ای تشخیص دهند، بنابر آنچه گفته شد و با توجه به افزایش روزافزون تقلب ها و جرایم رایانه‌ای ضروری ا ست حسابداران و مدیران که نقش کلیدی در طراحی سیستمهای اطلاعاتی دارند با ماهیت تقلب و فرایندی که افراد برای انجام تقلب و مخفی سازی آن انجام می‌دهندآ شنا شده و راه های چگونگی جلوگیری از تقلب و جرایم رایانه‌ای را بشنا سند . مقوله های طبقه بندی شده در این پژوهش، به طراحی کنترلهای داخلی مناسب توسط مدیران کمک میکند و در انتخاب درست روش های مختلف پیشگیری از تقلب، به منظور کاهش جرایم رایانه ای، موثر است، و همچنین می تواند برای نهاد های نظارتی و استاندارد گذاران در توسعه ی استانداردها و الزامات گزارشگری سودمند واقع گردد. و در نهایت وضوح مفهومی حاصله ازمقوله بندی این پژوهش با ارائه اطلاعات طبقه بندی شده ،پیش بینی کننده و بازدارنده، به حمایت از دقت وامنیت استانداردگذاری وگزارشگری مالی سازگاردر محیط ریسک پذیر امروز می پردازد .و تا به امروز موضوع حاضر از دیدگاه محتوایی، مورد طبقه بندی و بررسی قرار نگرفته و دردسترس استفاده کنندگان نبوده است همچنین تهیه پرسشنامه روا و پایا، نیازمند زیر ساخت دقیق و علمی است که در پژوهش حاضر با مقوله بندی علمی امکان تهیه ی پرسشنامه ی مناسب برای پژوهش های تجربی فراهم گردیده است .

## ۲- مبانی نظری وپیشینه ی پژوهشی:

تقلب در اطلاعات مالی، یکی از مو ضوعات شایان توجه در تئوری نمایندگی ا ست این تئوری به وجود ت ضاد منافع میان ذینفعان یک سازمان اشاره دارد که خودانگیزه[10] برای ایجاد تقلب است (خواجوی و ابراهیمی، ۱۳۹۷) تقلب در مفهوم کلی خود دربرگیرندۀ تمام ابزارهای ساختۀ انسان است و فرد با استفاده از آن مزیتی را از طریق توصیه های دروغین یا کتمان حقیقت کسب می کند و شامل تمام رویدادهای ناگهانی، ترفندها ، مخفی کاری ها و سایر راه های غیرمنصفانه برای فریب دیگری می شود. (قادری و قادری،۱۳۹۶) با الهام از گزارش سازمان ملل متحد ، ا ساس مبانی نظری جرایم رایانه ای در حسابداری ریشه در چهار عنصر ا صلی دارد: انحصار متقابل ، ساختار ، جامعیت و دسته بندی های مشخص با توصیفات واضح.

---

9 Computer information
10 Self-motivated

انحصـار متقابل: انحصـار متقابل این امر را تضـمین می کند ، عملی که یکبار در یک گروه طبقه بندی می شـود ، نمی تواند متعلق به گروه دیگری باشد ، بنابراین نتیجه این امر ، حذف عملیات همپوشانی است.

ساختار : ساختار گروههای گسترده ای ایجاد می کند و عملا سطوح سلسله مراتبی را محدود می کند ، در نتیجه پیچیدگی ها را کاهش می دهد و خود دلیلی بر ایجاد تقلب است (آنودس۲۰۱۲ )

- اشتباه در برنامه‌ها
- اشتباه در ورود اطلاعات از سوی کاربران
- مشکلات سخت‌افزاری و نرم‌افزاری مرتبط با داده‌ها
- عدم انجام کامل فرایند بر روی داده‌ها
- وجود افزونگی و تعدد در داده‌های تکراری.

برای کنترل و تضـمین جامعیت، قواعدی لازم اسـت تا سـیسـتم مدیریت بتواند بر اسـاس آن‌ها عمل کرده و باعث انطباق محتوای پایگاه با واقعیات باشـد و این قواعد را قواعد جامعیتی یا محدودیتهای جامعیتی گویند.( رانکوهی ۱۳۸۸)

چهار عنصر اساسی بیان شده امکان شناسایی و دسته بندی یک جرم سایبری(رایانه ای) منحصر به فرد را فراهم می کند که هر کدام به طور مشـخص برای تعیین موقعیت مناسـب آن در طبقه بندی قرار گرفته و برای شـناسـایی تغییرات جدید آن فعال است . طبقه بندی سلسله مراتبی[۱۲] و طبقه بندی های ذاتی باعث درک آسان جرایم سایبری شده است و تنوع آن را به طور معنی داری سازماندهی می کند. اثر جرایم رایانه ای صدمه ای است که به قربانی وارد می شود.این صدمات آسیب هایی ملموس یا[۱۳] ناملموس[۱۴] برای قربانیان هستند.

در جرایم رایانه ای بیشـترین تمرکز بر قربانیان اسـت . انواع قربانیان در اشـکال زیر ظاهر می شـوند: اکوسـیسـتم فناوری رایانه مسـتقیم (مانند سـیسـتم های کامپیوتری ، فناوری های مرتبط با رایانه ، سـیسـتم های شـبکه ای) ، اکوسیستم فناوری رایانه غیر مستقیم(اشخاص حقیقی ، نهادهای تجاری ، دولت ها )

برای شـناسـایی اثر یک جرم رایانه ای یا سـایبری ، بیشـترین تمرکز بر قربانیان مسـتقیم اسـت ، که به عنوان تاثیر پذیرترین عامل در جرایم رایانه ای تعریف میشوند.و اما در شرایط معکوس ، یک قربانی غیرمستقیم، نسبت به یک قربانی مستقیم ، یا قدرتمند تر شده و یا از سیستم حذف میشود. لازم به ذکر است قربانیان مستقیم همیشه قربانی نهایی نیسـتند، . اما قربانیان غیر مسـتقیم ، افراد ، نهادها یا دارایی هایی هسـتند که در جرایم سـایبری متحمل ضـرر مالی می شوند.علاوه بر این ، افراد یا نهادها نیز ممکن است دارای حقوق مالکیت یا دسترسی به دارایی هایی باشند که ارزش خود را در جرایم سـایبری[۱۵] از دسـت می دهند. بنابراین ، برای تطبیق تحولات آینده در فناوری ، طبقه

---

12 UNODC
13 Hierarchical classification
14 Tangible injuries
15 Intangible injuries
16 Cybercrime

بندی مبانی نظری برای جرایم رایانه ای در رشته حسابداری را در چهار مقوله ، طراحی ، حاکمیت شرکتی ، ریسک و کنترل ،تقسیم بندی میکنیم ، این مقوله ها، به دنبال حصول پیامد هایی به شرح زیر است:

مقررات : که به دنبال ایجاد شفافیت و پاسخگویی است ؛

اجرا : که نیاز به وضوح مفهومی دارد ؛

سیاست عمومی : که به دنبال افزایش ظرفیت و توسعه مهارت در جامعه است.

یکی از عوامل موثر بر تقلب، حاکمیت شرکتی است که از دو طریق درون سازمان و برون سازمان می تواند مهار کننده ی جرایم فوق الذکر با شد، سازوکارهاي درون سازمانی به پنج د سته ا صلی د سته بندی می شوند که عبارت اند از: ۱- هیئت مدیره (نقش ها، سازه ها و انگیزه ها)؛ ۲- انگیزه های مدیریتی۳- .ساختار سرمایه؛ ۴- اساسنامه و مقررات شرکت ها، ۵- سیستم کنترل داخلی .در حالی که سازوکار برون سازمانی به پنج دسته بدین شرح طبقه بندی می شود ۱- .قانون ومقررات، ۲- بازار؛ ۳- اطلاعات بازار سرمایه و تجزیه و تحلیل؛ ۴- بازار حسابداری ۵- .امور مالی و قانون ؛ ۶- منابع ویژه کنترل برون سازمانی(دراماستیتو و واهودی ۲۰۱۳)

به طور کلی تقلب رایانه ای شامل موارد زیر ا ست سرقت، ا ستفاده، د ستیابی، تغییر دادن، نسخه برداری و خراب کردن غیرمجاز نرم‌افزارها و یا اطلاعات، برای مثال: مسئول تعمیرات و رفع خطاهای نرم‌افزاری مکرراً برای انجام تحقیقات به شرکت فرا خوانده می‌شود پس از مدتی شرکت این موضوع را کشف کرد که این فرد با هر بار مراجعه به شرکت خرابکاری هایی را در سیستم انجام می‌دهد تا برای تعمیرات بعدی مجددا به شرکت دعوت شود و با انجام این کار میلیون‌ها دلار از منابع شرکت را به نوعی سرقت کرده است، سرقت پول به وسیله تغییر اطلاعات رایانه یا سرقت زمان رایانه ها برای مثال کارمندان انبار با ثبت تعدادی از موجودی ها به عنوان موجودی های فرسوده شده و از رده خارج شده اقدام به تغییر سریال وسرقت و فروش این موجودیها می نمایند سرقت یا خراب کردن سخت افزار رایانه برای مثال چنانچه حفاظت های امنیتی به خوبی رعایت نشود ممکن است افراد اقدام به سرقت سخت افزار های رایانه ای نمایند.( مرادی و بیات ۱۳۹۴)، ( رمضانعلی و همکاران ۱۳۸۹)

دومین مورد استفاده یا تبانی در استفاده از منابع ریالی رایانه‌ای برای ارتکاب خیانت است ، برای مثال کارمندان بخش خرید با تبانی اقدام به تهیه فاکتور های خرید جریان نمودند و وجوه نقد شرکت را به این طریق سرقت کردند تلاش برای دستیابی غیرقانونی به اطلاعات یا داراییهای مشهود از طریق به کارگیری رایانه نفوذگران برای دسترسی به اطلاعات محرمانه شرکت اقدام به هک کردن سیستم‌های رایانه‌ای شرکت می نمایند تا پس از دستیابی به اطلاعات محرمانه کامان آنها را به رقبای شرکت بفروشند گزینه بعدی اخاذی از طریق سیستم‌های رایانه‌ای برای مثال کارمندان یک شرکت پس از اینکه متوجه شد مدیر شرکت قصد اخراج وی را دارد اقدام به سرقت تمام اطلاعات محرمانه از شرکت کرد و برای بازگرداندن آنها مبلغ قابل توجهی را طلب کرد در یک د سته بندی کلی می توان تقلب های رایانه ای را به دو دسته تقسیم کرد دسته اول گروهی از تقلب هاست که توسط افراددرون سازمان صورت می‌گیرد برای مثال حمله هکرها به سایت شرکت نمونه ای از تقلب رایانه‌ای برون سازمانی است

در مقابل د سته دیگری از تقلب ها مستقیماً تو سط افراد درون سازمانی صورت می گیرد برای مثال اختلاس مبالغ شرکت با حساب سازی و یا تبانی کارمندان و برای اختلاس از جمله موارد تقلب درون سازمانی است به طور کلی تقلب های داخلی را می توان به دو د سته طبقه بندی کرد ا ستفاده از دارایی‌های اختلاس سرمایه تو سط شخص یا گروهی صورت می گیرد که هدف آنها کسب منافع شخصی است این کار معمولاً توسط کارمندان یک سازمان صورت می گیرد هرچند ممکن ا ست افراد دیگری نیز برای انجام چنین کاری با یکدیگر همد ستی نمایند این نوع جرایم کلاهبرداری شغلی نامیده می شود گزینه بد گزار شگری مالی فریبکارانه ا ست اقدامات امنیتی در حذف یا انجام فعالیت هایی که منجر به ارائه نادرست صورتهای مالی شده و صورت‌های مالی مزبور را گمراه کننده می سازد در این نوع تقلب مدیران ارشد سازمان عمدتا ثبت های حسابداری را به منظور گمراه نمودن تحلیلگران بستانکاران و سرمایه‌گذاران تحریف می‌کنند به همین دلیل صورت‌های مالی وضعیت مالی واقعی شرکت را نشان می‌دهد. (مرادی و بیات ۱۳۹۴)

## ۳- روش شناسی:

اهمیت طبقه بندی در تحقیقات ، به دوران ار سطو باز میگردد (فیدلر و همکاران ، ۱۹۹۶ ). پی شینه های پژوهش ها مملو از تحقیقات در زمینه تو سعه طبقه بندی ا ست که حاوی بین شی ا ست که از ر شته های مختلف مانند زی ست شناسی ، شیمی ، معماری داده ها و علوم اجتماعی استخراج شده است ، نیکرسون و همکاران (۲۰۱۳). حسابداری نیز، از این مهم مستثنی نیست چرا که جز طبقه بندی رشته های علوم اجتماعی قرار گرفته است .مقوله بندی به معنای، ارائه ساختاری نوین و سازماندهی شده است ، که درک و تجزیه و تحلیل حوزه های پیچیده را سهل نموده و باعث ایجاد ارتقا علمی و آگاهی مخاطبان میگردد و به دقت اندازه گیری در پژوهش های تجربی آینده می افزاید . (وند و همکاران ، ۱۹۹۵ ، ص ۲۹۱) دراین پژوهش به شیوه ی کیفی وبا داده های کتابخانه ای به توصیف و تطبیق( کیفی – تطبیقی) مباحث تقلب رایانه ای پرداخته شد و با استخراج مقوله های با اهمیت تقلب رایانه ای از منظر متخصصان رشته حسابداری و مالی (مجموعا کتب ومقالات ۱۵ متخصص درایران و۲۰ متخ صص در خارج از ایران) طبقه بندی و تحلیل محتوا گردید و مقوله ها در پنج بخش به شرح جداول در بخش یافته ها، استخراج گردید.

## یافته های پژوهش:

## ۴- مفاهیم و دلایل ایجادو افزایش تقلب رایانه ای :

۴-۱ – برخی دلایل افزایش تقلب و جرایم رایانه‌ای:

۱) یک تعریف کلی برای تقلب و جرایم رایانه‌ای وجود دارد برای مثال بسیاری از کاربران از این موضوع اطلاع ندارند که نسخه برداری از یک نرم افزار بدون اجازه شرکت سازنده ایرانی جرم رایانه‌ای محسوب می‌شود به طور مشابه بسیاری از کارمندان استفاده شخصی از منابع رایانه‌ای شرکت‌ها را جرم نمی دانند

۲) عدم کشف بسیاری از تقلب های خود عامل افزایش تقلب ها شده است استفاده از روش ها و شگرد های پیچیده توسط مجرمین رایانه‌ای باعث شده است که تنها یک درصد تقلب ها کشف شود.

۳) بسیاری از تقلب های کشف شده گزارش نمی شوند زیرا بسیاری از مدیران معتقدند که هزینه گزارشگری تقلب از هزینه خود تقلب بیشتر است آنها معتقدند گزارش موارد تقلب باعث از بین رفتن اعتماد مشتریان و اعتراف به وجود نقاط ضعف در سیستم های اطلاعاتی و تکرار تقلب می شود

۴) امنیت پایین و ضعف شبکه های بسیاری از شرکت‌ها خود باعث افزایش تقلب‌های رایانه‌ای شده است بسیاری از شرکت‌ها هنوز ضرورت و اهمیت برقراری امنیت غذایی را برای خود احساس نکردند

۵) بسیاری از مجرمین رایانه‌ای با قرار دادن تجربیات خود در اختیار سایر افراد به افزایش جرایم رایانه‌ای کمک می کنند در بسیاری از سایت های رایانه‌ای دستورالعمل گام به گام در مورد چگونگی ارتکاب جرایم رایانه ای وجود دارد

۶) وجود قوانین ضعف و بعضاً ناقص خود منجر به افزایش جرایم رایانه‌ای شده است در شرایط نبود نظارت دقیق بر فضای اینترنتی و عدم پیگیری مناسب پرونده‌های جرایم رایانه‌ای نمی‌توان انتظاری جز افزایش این جرایم داشت(تختایی و صیفوری ۱۳۹۶)

۴-۲- آسیب پذیری سیستم های اطلاعاتی رایانه ای:

تخلفات و جرایم رایانه‌ای رشته وسیعی از جرایم را از طریق سرقت فیزیکی و تخریب وسایل گرفته تا کارشکنی الکترونیکی و خرابی داده‌ها، اختلاس از اطلاعات و سیستم ها و سرقت های آشکار پول که این روزها در سطح وسیع به صورت الکترونیکی شکل می‌گیردرا در بر می‌گیرد برخی از آسیب های اصلی در هر سیستم اطلاعاتی رایانه ای شامل سخت‌افزار، نرم‌افزار، اطلاعات و ارتباطات است که در اینجا به آنها اشاره می شود.

۴-۲-۱- تخریب و سرقت سخت‌افزار:

سخت افزارهای رایانه‌ای هدف جالب توجه ای است برای سارقینی که این قطعات را به فروش می رسانند در جامعه رایانه‌ای امروز مشکلات کمی برای فروش سخت افزار از هر نوع وجود دارد همچنین ممکن است با سرقت سخت افزار سارق سیستم را از کار بیندازد و در این مدت خود از سیستم استفاده کند و اقدامات خرابکارانه را انجام دهد ،همچنین تخریب سخت افزار ها توسط تروریست‌ها و یا به وسیله وجود کارمندان عصبی به کارمندان اخراجی باعث از دست دادن اطلاعات و نرم افزارهای موجود می شود.

۴-۲-۲- سرقت و خرابی نرم‌افزار:

نرم افزار یک دارایی هوشمند است و ممکن است با توجه به نوع وکارکردآن ارزش و حساسیت متفاوتی داشته باشد ، برخی از سرقت های نرم افزار، خیلی سریع اتفاق می‌افتاد کارمندانی را تصور کنید که نرم‌افزارهای مربوط به سازمان را برای رایانه های شخصی خویش کپی می‌کنند، و یا با فیلتر شکن از آن نسخه برداری میکنند، و یا حتی ممکن است این نرم افزار ها دارای حق چاپ و کپی رایت بوده باشند اما تنها برای استفاده در رایانه‌های

کارفرما خریداری شده است و اجازه استفاده شخصی برای سایرین وجود ندارد ، همچنین نرم‌افزارهای رایانه‌ای ممکن است با سهل‌انگاری کارمندان و یا اقدامات خرابکارانه و یا عدم دانش رایانه ای ، انتشار ویروس و ... در معرض تخریب قرار گیرد، که این موضوع هزینه‌های سنگینی را به سازمان‌ها تحمیل می کند.

۴-۲-۳- داده ها و اطلاعات:

داده‌ها و اطلاعات با ارزش‌ترین دارایی‌های شرکت می باشند سخت افزارها و نرم افزارها قابل جایگزینی می باشند اگرچه ممکن است هزینه آنها گران باشد اما جمع‌آوری مجدد داده ها و اطلاعات و جایگزین کردن آنها کار ساده‌ای نیست و شاید غیرممکن باشد. علاوه بر اینها سرقت داده و اطلاعات ممکن است منجر به انتشار اطلاعات محرمانه شرکت ها و موسسات تجاری آنها شود با توجه به اهمیت اطلاعات برای سازمان‌های لازم است اقدامات امنیتی و کنترلی موثری برای حفاظت از این دارایی ها با ارزش برقرار شود، امروزه اطلاعات مالی وبرنامه ریزی های مالی برای رقبا بسیار با ارزش، و شاید عاملی باشد برای تضعیف قدرت شرکت ها.

۴-۲-۴- ارتباطات:

ارتباطات در شبکه ها ی رایانه ای شکل میگیرد، گسترش روز افزون اتصال رایانه ها به شبکه ها و به ویژه اینترنت جهانی آسیب‌پذیری اطلاعات ذخیره شده در آنها را افزایش می‌دهد و از آنجایی که شبکه‌هایی داخلی و خارجی زیادی توسعه یافته اند، به طبع این توسعه، بستری برای نفوذ کنندگان غیر قانونی به داخل یک سیستم ایجاد شده است ، این سارقین فرصت طلایی برای سرقت سیستم های شبکه ای یافته اند ، نفوذ کننده غیر قانونی اغلب از شبکه ای به شبکه دیگر جهش پیدا می کند و همین امر شناسایی و ردیابی آنها را مشکل می کنند.

۴-۳ - طبقه بندی تقلب های رایانه‌ای:

آشنایی با تقلب ها و انواع آن به مسئولین سازمانی در برقراری کنترل های داخلی مناسب کمک میکند یک روش برای طبقه‌بندی تقلب های رایانه ای استفاده از مدل پردازش داده هاست این مدل بیان می کند که ممکن است تقلب در هر یک از مراحل پردازش داده از ورود ورودی، پردازش اطلاعات، دستورهای رایانه‌ای و ستادها رخ دهد در ادامه به تشریح تقلبها در مراحل مختلف می پردازیم.

۴-۳-۱- تقلب در داده های ورودی:

سهل ترین ومرسوم ترین راه ارتکاب یک تقلب تحریف داده های اولیه و یا ورود داده های غلط به رایانه است برای انجام این نوع تقلب مهارت‌های رایانه ای اندکی لازم است و فقط کافیست فرد متقلب بداند سیستم چگونه کار می کند تا بتواند تقلب را انجام دهد، توجه داشته باشید که به دلیل اتوماسیون بسیاری از فرآیندهای ورود داده هایی که به صورت دستی وارد سیستم می شوند بیشتر در معرض آسیب پذیری و تقلب قرار دارند به عنوان مثال در تقلب دریافت‌های نقدی مبلغ اختلاس با دستکاری داده های ورودی به سیستم پنهان می شود برای مثال فرد متخلف مبالغ فروش های نقدی را به عنوان فروش نسیه در سیستم ثبت می کند و از طریق کلاه به کلاه کردن مانده حسابهای دریافتنی اختلاس خود را مخفی نگه میدارد در تقلب پرداخت‌های نقدی فرد با ایجاد صورت حساب

های تقلبی برای کالاهای خریداری نشـــده از شـــرکت اختلاس می کند همچنین در تقلب موجودی کالا فرد با معرفی موجودی کالا به صورت اقساط شده آنها را از سیستم خود خارج می کند به سرقت می‌برد فردا متولد در تقلب های حقوق و دستمزد با ایجاد کارمندان جعلی و یا نگه داشتن نام یک کارمند بازنشسته در لیست حقوق وجوهی را از شرکت اختلاس می کند همانطور که ملاحظه می کنید تمام این تقلب ها در نبود متنزع ساختن موثر وظایف شـــکل می گیرد به عنوان مثال چنانچه در تقلب دریافت‌های نقدی، تفکیک وظایف دریافت وجوه و ثبت در دفاتر صورت می گرفت شاهد وقوع چنین تقلبی نبودیم و فرد دریافت کننده نمی‌توانست فروش های نقدی را به عنوان فروشـــهای نســـیه ثبت کند به طور کلی تفکیک وظایف، صـــدور مجوزها، ثبت معاملات و نگهداری دارایی‌ها ضرورت دارد .

۴-۳-۲- تقلب پردازشگر:

تقلب رایانه‌ای می‌تواند از طریق استفاده های غیرمجاز از سیستم باشد که شامل سرقت زمان و خدمات رایانه ای انجام شـود منظور از سـرقت زمان خدمات رایانه‌ای، وقت‌کشـی کارمندان و اسـتفاده شـخصـی از خدماتی مانند اینترنت می باشد. حوزه تقلب های رایانه ای بسیار وسیع است و ممکن است که افراد متوجه این موضوع نباشند که عمل انها به نوعی تقلب منجر میشود. به عنوان مثال کارمندی که اقدام به استفاده شخصی از اینترنت سازمان و یا خطوط تلفن شرکت می کند ممکن است متوجه این موضوع باشد که عملا به شرکت و منابع آن خسارت وارد می کند واین موضوع نوعی تقلب محسوب می‌شود.

۴-۳-۳- تقلب برنامه نویسی(دستور رایانه ای):

برخی از تقلب های رایانه ای با دستکاری در برنامه نرم‌افزارهای شرکت ایجاد می شود این عمل ممکن است با طراحی و توسعه برنامه نویسی یک نرم‌افزار جدید همراه باشد برای مثال فرد متقلب می‌تواند با تغییر دادن نرخ سود تضمین شده تعریف شده برای سیستم بانکی مبلغ سود تضمین شده را افزایش داده و مابه التفاوت ایجاد شده را برای خود بردارد این روش تقلب رایانه مستلزم داشتن مهارت خیلی زیاد در برنامه‌نویسی رایانه‌ای است که نمونه آن فراتر از توان بیشتر کاربران معمولی است

۴-۳-۴- تقلب اطلاعات:

اطلاعات تنها برای به کارگیری راه های مجاز توسط اشخاص مجاز استفاده شد بنابراین هر کاربر تنها اجازه دارد اطلاعات را در حدی که مجاز اسـت دریافت و برای دیگرکاربران در قرار دهد. مدیران همواره باید مطلع باشـند که اطلاعات برای یک سازمان دارای اهمیت استراتژیکی می باشد و حفاظت از آن ضرورتی انکارناپذیر است، صرف نظر از نوع تقلب آنچه که مهم است از بین رفتن اطلاعات و خساراتی است که به سازمان وارد می شود. ویژگی جالب تقلب اطلاع دارند که می توانند اطلاعات را نسخه برداری و سرقت کرده بدون اینکه مالک حقیقی اطلاعات آگاهی یابد، مهاجم دیگر می‌تواند به طور غیرمجاز به اطلاعات دسترسی پیدا کند در واقع تقلب رایانه‌ای می‌تواند با تخریب و تغییر فایل های اطلاعاتی شرکت و استفاده بدون مجوز از آنها و یا کپی‌برداری از آنها انجام

شود. محرمانه بودن اطلاعات و دسته بندی آنها را از دسترسی افراد غیر مجاز مصون می‌سازد. حفظ اصالت داده ها منوط به حفظ آنها در برابر هرگونه تغییرات از سوی افراد غیر مجاز است، سرقت و یا نسخه برداری غیر مجاز از اطلاعات محرمانه نوعی تهدید آشکار است که در این مقوله جای می‌گیرد برای مثال کارمندان ناراضی ممکن است اقدام به از بین بردن فایل های اطلاعاتی و حافظه های سخت افزاری شرکت نمایند.

۴-۳-۵- تقلب ستاده: پس از انجام فرایندهای پردازش اطلاعات ستاده سیستم است که به عنوان خروجی مورد توجه مدیران و سایر تصمیم‌گیران قرار می گیرد حفاظت از این ستادها به منظور جلوگیری از انتشار غیرمجاز آنها دارای اهمیت ویژه‌ای است تقلب رایانه‌ای می‌تواند با سرعت و یا استفاده ناصحیح از ستادهای سیستم ایجاد شود کارمندان باید در رابطه با استفاده صحیح از استادها و محافظت از آنها آموزش دیده باشند و غیر ضروری ستادها و به سطل آشغال انداختن این گزارش ها اثر سوء استفاده و تقلب را ایجاد می‌کند برای مثال طراحی یک محصول جدید برای یک خط تولید جدید به عنوان یک ستاره سیستم می باشد که ممکن است با کپی برداری ناماذون توسط فرد متقلب در اختیار قوای شرکت قرار گیرد.

**جدول شماره ۱: طبقه بندی تقلب های رایانه‌ای به همراه مثال دررشته حسابداری.**

| *انواع تقلب رایانه | * ویژگی انواع تقلب ها به تفکیک | | | * نمونه ی تقلب رایانه ای در سیستم حسابداری | * راهکار پیشگیری |
|---|---|---|---|---|---|
| ✓ **تقلب اطلاعات** | ۱- نسخه برداری بدون اطلاع مالک حقیقی | ۲-تخریب و تغییر فایل اطلاعاتی | ۳-از بین رفت اطلاعات و ایجاد خسارت | ✓ برداشت اطلاعات و ابزار های سخت افزاری توسط کارمندان ناراضی | ✓ حفظ محرمان گی و دسته بندی اطلاعات ✓ حفظ اصالت داده ها |
| ✓ **تقلب پردازشگر** | ۱- استفاده غیر مجاز از سیستم | ۲- سرقت زمان | ۳-سرقت خدمات رایانه ای | ✓ استفاده شخصی کارمندان از خطوط تلفن و اینترنت شرکت | ✓ آموزش اخلاق حرفه ای به کارمندان |
| ✓ **تقلب در داده های ورودی** | ۱-سهل و مرسوم | ۲-مهارت رایانه ای اندک | ۳-خطر بیشتر برای داده ها ی دستی | ✓تقلب دریافت نقدی ✓تقلب پرداخت نقدی | ✓ تفکیک وظایف، ✓ صدور مجوزها، ✓ ثبت معاملات ✓ نگهداری دارایی‌ها |
| ✓ **تقلب دستورهای رایانه** | ۱-نیاز به مهارت تخصص زیاد | ۲-غیر قابل انجام برای کارمندان معمولی | ۳- دستکاری و تغییر برنامه نویسی نرم افزار | ✓ تغییر نرخ سود تضمین شده توسط کارمندان بانک ، و سرقت مابه التفاوت | ✓ استخدام برنامه نویسان قابل اعتماد و حرفه ای و وجود برنامه |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | های امنیتی |
| ✓ **تقلب ستاده** | ۱- تقلب اطلاعات خروجی و مهم سیستم مالی | ۲-عدم حفاظت از ستاده ها | ۳-استفاده نادرست کارمندان از ستاده | ✓ به سطل زباله انداختن اطلاعات خروجی و مهم سیستم مالی( اطلاعات محرمانه خط تولید جدید) | ✓ عدم انتشار غیر مجاز اطلاعات ✓ آموزش کارمندان |

منبع:یافته های پژوهشگر

۴-۴- چه افرادی مرتکب جرایم رایانه‌ای میشوند؟

می توان این افراد را در شمار گروهی با استعداد و با هوش سیاه دید یا باید آن را در ردیف بیماران روحی و روانی قلمداد کرد و روانشناسان معتقدند مجرمان رایانه‌ای به دو دسته تقسیم می‌شوند برخی از ان ها از هوش بالایی برخوردار نیستند اما با راهکارهای ساده،یادگیری ا صول کار با رایانه و اینترنت ، یک شبه ره صد ساله را می‌پیمایند دست دوم گروهی با هوش سیاه هستند ،که از استعداد و توانمندی خویش در راه های نادرست استفاده می کنند، رو شهای گوناگونی برای د سته بندی و برر سی مجرمین رایانه‌ای وجود دارد این کار با یک د سته بندی ساده تفاوت دارد زیرا ما در بحث جرایم رایانه‌ای با خیل عظیمی از متخلفان روبرو هستیم که با یک شوخی و تفریح ساده کار خود را شروع و به یک فعالیت تروریستی بین‌المللی به پایان می‌ر سانند مجرمین رایانه‌ای اکثراً از طبقات روشنفکر و تحصیلکرده هستند برعکس سایر مجرمین، آنها قادر به انجام حتی یک جرم ساده مانند سرقت این مشکلات از مغازه نمی باشند اما قادر مبالغ زیادی را با استفاده از روش های رایانه ای به سرقت ببرند انگیزه های مهمی که مرتکبین جرایم رایانه ای را به صورت بسوی ارتکاب جرم سوق می‌دهد گوناگون هستند ولی عمده ترین آنها می تواند برای نشان دادن مهارت سرگرمی و تفریحی به مهارت انتقام‌جویی بیان نقش مجرمانه با شند بر این ا ساس معمولاً انواع مجرمین متخلفان رایانه ای در سه د سته کلی زیر تقسیم بندی می شوند ۱- نفوذ کننده غیرمجاز ۲- مجرمین و ۳- خرابکاران( مرادی و بیات۱۳۹۴ )

## ۵- مقوله های پیشگیری و کشف تقلب های رایانه ای در حسابداری:

در موضوع امنیت و کنترل سیستمهای اطلاعاتی،مبحث فناوری در مقایسه با مدیریت هوشمندانه از اولویت کمتری برخوردار است ، فناوری بستر مناسب را برای کار فراهم می کند اما موضوع اساسی این است که در غیاب خط و مشی های مدیریت هوشمندانه ، بهترین فناوری‌ها نیز در هم شکسته خواهد شد.

امنیت رایانه ها و اطلاعات تنها با مدیریت موثر و سیا ست های امنیتی کارآمد تامین می شود، متا سفانه بسیاری از مدیران به طور کامل از خطر جرایم رایانه و سوء استفاده‌ها ی رایانه‌ای آگاهی لازم و مفید را ندارند ، مدیران

اهداف مربوط به عملیات سازمان را مشخص می نماید و از طریق گزارش ها و رعایت کنترل ها، ریسک هایی که اهداف موسسه را تهدید می‌کند شناسایی و مورد تجزیه و تحلیل قرار می دهد همچنین مدیران سازمان باید هر اقدام احتیاطی را برای حفاظت از سیستم های اطلاعاتی خود به کار بندند.

پس از ارزیابی خطر سازمان می‌تواند اقدامات مشخصی را برای کاهش تقلب و ضرر های ایجاد شده از آن به کار گیرد این اقدامات شامل موارد زیر است:

۱. کاهش احتمال وقوع تقلب گزینه
۲. افزایش دشواری و سختی ارتکاب به تقلب
۳. بهبود شیوه های کشف و شناسایی تقلب
۴. کاهش زیان‌های ناشی از تقلب

مقوله بندی محتوایی چهار گزینه فوق به همراه اجزا ی مربوطه، در جدول شماره دو نگاشته شده است .

**جدول شماره ۲: «مقوله بندی پیشگیری و کشف تقلب های رایانه ای »**

| مقوله های اصلی | ➢شیوه های کاهش احتمال وقوع تقلب | ➢شیوه های سختی ارتکاب به تقلب | ➢روش های بهبود شیوه های کشف تقلب | ➢ شیوه های کاهش زیان های ناشی از تقلب |
|---|---|---|---|---|
| مقوله های فرعی و زیر مجموعه | استفاده از رویه ها و مقررات مناسب برای استخدام و اخراج | طراحی یک سیستم کنترل داخلی قوی | | داشتن پوشش بیمه‌ای کافی |
| | آموزش و مسئولیت کارکنان:<br>آموزش اقدامات امنیتی<br>آموزش افشای تلفنی<br>آگاهی از تقلب<br>رعایت آیین رفتار حرفه‌ای<br>مجازات رفتارهای خلاف آیین رفتار حرفه‌ای | تفکیک مناسب وظایف | اقدامات بازدارنده :<br>تشکیل تیم مدیریت بحران<br>ایجاد یک خط تلفن سری برای کشف تقلب<br>بازبینی فعالیت های سیستم<br>استفاده از نرم افزار کشف تقلب | نگهداری نسخه های پشتیبان<br>طراحی یک طرح اقتضایی<br>استفاده از نرم افزارهای کنترل<br>فعالیت سیستم کشف تقلب |
| | کنترل و رد یابی هدف حق امتیاز استفاده از نرم‌افزار | اجرای برنامه کار شیفتی و چرخشی | اقدامات واکنشی:<br>اجرای حسابرسی های مکرر<br>استفاده از حسابداران کاراگاه | استفاده از قوانین مربوط به منع تقلب و جرایم را یا نه ای در سطح بین المللی |

| | | | | |
|---|---|---|---|---|
| | | محدود کردن د ستر سی به تجهیزات را یانه‌ای و فا یل های اطلاعاتی | | استفاده از پیشنهادات کمیسیون ملی گزارشگری مالی: ایجاد محیط سازمانی که دقت و صحت پردازش گزارشگری مالی را موجب می شود. شناسایی و آگاهی از عوامل ا یجاد کننده گزارشگری مالی متقلبانه. ارزیابی گزارشگری مالی متقلبانه در شرکت طراحی و اجرای کنترل های داخلی به منظور حصول اطمینان منطقی از عدم گزارشگری مالی متقلبانه. |
| | | کد بندی داده ها اطلاعات و برنامه ها | | |
| | | محافظت از کابل های شبکه و خطوط تلفن | | |
| | الزامی کردن امضای قراردادهای محرمانه | محافظت سیستم ها در برابر ویروس ها و مزاحمت ها | | |
| | | کنترل اطلاعات حساس و محرمانه | | |
| | | نمایش اطلاعات ریخته گران | | |
| | | کنترل رایانه های کیفی | | |

منابع : یافته های پژوهشگر

## ۵-۱- شیوه های کاهش احتمال وقوع تقلب:

بزرگترین آسیب پذیری و تهدید در هر سیستم رایانه‌ای متوجه حفاظت رایانه های شخصی است .هکرها و بیشتر سوء استفاده کنندگان و مرتکبین جرایم رایانه‌ای کارمندان همان شرکتی هستند که جرم در آنها اتفاق افتاده است و از کارمندان ممکن ا ست آموزش‌های کافی و منا سب را ندیده با شند و یا به صورت نا شناس اطلاعات مهمی را که در سیستم‌های رایانه‌ای ذخیره شده است را خراب کرده و یا حذف نمایند همچنین ممکن است از سیستم‌های رایانه‌ای برای کارهای شخصی خود و تفریح ا ستفاده کنند و برخی نیز ممکن ا ست، تجهیزات رایانه‌ای را تخریب نمایند در حالی که اکثریت تقلبها توسط کارمندان سابق و فعلی صورت می گیرد اما برخی از مشاوران حرفه ای رایانه معتقدند که موثرترین روش دستیابی به امنیت سیستم اعتماد به صداقت و درستکاری کارمندان شرکت ا ست( تئوری نماندگی رفتاری) حفاظت کارمندان مو ضوع گسترده ا ست که چیزی بیشتر از جلوگیری از جرایم رایانه‌ای را شامل می شود برخی از اقداماتی حیاتی به منظور افزایش صداقت و درستی کارمندان و کاهش احتمال تقلب آنان است بهشرح زیر است.

۵-۱-۱- استفاده از رویه ها و مقررات مناسب برای استخدام و اخراج:

یکی از مهمترین مسئولیت های یک مدیران استخدام ، حفظ و به کارگیری نیروی کار با صلاحیت و در ستکار است بررسی در مورد پیشینه کارمندان اولین خط دفاعی در برابر حفاظت کارمندان می باشد معمولاً سازمان‌ها بررسی های سطحی را در این رابطه انجام می‌دهند میزان بررسی صلاحیت و درستکاری کارمندان اساس آن بستگی به نوع شغل و نوع اطلاعاتی دارد که ممکن است در اختیار فرد قرار گیرد در واقع برای استخدام کسی که قرار است با اطلاعات حساس سروکار داشته باشد بررسی‌های بیشتری برای باید انجام گیرد و با دقت بیشتری باید عمل نموده تحقیقات محلی ممکن است به ما در تعیین اینکه آیا کارمندان قبل از پیوستن به سازمان مشکلاتی را داشتند کمک کند دومین خط دفاعی کنترل رفتار کارمندان است هرچه کارمندان در عملکرد سیستم و یا اطلاعات حساس نزدیک تر باشد کنترل رفتار آنها مهمتر است تغییر در رفتار علامت این است که ممکن است کارمند به کمک نیاز داشته باشد تغییر در وضعیت مالی نیز علامت دیگری است که سرپرستان باید به آن توجه داشته باشند گاهی اوقات مشکلات کارمندان قد وقتی می شود که سازمان باید گام‌هایی را برای حفاظت از خود انجام دهد چنانچه تهدید اساسی بروز نماید ممکن است سازمان اقدام به اخراج کارمند خاطی نماید شرکت‌ها باید هنگام اخراج کارمندان خود خیلی مواظب باشند ارتباط کارمندان اخراجی باید به سرعت با شغل های حساس قطع شود به منظور پیشگیری از خرابکاری های نسخه برداری از داده‌ها و اطلاعات محرمانه قبل از ترک شرکت آنها را از دسترسی به سیستم رایانه‌ای منع کرد.

| ➢ جدول شماره ۳: استفاده از رویه ها و مقررات مناسب برای استخدام و اخراج | | | |
|---|---|---|---|
| ➢ «کارمندان استخدام شده» | | ➢ «کارمندان اخراج شده » | |
| **خطوط دفاعی در برابر حفاظت کارکنان:** | **عوامل موثر:** | **خطوط دفاعی در برابر کارمندان اخراجی:** | **عوامل موثر:** |
| ۱- میزان بررسی صلاحیت و درستکاری | • نوع شغل<br>• نوع اطلاعات در دسترس | ۱- قطع ارتباط کارمند اخراجی با شغل حساس | • منع از ارتباط با رایانه ها و دادهها |
| ۲-کنترل رفتار کارمندان | • تغییر در رفتار<br>• تغییر وضعیت مالی | ۲- نسخه برداری از داده هاو پیشگیری از خرابکاری | • قبل از ترک کارمند اخراجی از شرکت نسخه برداری صورت گیرد. |

منبع: یافته های پژوهشگر

۵-۱-۲- آموزش و مسئولیت کارمندان:

آموزش کاربران درباره اهمیت جرایم رایانه‌ای و هزینه‌هایی که به سازمان تحمیل می شود نقش مهمی در پیشگیری از جرایم رایانه‌ای دارد ابتدا باید کارمندان را نسبت به عملکرد اصلی سیستم آموزش داد و این نکته را

پذیرفت که تمامی وقایع امنیتی ناشی از کینه‌توزی نیست در برخی مواقع به دلیل آموزش نامناسب کارمند اشتباه‌های در استفاده از سیستم صورت می گیرد همچنین کارمندان باید بدانند که مسئول اعمال خود بوده و هرگونه استفاده از منابع رایانه سازمان مسئولیت آور است، آنها باید بدانند که تنها مسئول استفاده از این منابع می باشند و برای حفظ آنها در مقابل مهاجمان نیز مسئولیت دارند.

سازمان ، به منظور کاهش احتمال وقوع تقلب شرکت باید کارکنان خود را در حوزه‌های زیر آموزش و تعلیم دهد:

۵-۱-۳- اقدامات امنیتی :

کارمندان باید در زمینه اقدامات امنیتی به خوبی آموزش داده شوند اهمیت اقدامات امنیتی را بدانند و برای اجرای جدی آن تشویق شوند

- افشای تلفنی: باید به کارمندان آموزش داده شود که بدون آگاهی و اطمینان از ایمن بودن خطوط تلفن اطلاعات محرمانه را از طریق تلفن ارسال نکنند، آنان باید اهمیت امنیت خطوط را درک نمایند

- آگاهی از تقلب: کارمندان باید تقلب های رایج و متداول و خطرات آنها را بشناسند آنان باید بیاموزند چرا بعضی از افراد مرتکب تقلب می شوند و چگونه می تواند تقویت قلب پیشگیری آن را کشف کرد

- رعایت آیین رفتار حرفه‌ای: شرکت باید استانداردهای آیین رفتار حرفه‌ای را در فعالیت ها و دستورالعمل های خود ترویج کند تا کارمندان از مشکلات ناشی از زدن رعایت آن آگاه شوند.

-مجازات رفتارهای خلاف آیین رفتار حرفه‌ای: کارمندان باید عواقب رفتارهای خلاف آیین رفتار حرفه‌ای آگاه شوند البته این موضوع نباید یک تهدید باشد بلکه باید به عنوان نتیجه خلاف آیین رفتار حرفه‌ای مطرح شود.

۵-۱-۴- کنترل و ردیابی هدف حق امتیاز استفاده از نرم‌افزار:

مدیریت شرکت باید به منظور جلوگیری از طرح دعوی علیه شرکت در رابطه با تکثیر غیر مجاز نرم‌افزارها در چهارچوب حق امتیاز نرم‌افزارهای خریداری شده اقدام کند در این زمینه باید از کافی بودن امتیاز استفاده از نرم افزار با توجه به تعداد کارمندان و نیازهای آنها و همچنین عدم وجود کار برم آزادتیران حاصل نمایند طرح چنین مباحثی باعث می‌شود که شرکت با توجه به نیازهای اقدام به خرید حق امتیاز استفاده از نرم‌افزار کند و انجام هزینه های اضافه در این زمینه خودداری کنند.

۵-۱-۵- الزامی کردن امضای قراردادهای محرمانه:

در رابطه با محرمانه نگه داشتن اطلاعات شرکت و عدم افشای آن با تعهداتی از کارمندان که به این اطلاعات دسترسی دارند گرفته شود امضای قراردادهای که برای کارمندان تعهداتی را ایجاد می کند می تواند روش مناسبی برای جلوگیری از شکل‌گیری تقلب افشای اطلاعات محرمانه باشد.

## ۵-۲- افزایش دشواری و سختی ارتکاب به تقلب:

یک راه برای پیشگیری از تقلب برقراری روش های صحیح می‌تواند مجرمین رایانه‌ای را از ارتکاب جرم بازدارد برای این منظور طراحی یک سیستم با کنترلهای کافی امکان تقلب را برای شخص متقلب مشکل می سازد بیشتر متخصصان بر این باورند که امنیت رایانه و مدیریت موثر و برقراری سیاست های امنیتی آغاز می‌شود متاسفانه بسیاری از مدیران به طور کامل از خطرات جرایم رایانه‌ای استفاده و کلاهبرداری هایی که متوجه سازمان است آگاهی ندارد حفاظت رایانه ها تنها در صورتی موثر است که مدیر سازمان اهمیت جرایم رایانه ای را جدی بگیرد یک سیاست کنترلی مناسب را برای توقف و یا حداقل کاهش جرایم رایانه اجرا کند

به منظور تهیه یک برنامه عملیاتی و طرح طراحی یک سیستم کنترل داخلی قوی باید مانند یک مجرم رایانه ای فکر کنید و به این سوالات پاسخ دهید که:

انگیزه هایی برای نفوذ به یک هدف خاص دارید؟

برای تهاجم به هدف خاص نیاز به چه مهارت هایی است؟

چه اطلاعاتی ممکن است برای شما اهمیت داشته باشد؟

چگونه می توان به این اطلاعات دست یافت؟

مسئولیت امنیت و کفایت یک سیستم کنترل داخلی با مدیریت ارشد سازمان است البته مدیران معمولاً این کار را به تحلیلگران طراحان و کاربران نهایی واگذار می‌کنند این موضوع نیز اهمیت دارد که اطمینان حاصل شود که کنترل های داخلی تعطیلات پایان سال نیز به دقت به اجرا در می آید بر اساس تحقیقات بخش قابل توجهی از تقلب های رایانه‌ای در طول تعطیلات اتفاق می‌افتد در ادامه برخی دیگر روشهای که ارتکاب تقلب را دشوار می‌کند معرفی می‌شود

۵-۲-۱- تفکیک مناسب وظایف:

بزرگ کردن وظایف و فعالیتهای ناسازگار می‌توان از بروز برخی از تقلب و سوءاستفاده‌ها پیشگیری نمود اگر وظایف با دقت و صحت جداسازی شوند باعث می شود که یک نفر نمی‌تواند به تنهایی انجام تمام مراحل یک کار را به عهده بگیرد تفکیک وظایف به خصوص در رابطه با مسئولیت‌های صدور مجوز معاملات ثبت معاملات و نگهداری داراییهای اهمیت ویژه‌ای دارد

۵-۲-۲- اجرای برنامه کار شیفتی و چرخشی:

چرخشی مسئولیتها همانند لزوم مرخصی به آشکار کردن تقلب و جرایم کمک می‌کند چرا که مسئولیت یعنی جابجایی تصادفی افراد در شغل ها برخی از طرح های تقلب مانند کلاه به کلاه کردن به زمان زیاد و کنترل مستمر به منظور جلوگیری از افشای آن نیاز دارد چنانچه تکالیف و وظایف کارمندان را در مقاطع زمانی نامشخص به طور چرخشی تغییر دهیم امکان شناسایی برخی از این تقلب ها به وجود می‌آید

۵-۲-۳- محدود کردن دسترسی به تجهیزات رایانه‌ای و فایل های اطلاعاتی:

درس فیزیک اختیار باید دقت شود د ستر سی به رایانه ها اطلاعات طبقه بندی شده محدود با شد با محدود کردن این دسترسی ها به تجهیزات رایانه ای و فایل های اطلاعاتی می توانیم تقلب رایانه‌ای را به صورت چشمگیری کاهش دهیم

کد بندی داده ها اطلاعات و برنامه ها:

یکی از شیوه های محدود نمودن دسترسی افراد به اطلاعات محرمانه رمزنگاری و به صورت رمز درآوردن اطلاعات میبا شد رمزنگاری داده‌ها و اطلاعات به ویژه در شبکه‌های رایانه‌ای در انتقال اطلاعات ضرورت دارد در این فرآیند اطلاعات و یا محتویات یک متن ساده به اطلاعات و متون رمزی تبدیل می‌شود و بدون کدگشایی داده های مزبور برای دیگران بی‌معنی و غیرقابل فهم است

۵-۲-۴- محافظت از کابل های شبکه و خطوط تلفن:

کابل های حامله داده ها در برابر تهدیدها بسیار آسیب پذیرند کابل و خطوط ارتباطی از جمله خطوط تلفن به راحتی قابل شما هستند با قطع سیم یک شبکه به راحتی در بخشی از آن اختلال ایجاد می شود همچنین نفوذگران از طریق این خطوط ارتباطی اقدام به انتقال ویروس دستیابی به سیستم سرقت از بین بردن داده و اطلاعات می کنند بنابراین محافظت از کابل های شبکه خطوط ارتباطی بسیار بسیار حائز اهمیت است

۵-۲-۵- محافظت سیستم ها در برابر ویروس ها و مزاحمت ها:

اتصال به شبکه ها و مبادلات اطلاعات بدون حفاظت در برابر بدافزارها و مزاحمان بسیار خطرناک است دیواره‌های آتش سیستم های تشخیص مزاحمت و نرم افزارهای ضد ویروس امروز به یکی از ابزارهای حیاتی برای هر کسب و کار تبدیل شده است

در مورد سیستم های تشخیص مزاحمت باید گفت که این سیستم ها با نصب ابزارهای نظارت تمام وقت در آسیب پذیرترین نقاط شبکه‌های سازمان مزاحمان را شناسایی ترک می کند این سیستمها در صورت وجود با رویدادهای مشکوک غیرعادی به کاربر هشدار می‌دهند

به کارگیری نرم افزارهای ضد ویروس برای هر رایانه باید در تمامی برنامه‌های تدافعی و حفاظتی شخصی و سازمانی قرار گیرد نرم افزار ضد ویروس سیستم ها و درایوهای رایانه‌ای را از لحاظ وجود ویروس ها بررسی می کند این نرم‌افزار معمولاً نواحی آلوده را از وجود هرگونه ویروس پاکسازی می کند اما باید توجه داشت که بسیاری از این نرم‌افزارها تنها در برابر ویروس‌های موثر هستند که تا زمان عرضه آنها نوشته و منتشر شدند به همین دلیل برای حفظ اثربخشی نرم افزار ضد ویروس باید آنها را به صورت مرتب به هنگام کرد

استفاده از هر یک از این سیستم ها و برنامه های اشاره شده در بالا و احتمال وقوع تقلب را کاهش داده و در واقع مانعی برای نفوذ متقلبین به سیستم است

۵-۲-۶- کنترل اطلاعات حساس و محرمانه:

سازمان باید اطلاعات خود را از نظر اهمیت و محرمانه بودن طبقه بندی کند و متناسب با هر طبقه محدودیت های د ستر سی متنا سب با آنها را اعمال نماید اطلاعات حساس و محرمانه باید در یک مکان قفل شده نگهداری شوند رایانه ها باید در هنگام عدم استفاده خاموش و قفل شوند همچنین شرکت نماید همه داده و اطلاعات خود را در یک مکان نگهداری کنند و یا به یک کارمند اجازه دسترسی به همه آنها را بدهند شبکه‌های محلی می تواند از یک سرویس دهنده اختصاصی استفاده کنند اجازه دریافت داده ها و اطلاعات را می‌دهد اما اجازه وارد کردن داده ها به منظور جلوگیری از ورود ویروس ها و کرم ها به آن می‌دهد و اعمال این کنترل ها امکان تقلب و سوء استفاده از این اطلاعات حساس کاهش می یابد

۵-۲-۷- نمایش اطلاعات ریخته گران:

متا سفانه کتب ووب سایت های زیادی اطلاعات درباره چگونگی ورود غیرمجاز به سیستم ها آموزش می دهند بازبینی مشاهده این سایت ها و پیدا کردن مقاله هایی که به سیستم مورد ا ستفاده شرکت مربوطه ا ست از اهمیت ا سا سی برخوردار ا ست زیرا موجب شنا سایی روش های مورد ا ستفاده تو سط رخنه گران و به کارگیری اقدامات حفاظتی در مقابل حملات آنان می‌شود .( کیانخواه ۱۳۸۹)، ( مرادی و بیات ۱۳۹۴)

۵-۲-۸- کنترل رایانه های کیفی:

با توجه به امکان جابجایی رایانه های کیفی انتقال آنها به هر مکانی باید مراقبت‌های ویژه از این رایانه ها به عمل آید برخی از این روش های کنترل عبارتند از:

_ آشنایی کاربران با خاطراتی که متوجه رایانه‌های کیفیت و آگاهی آنان از اهمیت اطلاعات درون آن ها روشی مناسب برای اعمال اقدامات کنترلی توسط کارمندان است.

_ ایجاد رویه ها و مقرراتی برای کنترل رایانه های کیفی و ملزم کردن کاربران برای تهیه نسخه های پشتیبان از داده ها و اطلاعات نیز روشی برای کنترل این رایانه ها می باشد.

_ نام و آرم شرکت بر روی رایانه ها حک شود.

_ برای محافظت از اطلاعات درون رایانه ها راه اندازی بدون کلمه عبور غیر ممکن با شد همچنین این سیستم باید به گونه ای تنظیم شود که پس از چند بار ورود کلمه عبور اشتباه سیستم قطع شود و دیگر پاسخ ندهد.

_ داده‌ها و اطلاعات درون رایانه نیز با فناوری رمزگذاری کدبندی شوند.

_ نصب تجهیزات بر روی رایانه ها که در صورت جابجایی رایانه آژیر بکشد.

_ نصب نرم افزاری که در زمان های معین محل رایانه را به اطلاع صاحب خود برساند استفاده از برچسب های rfid بر روی رایانه های کیفی می‌تواند در جلوگیری از خروج و سرقت رایانه از شرکت موثر باشد.

_ ذخیره اطلاعات محرمانه در یک حافظه جانبی و در حافظه رایانه نیز روش مناسبی برای پیشگیری از سوء استفاده از اطلاعات درون رایانه ای است. (مرادی و بیات ۱۳۹۴)

## ۵-۳- بهبود روشهای کشف و تقلب رایانه‌ای:

سومین گام برای پیشگیری و کشف تقلب های رایانه‌ای بازنگری و بهبود در روشهای کشف و تقلب از شناسایی تقلب های رایانه‌ای با اتخاذ تدابیر خاص میسر می‌شود برخی از این تدابیر پرهزینه و بسیار تخصصی و برخی دیگر ساده و کم هزینه هستند به طور کلی این اقدامات را می‌توان دو مقوله کلی اقدامات بازدارنده و اقدامات واکنشی تقسیم کرد.

۵-۳-۱ - اقدامات بازدارنده:

اقدامات بازدارنده به منظور شناسایی جرایم در حال وقوع و یا پیش از وقوع انجام می‌شود نرم‌افزارهای موجود است که مشابه سیستم های دزدگیر عمل می‌نمایند و کاربر را پیش از هرگونه عملیات مجرمانه مطلع می سازند در ادامه برخی از اقدامات بازدارنده در وقوع تقلب معرفی می شود.

۵-۳-۱-۱ تشکیل تیم مدیریت بحران:

برخورد با جرایم رایانه‌ای نیاز به یک گروه و تیم متخصص دارد سازماندهی این تیم باید پیش از وقوع جرایم صورت گیرد زیرا پس از وقوع جرم دیگر فرصت تشکیل چنین تیمی نیست، بیش از بروز هرگونه حادثه باید افراد تیم و عملکرد آنها مشخص شود، تیم مزبور شامل افراد مستقل و بخش‌هایی است که در ایجاد، نگهداری و دستر سی به اطلاعات نقش دارند هدایت تیم مدیریت بحران و نحوه مقابله با جرایم رایانه‌ای با مدیریت سیستم است چرا که توانایی ارزیابی و محاسبه ارزش واقعی اطلاعات به مخاطره افتاده و آثار آن را در سازمان دارد، بسیاری از شرکت‌ها برای آزمایش و ارزیابی روشهای امنیتی و سیستمهای رایانه خود از مشاوران فنی رایانه استفاده می‌کنند اما برخی شرکت‌ها برای استفاده از این افراد تمایلی نشان نمی دهند زیرا نمی‌خواهند بپذیرند که سیستم اطلاعاتی شرکت ممکن است هر لحظه در مقابل نفوذ تجاوزگران و حملات رایانه‌ای شکست بخورد .(مرادی و بیات ۱۳۹۴)

۵-۳-۱-۲- ایجاد یک خط تلفن سری برای کشف تقلب:

کارکنان ممکن است بین تعهد نسبت به شرکت و طرد شدن از طرف دوستان درشت و دودلی قرار گیرند در واقع آنها از یک طرف خود را نسبت به شرکت حفاظت از دارایی‌های آن مسئول می داند و از طرف دیگر از دادن دیگران ناراحت هستند و ترجیح می‌دهد سکوت کند یک روش برای برطرف کردن این شک استفاده از کانال‌های است که افراد بتوانند مدیریت را از حالت های مشهور آگاه سازند ایجاد خطوط تلفن سری به همین منظور از تا کارکنان بتوانند به صورت ناشناس تقلب هایی را که در حال رخ دادن هستند را گزارش کنند البته مشکل بالقوه این خطوط این است که ممکن است کارکنان فعالیت های مربوط به تقلب را به کسانی گزارش کند که خود در تقلب مدیریت ارشد سهیم هستند البته این تهدید با استفاده از خطوط ایجاد شده توسط یک سازمان یا شرکت تجاری مستقل برطرف می شود نقطه ظرفیت خطوط تلفن سری این است که ممکن است تعدادی از این مکالمات ارزش پیگیری نداشته باشند در واقع برخی از آنها با نیت انتخاب جویانه و یا سرکار گذاشتن مدیریت صورت گرفته باشد.

۵-۳-۱-۳- بازبینی فعالیت های سیستم:

کلیه فعالیتهای سیستم باید در دفتر یادداشت روزانه ثبت شود این دفتر باید نشان دهد چه کسی چه زمانی از کدام ترمینال به چه اطلاعاتی دسترسی پیدا کرده است این دفاتر باید به طور مداوم به منظور بازبینی فعالیت سیستم و ردیابی هر مشکلی تا منشاء آن بررسی شود البته نرم‌افزارهای وجود دارد که نقاط ضعف و قوت سیستم را ارزیابی و سپس گزارش های حاوی نقاط ضعف روش های اصلاحی پیشنهادی را ارائه می کند.

۵-۳-۱-۴ استفاده از نرم افزار کشف تقلب:

افراد متخلف برای اینکه توجه دیگران به فعالیتشان جذب نشود، از الگوی خاصی برای ارتکاب تقلب استفاده می کنند این الگو در نرم‌افزارهای کشف تقلب طراحی شده است ( کیان خواه ۱۳۸۹)، در واقع با این نرم افزارها می‌توان به روندهای غیرعادی در حسابها ، افزایش بیش از حدیاکاهش یکباره آنها و سایر موارد مشکوک پی برد و این موارد را پیگیری کرد در برخی از موارد با توجه به حساسیت موضوع از شبکه های عصبی که مانند مغز انسان رفتار می کند در شناسایی کشف تقلب استفاده می شود این نرم افزارها بسیار دقیق هستند و توانایی پیش بینی رفتار یک مجرم را دارند برای مثال برای پیگیری سرقت مبالغی از کارت های اعتباری مختلف می توانند از این سیستم برای شناسایی کارت های اعتباری که در معرض خطر و سرقت بعدی هستند استفاده کرد.

۵-۳-۲- اقدامات واکنشی:

این طراحی به منظور شناسایی جرایم در حال وقوع و جرایمی که صورت پذیرفتند اتخاذ می‌شود این اقدامات شامل اجرای حسابرسی مکررو استفاده از حسابداران کارآگاه می باشد که در ادامه درباره آنها توضیحاتی را ارائه می کنیم.

۵-۳-۲-۱- اجرای حسابرسی های مکررو مداوم :

برای افزایش احتمال کشف تقلب باید از حسابر سی مستقل و داخلی ا ستفاده کرد، حسابر سان باید به طور منظم کنترل‌های سیستم را آزمون کرده و به صورت ادواری به منظور پیدا کردن فعالیت های مشکوک فعالیت‌های داده را بررسی کنند اما این کار نباید باعث شود که کارکنان احساس کند حریم خصوصی آنها نقض می‌شود باید کارکنان را توجیه کرد این بررسی و پاییدن تصادفی حسابرسان تنها به حل موضوعات محرمانه کمک کرده بلکه بازدارندگی مهمی بر روی تقلب های رایانه ای ایجاد می کند.(مرادی و بیات ۱۳۹۴)

۵-۳-۲-۲- استفاده از حسابداران کاراگاه:

حسابداران کارآگاه تخصص ویژه در بازر سی و حسابر سی دارند این افراد دارای مدارج بالایی در حسابداری هستند و گواهینامه بازرس رسمی تقلب را دارا می با شند ا ستفاده از چنین افرادی و با چنین تخصصی در کشف پیشگیری یک تقلب بسیار مفید می باشد امروزه بیش از ۱۵ هزار بازرس رسمی تقلب در جهان مشغول به کار هستند که با توجه به روند رو به رشد انواع تقلب ها و جرایم رایانه‌ای تعداد این افراد متخصص نیز در حال افزایش

ا ست با توجه به گسترش ا ستفاده از سیستم‌های اطلاعاتی رایانه ای در ایران و به تبع آن افزایش جرایم رایانه ای استفاده از حسابداران کاراگاه نیز بیشتر از پیش احساس می شود.

۵-۴- شیوه های کاهش خسارت های تقلب رایانه‌ای:

آخرین راهکار به منظور پیشگیری و کسب تقلب های رایانه ای استفاده از روش هایی برای کاهش خسارات تقلب های رایانه ای است، (آسترکی ۱۳۸۸) که در واقع با وجود تمام تلاش‌هایی که برای پیشگیری و کاهش احتمال وقوع تقلب صورت می گیرد همواره احتمال وقوع تقلب در یک سازمان وجود دارد به همین منظور باید اقداماتی برای کاهش زیان ناشی از تقلب ها صورت گیرد برخی اقدامات مذکور عبارتند از:

۵-۴-۱- داشتن پوشش بیمه‌ای کافی:

در صورت وقوع یک جرم رایانه‌ای باید اطلاعات جمع‌آوری شده در اختیار شرکت بیمه قرار گیرد، نکاتی که شرکت بیمه به آن نیاز دارد عبارتند از ترتیب زمان وقوع جرم ،معرفی مظنونین و میزان خسارت اقداماتی که سازمان زیادی قبل و یا در هنگام وقوع جرم و حتی پس از آن انجام می دهند بر میزان مبلغ کسر شرکت بیمه پرداخت می‌شود تاثیر دارد.(مرادی و بیات ۱۳۹۴)

۵-۴-۲- نگهداری نسخه های پشتیبان:

روش دیگری که برای کاهش خسارت تقلب و جرایم رایانه ای می توان به کار برد تهیه نسخه های پشتیبان از داده ها و اطلاعات است ( آسترکی ۱۳۸۸)، با این کار در صورت از بین رفتن اطلاعات توسط مجرمان رایانه دیگر نگران از د ست دادن آنها نباید بود و روش های مختلفی مانند پشتیبان گیری آنلاین و یا ذخیره اطلاعات در حافظه های جانبی در این زمینه موثر است درباره انواع روش های پشتیبان گیر در فصل ده صحبت شده است.(مرادی و بیات ۱۳۹۴)( کیان خواه ۱۳۸۹)

۵-۴-۳- طراحی یک طرح اقتضایی:

به منظور کاهش خسارت تقلب های رایانه ای لازم ا ست از قبل برنامه طراحی شود که در آن تمهیداتی پیش‌بینی گردد تا در صورت وقوع سوء استفاده و تقلب اقدامات لازم برای حفظ و بقای شرکت انجام شود برنامه مدیریت خطر تقلب باید به عنوان بخشی از ساختار رهبری شرکت تدوین شود و شامل خط مشی های مکتوب برای برآوردن انتظارات هیئت مدیره و مدیریت ارشد برای اداره خطر تقلب باشد برای مثال چنانچه اطلاعات و داده های شرکت از بین رفت سریع از نسخه های پشتیبان از قبل تهیه شده است برای برگرداندن وضعیت به حالت سابق استفاده شود.(مرادی وبیات۱۳۹۴)

۵-۴-۴- استفاده از نرم افزارهای کنترل فعالیت سیستم کشف تقلب:

امروز نرم‌افزارهای طراحی شده اند که قادرند تمامی فعالیت های کاربران را هر لحظه ثبت نمایند این امکان را به مدیریت می دهد تا در صورت بروز تقلب با سرعت آنها را کشف کند و جلوی خسارتهای بعدی را بگیرد در واقع استفاده از چنین نرم‌افزارهای به شرکت کمک می کند تا در صورت وقوع تقلب نواحی آسیب دیده به سرعت

شناسایی و ترمیم شوند(کیان خواه۱۳۸۹)، علاوه بر نرم‌افزارهای ثبت فعالیت نرم افزارهای هوشمند به منظور کشف تقلب وجود دارند که فعالیت کاربران را بررسی و تحلیل می کند و هرگونه اقدام غیر معمول و مشکوکی را به اطلاع مدیران شرکت می‌رسانند برای مثال حذف اطلاعات مربوط به فایل مشتریان اقدام غیر معمول است که چنانچه این کار توسط کاربر انجام شود سریعا به اطلاع مدیران می‌رسد. (آسترکی و همکاران۱۳۸۳)

۵-۴-۵- قوانین مربوط به منع تقلب و جرایم رایانه ای در سطح بین الملل:

دادگستری ایالات متحده آمریکا تقلب رایانه‌ای را هر عمل غیرقانونی که دانش فناوری رایانه‌ای لازمه ارتکاب، رسیدگی و تعقیب قانونی آن باشد معرفی کرده است ،قانون سوء استفاده رایانه‌ای که در سال ۱۹۸۶ تاسیس شده است قانونی است اکثراً جرایم رایانه ای را کنترل می کند و علاوه بر این دولت فدرال ایالات متحده قوانینی را نیز برای پیشگیری جرایم رایانه‌ای ارایه کرده است این قوانین شامل مواردی مانند استفاده متقلبانه از کارت‌های اعتباری، نسخه‌برداری های غیرقانونی، کپی رایت، آیین دادرسی مجرمین و جرایمی مانند اختلاس و سرقت اموال و دارایی‌ها، جاسوسی، کلاهبرداری وحمله به دارایی‌های دولتی، خرابکاری، استراق سمع و غیره می باشد.

و اما کمیسیون ملی گزارشگری مالی متقلبانه، گزارشگری مالی متقلبانه را مجموعه اقداماتی برای حذف و یا ارائه نادرست و گمراه کننده صورت مالی تعریف کرده است ،کسانی که اقدام به گزارشگری متقلبانه می کنند قطعاً منافع مالی غیرمستقیمی را به دست می‌آورند این منافع شامل افزایش قیمت سهام ، بهبود وضعیت نقدینگی شرکت، حفظ مقام و منصب ، دریافت پاداش و ترفیع شغلی می باشد این کمیسیون به منظور جلوگیری و کاهش احتمال گزارشگری متقلبانه ۴ پیشنهاد به شرح زیر ارائه کرده است:

۱) ایجاد محیط سازمانی که دقت و صحت پردازش گزارشگری مالی را موجب می شود

۲) شناسایی و آگاهی از عوامل ایجاد کننده گزارشگری مالی متقلبانه

۳) ارزیابی ۲۰ گزارشگری مالی متقلبانه در شرکت

۴) طراحی و اجرای کنترل های داخلی به منظور حصول اطمینان منطقی از عدم گزارشگری مالی متقلبانه(آسترکی و همکاران ۱۳۸۳)

## نتیجه گیری و پیشنهاد:

اعمال متقلبانه شامل دروغ گفتن، کتمان حقیقت ، حقه بازی و فریبکاری است و اغلب ناشی از تخطی از اعتماد و امانت داری است . تقلب می تواند توسط یک نفر در داخل سازمان یا گروه‌های برون سازمانی انجام شود ، (یکاو و همکارانئ۱۳۸۳)، پس از انجام فرایندهای پردازش اطلاعات ستاده سیستم است که به عنوان خروجی مورد توجه مدیران و سایر تصمیم‌گیران قرار می گیرد حفاظت از این ستادها به منظور جلوگیری از انتشار غیرمجاز آنها دارای اهمیت ویژه‌ای است، تقلب رایانه‌ای می‌تواند با سرعت و یا استفاده ناصحیح از ستادهای سیستم ایجاد شود ستاده ها همان اطلاعات است( مرادی و بیات ۱۳۹۴) انواع مختلفی از تهدیدها متوجه اصالت

[۱۶] Computer Abuse

طبقه‌بندی اطلاعات و داده های سازمان می باشد، همچنین در دنیای تجارت امروز رسیدن به موفقیت بدون سرمایه گذاری در نرم‌افزارهای رایانه‌ای امکان‌پذیر نیست.(کیان خواه ۱۳۸۹)، نتایج حا صل از پژوهش شامل ۳ جدول ا ست که در قسمت یافته ها بیان شده ا ست. درجدول شماره ۱ طبقه بندی تقلب های رایانه‌ای بیان شده ا ست که شامل ۵ مورد ا ست: ۱- تقلب اطلاعات۲_ تقلب پرداز شگران۳_ تقلب در داده های ورودی۴- تقلب دستورهای رایانه‌ای۵_ تقلب ستاده همچنین ویژگی های هر نوع تقلب مشخص و از هر نوع نمونه ای در سیستم حسابداری بیان شده ا ست، در جدول شماره دو مقوله بندی پیشگیری و کشف تقلب های رایانه‌ای بیان شده است در این طبقه بندی، مقوله های اصلی شامل چهار فاکتور تحت عناوین، ۱- شیوه‌های کاهش احتمال وقوع تقلب ۲- شیوه‌های سختی ارتکاب به تقلب ۳- روش های بهبود شیوه های کشف تقلب و۴- شیوه‌های کاهش زیان‌های ناشی از تقلب طبقه بندی شده است با استفاده از کتب و منابع مشخص از طریق تحلیل محتوا زیرشاخه‌های مقوله های اصلی مورد بررسی قرار گرفته ،شیوه های کاهش احتمال وقوع تقلب شامل۱- استفاده از رویه ها و مقررات ۲- آموزش و مسئولیت کارکنان شامل آموزش اقدامات امنیتی، آموزش های تلفنی، آگاهی از تقلب رعایت آیین رفتار حرفه ای ، مجازات رفتارهای خلاف آیین رفتار حرفه ای و کنترل و ردیابی هدف حق امتیاز استفاده از نرم‌افزار و در نهایت الزامی کردن امضای قراردادهای محرمانه دومین مورد شیوه های سختی ارتکاب به تقلب ا ست که شامل۱- طراحی یک سیستم کنترل داخلی قوی ۲- تفکیک منا سب وظایف ۳-اجرای برنامه کار شیفتی و چرخشی ۴- محدود کردن دسترسی به تجهیزات رایانه‌ای و فایل های اطلاعاتی۵- طبقه بندی داده های اطلاعات و برنامه ها۶- محافظت از کابلهای شبکه و خطوط تلفن۷- محافظت سیستم ها در برابر ویروس ها و مزاحمت ها ۸-کنترل اطلاعات حساس و محرمانه۹- نمایش اطلاعات ریخته گران۱۰- کنترل رایانه های کیفی، سومین گزینه روش های بهبود شیوه های کشف تقلب است که شامل اقدامات بازدارنده مانند تشکیل تیم مدیریت بحران و ایجاد یک خط تلفن سری برای کشف تقلب و استفاده از نرم افزار کشف تقلب و اقدامات واکنشی شامل اجرای حسابرسی های مکرر و استفاده از حسابداران کاراگاه، چهارمین مورد شیوه‌های کاهش زیان‌های ناشی از تقلب که شامل مواردی چون ۱- داشتن پوشش بیمه ۲- نگهداری نسخه های پشتیبان ۳- طراحی طرح اقتضایی۴- استفاده از نرم افزارهای کنترل فعالیت سیستم کشف تقلب۵- استفاده از قوانین منتقل و جرایم در سطح بین‌الملل و استفاده از پیشنهادات کمیسیون ملی گزارشگری مالی که دقت و صحت پردازش گزارش را موجب می شود و شناسایی آگاهی از عوامل ایجاد کننده گزارشگری مالی متقلبانه را سهولت بخشد. جدول شماره ۳ مقوله بندی استفاده از رویه ها و مقررات مناسب برای استخدام و اخراج کارکنان را طبقه‌بندی کرده است در ارتباط با کارمندان استخدام شده خطوط دفاعی شامل میزان بررسی صلاحیت و درستکاری و کنترل رفتار کارمندان است و عوامل موثر بر این مقوله۱- نوع شغل ۲- اطلاعات در دسترس۳- تغییر در رفتار و تغییر در وضعیت مالی است و اما خطوط دفاعی مقابل کارمندان اخراج شده شامل قطع ارتباط کارمندان اخراجی با شغل حساس و نسخه برداری از داده و پیشگیری از خرابکاری است و با عوامل

موثر بر این مقوله شامل منع ارتباط با رایانه ها و داده ها قبل از ترک کارمند اخراجی از شرکت ونسخه‌برداری است. مقوله بندی جرایم رایانه ای و راه های پیشگیری آن در حسابداری که در پژوهش حاضر انجام گرفته است، میتواند برای افراد ذینفع شامل مدیران به منظور نظارت و کنترل دقیقتر ، سرمایه گذاران به منظور افزایش اعتماد به شرکت ، پژوهشگران به منظور دستیابی به پرسشنامه های مناسب جهت انجام پژوهش های تجربی ، استاندارد گذاران به منظور تعیین استاندارد های مناسب برای کاهش و جلوگیری از تقلب رایانه ای ، ودر نهایت نهاد های ناظر جهت کشف و پیشگیری از تقلب رایانه ای مفید واقع گردد.

**منابع:**


۱. کیان خواه، احسان، ۱۳۸۹، مدیریت امنیت اطلاعات تهران انتشارات ناقوس

۲. یکاو، دیوید جی،سیگر،کارل ای و استروج، ویلیام ار وان ، (۱۳۸۳)، راهکارهای پیشگیری و مقابله با جرایم رایانه‌ای، ترجمه اکبر آسترکی، تورج ریحانی، محمد صادق روزبهانی، راحله الیاسی، تهران انتشارات دانشگاه علوم انتظامی

۳. مرادی ، مهدی و نعیمه، بیات، سیستم های اطلاعاتی حسابداری،انتشارات مرندیز،ویراست چهارم ، فصل ۶ و ۷

۴. محمودی، محمد، ،۱۳۹۱، سیستمهای اطلاعاتی در مدیریت ،چاپ سوم، تهران، انتشارات دانشگاه تهران

۵. مقدسی، علیرضا، ۱۳۸۶، سیستمهای اطلاعاتی مدیریت، مشهد انتشارات جهان فرد

۶. روحانی رانکوهی،سید محمد تقی (۱۳۸۸). پایگاه داده. انتشارات جلوه،ویراست چهارم، ص۱۰۲-۱۰۸

۷. رحیمیان، نظام الدین، ۱۳۹۰ ، کشف تقلب مجله حسابدار رسمی شماره ۱۳،صص۸۲_۹۱

۸. فروزنده، حبیب، ۱۳۹۰، مدیریت پایگاه داده. تهران، عابد .

۹. تختایی، نصر اله، صیفوری، یعقوب، تقلب در سیستم های اطلاعاتی حسابداری، نخستینکنفرانس بین المللی حسابداری و مدیریت،۱۳۹۶، Icam01-053

۱۰. خواجوی، شکرالله؛ ابراهیمی، مهرداد۱۳۹۷، بررسی تأثیر سازوکارهای حاکمیت شرکتی بر تقلب در صورت های مالی شرکت های . ، پذیرفته شده در بورس اوراق بهادار تهران .مدیریت دارایی و تأمین مالی،۷۱-۸۴

۱۱. قادری، کاوه، قادری، صلاحالدین( ۱۳۹۶) تحلیل بیش اطمینانی مدیران از عملکرد خود در شرکت های متقلب . بررسیهای حسابداری وحسابرسی ۲۴(۲)، ۲۴۳- ۲۶۲

12. Fiedler, K.D., Grover, V., Teng, J.T.C., 1996. An empirically derived taxonomy of information technology structure and its relationship to organizational structure.J. Manag. Inf. Syst. 13 (1), 9–34.
13. Wand, Y., Monarchi, D.E., Parson, J.,Woo, C.C., 1995. Theoretical foundations for conceptualmodeling in information systems development. Decis. Support. Syst. 15 (4),285–304

14. Nickerson, R.C., Varshney, U., Muntermann, J., 2013. A method for taxonomy development and its application in information systems. European Journal of Information Systems 22 (3), 336–359
15. Dharmastuti, C., Wahyudi, S. (2013). The Effectivity of Internal and External Corporate Governance Mechanisms Towards Corporate Performance. Research Journal of Financeand Accounting, 4(4), 132-139.
16. UNODC (United Nations Office on Drugs and Crime) 2012. Principles and Framework for an international classification of crimes for statistical purpose: report of the UNODC /UNECE Task Force on Crime Classification to the Conference of European Statisticians

Title :Recognize computer fraud in accounting information systems and provide prevention strategies

Ali Amiri17
Mahrokh darabi18

The reason for the importance of accounting information system for computer offenders and criminals is the role of accounting information systems in controlling financial resources. Given the importance of these systems for managing the organization's operations, they may be exploited by opportunists and individuals with conflicting interests with the organization. This study can provide new solutions to prevent criminal acts by examining computer crimes in the field of accounting information and its classification in order to inform accountants, auditors and other stakeholders of financial information. Writing future experimental research. This research is from the perspective of descriptive-comparative purpose, which has been analyzed in a library manner. (The results of the research include three tables that first categorize the types of computer fraud including 1- information fraud 2- processor 3- input data 4- computer commands5- outputs Content analysis, then ways to prevent and detect computer fraud including detailed analysis and separation of 4 categories In other words, reducing the likelihood of fraud, factors increasing the difficulty and difficulty of committing fraud, factors improving the methods of detecting and detecting fraud, and finally providing solutions to prevent computer fraud and identifying ways to reduce the resulting loss in the accounting information category. Finally, the classification of the use of appropriate procedures and regulations for hiring and firing employees was examined in a qualitative manner and the content was analyzed.

[1] Assistant Professor, Department of Accounting and Finance, Faculty of Humanities, Islamic Azad University, Bandar Abbas Branch, Bandar Abbas, Iran

[1] PhD student, Department of Accounting and Financial Management, Bandar abbas branch, Islamic azad university, Bandar abbas, Iran.