مجله حسابداری مدیریت
سال سوم / شماره چهارم / بهار ۱۳۸۹

تبیین اهمیت آموزش دانشجویان رشته حسابداری در زمینه علوم کامپیوتری، جرائم مربوطه و رعایت اخلاق حرفه ای

دکتر رمضانعلی رویایی[۱]
جمال بحری ثالث[۲]
عسگر پاک‌مرام[۳]

تاریخ دریافت: ۸۸/۱۲/۱۵ تاریخ پذیرش: ۸۹/۰۲/۲۵

چکیده:

اخبار مربوط به اعمال متقلبانه در حسابداری در چند سال اخیر، به عنوان یکی از خبرهای شایع در رسانه‌های عمومی‌بوده است. حرفه حسابداری نیز به دلیل فشار افکار عمومی‌تاکید بر اهمیت رعایت اخلاق حرفه ای را شروع کرده است. براین اساس برخی از هیئت‌ها و انجمن‌های حرفه ای حسابداری، به ضرورت آموزش مستمر علوم کامپیوتری و موازین اخلاق حرفه ای تاکید کرده اند و آموزش مربوط را به عنوان بخشی از واحدهای اصلی جهت اخذ مدارج و گواهینامه‌های حسابدرای، ضروری دانسته اند. بیشتر اعمال متقلبانه در حسابداری در حال حاضر به شکل جرائم کامپیوتری می‌باشند. پس، دانشجویان حسابداری باید نسبت به انواع مختلف تقلب‌ها، از جمله جرائم کامپیوتری، و نیز چگونگی جلوگیری و تشخیص آنها آگاه باشند. این مقاله در مورد سطح مورد نیاز آموزش دانش کامپیوتر و معرفی چندین طبقه از جرائم کامپیوتری و ابزارهای تکنولوژیکی جهت جلوگیری و تشخیص این جرائم، مطالب مفیدی را ارائه می‌دهد. گوناگونی و تعدد جرائم کامپیوتری و ابزارهای تشخیص و جلوگیری از آنها به اندازه تعداد مرتکبان این جرائم می‌باشد.

همچنین این مقاله ترکیبی از چهار عنوان درسی را برای آموزش دانشجویان رشته حسابداری جهت آمادگی برای مشاغل حرفه ای شان، در زمینه آشنایی با مبانی زبان‌های برنامه نویسی و بانک‌های اطلاعاتی، جرائم کامپیوتری و رعایت اخلاق حرفه ای، پیشنهاد می‌دهد. این چهار عنوان درسی عبارتند از آشنایی با مبانی زبانهای برنامه نویسی و بانکهای اطلاعاتی ویژه نرم افزارهای حسابداری، سیستم‌های اطلاعات حسابداری (AIS)، جلوگیری و تشخیص تقلب (حسابداری حقوقی) و اخلاق حرفه ای حسابداری. این چهار عنوان درسی، که متفقاً مورد استفاده قرار می‌گیرند، در طول حرفه حسابداری دانشجویان رشته حسابداری و در مواجهه با رویدادهای متقلبانه و تصمیمات اخلاقی، ابزارهای مورد نیاز را فراهم می‌آورد.

واژه‌های کلیدی: آموزش، حسابداری، علوم کامپیوتری، جرائم، اخلاق حرفه ای.

۱ استادیار و عضو هیئت علمی دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران. (نویسنده مسئول و طرف مکاتبه) culturalmanagement@srbiau.ac.ir
۲ دانشجوی دکترای حسابداری دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران وعضو هیئت علمی ارومیهBHRYSLS@yahoo.com
۳ دانشجوی دکترای حسابداری دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران و عضو هیئت علمی بناب. pakmaram@gmail.com

۱ مقدمه

تقلب درحسابداری در چند سال اخیر به عنوان موضوعی رایج در رسانه‌های عمومی مورد توجه بوده است. به دلیل همین فشار منفی، حرفه حسابداری کم کم شروع به تأکید بر اهمیت رعایت موازین اخلاق حرفه ای نمود. وجود اسناد ومطالب بسیار زیاد در وب سایت انجمن حسابداران رسمی‌آمریکا[1] نشان از اهمیت موضوع تقلب و موازین حرفه ای از دیدگاه این انجمن می‌باشد.

هیئت‌های ایالتی حسابدارن رسمی‌آمریکا نیز بر لزوم آموزش واحدهای درسی در مورد اخلاق حرفه ای برای حسابداران رسمی‌جهت اخذ و تمدید مجوزفعالیت تأکید داشته اند. برای مثال، هیئت حسابداران رسمی‌ایالت لوئیزیانا سه ساعت آموزش اخلاق حرفه ای را به عنوان بخشی از نیازمندیهای آموزش مستمر حرفه ای الزامی‌کرده است. هیئت حسابداری ایالت تگزاس هم بخش نامه ای را مصوب کرده است که به موجب آن داوطلبان امتحان حسابداران رسمی‌باید سه ساعت آموزش اخلاق حرفه ای را به عنوان قسمتی از آموزش حسابداری شان پشت سر بگذارند. این الزام از زمانی که اجرا گردید، دانشکده‌های حسابداری در ایالت تگزاس را مجبور کرد تا ارائه واحدهای اخلاق حرفه ای را به عنوان بخشی از برنامه آموزشی آغاز کنند. با توجه به این الزامات بدون شک، دیگر مراکز اعطاء کننده مجوز فعالیت برای حسابداران رسمی‌در آمریکا نیز، می‌بایست الزامات مشابهی را برای اخلاق حرفه ای اجراء نمایند.

رشته حسابداری در بسیاری از دانشگاهها آمریکا بر لزوم آموزش اخلاق حرفه ای در برنامه آموزشی شان تأکید دارند. تقریباً تمامی‌متون حسابداری مباحثی را در مورد رعایت موازین اخلاق حرفه ای دارند، اما این سئوال باید پرسیده شود که آیا این مدت زمان محدود (سه ساعت) در حوزه برنامه‌های آموزش تحصیلی حسابداری کافی می‌باشند یا خیر. اساتید حسابداری نیز اجرای پژوهش‌های لازم در زمینه اخلاق حرفه ای در کلاسهای درسشان را آغاز کرده اند. در واقع، بعد از فوریه سال ۲۰۰۴ (به علت وقوع رسوائی‌های بزرگ حسابداری)یکی از موضوعات اصلی مورد توجه در مباحث آموزش حسابداری فراگیری موازین اخلاق حرفه ای در حسابداری بوده است.و دانشکده‌های حسابداری در آمریکا نیز ملزم به افزایش ساعات آموزش اخلاق حرفه ای در واحدهای حسابداری شدند.

به منظور درک دلیل اهمیت مسئولیت پذیری و حسابخواهی، دانشجویان حسابداری باید نسبت به این مسئله آگاهی یابند که تقلب‌های این حوزه منجر به تأکید فزاینده بر اخلاق حرفه ای در برنامه آموزشی تحصیلی گردیده است. یکی از حوزه‌های خاص تقلب در حسابداری که توجه ویژه ای را به خود جلب کرده است، جرائم وتقلب کامپیوتری می‌باشد. جرائم یا تقلب درحسابداری به طرق بسیار متفاوتی تعریف شده است. این باور وجود دارد که جرائم کامپیوتری جرائمی‌است که با استفاده از کامپیوتر انجام شده یا معطوف به کامپیوتر می‌باشد. باوردیگر شامل دیدگاه گسترده تری درمورد جرائم کامپیوتری است و تأکید می‌کند که جرم کامپیوتری جرمی‌است که برای ارتکاب آن از کامپیوتری با هر ظرفیتی استفاده می‌شود. (رومنی و استین بارت ۲۰۰۳)[2] بدون توجه به اینکه تعریف جرم کامپیوتری چه می‌باشد، تأثیرات جرائم کامپیوتری می‌تواند پیکره یک سازمان را ویران سازد وجامعه کنونی را که برای ارائه حجم گسترده ای از اطلاعات، وابسته به سیستم‌های کامپیوتری می‌باشدبا بحران مواجه کند. با نیاز بیشتر مردم به اطلاعات، سیستم‌های کامپیوتری پیچیده تر شده و در بسیاری از موارد محافظت از این سیستمها دشوار می‌باشد.

هرساله، انجمن امنیت کامپیوتری آمریکا (CSI)[3] و دفتر بازرسی فدرال آمریکا (FBI)[4] یک ارزیابی را در مورد جرائم و امنیت کامپیوتری اجرا می‌کنند (از این پس در این مقاله به آن گزارش ارزیابی CSI/FBI می‌گوئیم). گزارش ارزیابی CSI/FBI مشتمل بر پاسخ دهندگانی از سازمانهای زیادی از صنایع مختلف می‌باشد. این گزارش انوع جرائم کامپیوتری، فناوریهای به کار رفته برای جلوگیری از این جرائم، تعداد حملات و مبالغ دلاری خسارت ناشی از این حملات را نشان می‌دهد. گزارش سال ۲۰۰۳ نشان می‌دهد که تعداد این حملات تقریباً با تعداد دو سال قبل (۲۰۰۱ و ۲۰۰۲) برابر است، اما خسارت مالی ناشی از این حملات نسبت به دو سال قبل تقریباً ۵۶ درصد کاهش یافته است. این گزارش نشان داد که این خسارت در زمینه دزدی اطلاعات خصوصی[5] و ویروسها کاهش یافته است، اما در حوزه‌هائی نظیر حملات تخریب خدمات[6] (حمله هکرها به وب سایت‌ها واز کار انداختن آنها)دسترسی غیرمجاز[7]، و عملیاتهای تخریبی[8] افزایش داشته است. بر اساس گزارش انجمن امنیت کامپیوتری آمریکا در سال ۲۰۰۳ برآوردهای مربوط به زیانهای مالی ناشی از جرائم کامپیوتری از ۳۰۰ میلیون دلار تا بیش از ۹ میلیارد دلار در سال می‌باشد. اما به نظر دفتر بازرسی ایالتی تنها یک درصد از این جرائم تشخیص داده شده و شناسائی می‌شوند.جرائم کامپیوتری بسیاری شناسائی نشده یا گزارش نمی‌شوند، بنابراین، شاید هرگز نتوان مبلغ خسارت ناشی ازجرائم کامپیوتری درهر سال را برآوردکرد.(«کاسابونا» و«یو» سال۱۹۹۸)[9].

بخش بعدی این مقاله ضمن بیان سطح مورد نیاز آموزش زبانهای برنامه نویسی و بانکهای اطلاعاتی ویژه حسابداری چندین نوع از جرائم معمول کامپیوتری را مورد بررسی قرار می‌دهد. بخش بعد از آن نیز فناوریهای مورد استفاده برای جلوگیری و تشخیص جرائم کامپیوتری را بررسی می‌کند. سرانجام در بخش پایانی، ارائه واحدهای درسی جهت استفاده در آموزش دانشجویان حسابداری در زمینه آموزش دانش کامپیوتر،جرائم کامپیوتری، اخلاق حرفه ای، و شناسائی تقلب و نیز محتوای احتمالی این واحدها را پیشنهاد می‌دهد.

۲ مبانی نظری مطالعه

۲ـ۱ معیارهای لازم و دانش مورد نیاز در نرم‌افزارهای مالی

چه معیارهایی درانتخاب نرم افزارهای مالی مهم هستند ؟ اصولاً گاهی باید این پرسش را مجدداً در کلیه سطوح مطرح کرد و دلیل آن هم، بسیار ساده است. در دنیای امروز نیاز حسابداران و مدیران روز به روز به سیستمهای رایانه ای و نرم افزارهای مالی بیشتر می‌شود.و در این راستا هر مجموعه مالی که خود را با پیشرفتهای روز بهتر و سریع تر تطبیق دهد موفق تر خواهد بود. دراین بخش از مقاله سعی شده است بااستفاده ازنظرات کارشناسان برنامه نویسی و مالی مهمترین معیارهای انتخاب نرم افزار حسابداری مناسب با در نظر گرفتن میزان اهمیت آن ارائه شود.چرا که دانستن این معیارها سطح دانش کامپیوتری موردنیاز دانشجویان حسابداری را نیز آشکارمی‌کند. لذا در ابتدا برای آشنایی با این موضوع عناوین زبانهای برنامه نویسی و بانکهای اطلاعاتی با آخرین رتبه بندی،که برای نوشتن نرم افزارهای حسابداری استفاده می‌شود بیان شده و سپس درمورد ضرورت آموزش آن مطالبی ارائه می‌شود.

تاریخچه زبانهای برنامه نویسی مورد استفاده برای نرم افزارهای حسابداری در ایران و جهان:

الف) عناوین زبانهای برنامه نویسی نسل اول :

۱ـ فورترن[10]

۲ کوبال[11]
۳ پاسکال[12]
۴ سی[13]
۵ دیتا بیس[14]
۶ کلیپر[15]
۷ زبان برنامه نویسی پارادوکس[16]
۸ ایکس بیس[17]
۹ فاکس پرو[18]
۱۰ بیسک[19]
۱۱ ویژوال فاکس پرو[20]

جدول (۱): مقایسه کاربرد زبانهای مختلف برنامه نویسی در سالهای ۲۰۰۸ و ۲۰۰۹

نام زبان برنامه نویسی	درصد کاربرد در ۲۰۰۹	رتبه در سال ۲۰۰۸	رتبه در سال ۲۰۰۹
Java	20.715%	1	1
C	15.379%	2	2
C++	10.716%	5	3
(Visual) Basic	10.490%	3	4
PHP	9.243%	4	5
Python	5.012%	8	6
Perl	4.841%	6	7
C#	4.334%	7	8
JavaScript	3.130%	9	9
Delphi	3.055%	14	10
Ruby	2.762%	10	11
D	1.265%	13	12
PL/SQL	0.700%	11	13
SAS	0.640%	12	14
ActionScript	0.472%	23	15
Lisp/Scheme	0.419%	16	16
Lua	0.415%	18	17
Pascal	0.400%	22	18
PowerShell	0.384%	-	19
COBOL	0.360%	17	20

ب) عناوین زبانهای برنامه نویسی نسل دوم[21]

۱ ویژوال بیسیک[22]
۲ دلفی[23]
۳ ویژوال بیسیک دات نت[24]
۴ ویژوال سی دات نت[25]

ج) عناوین زبانهای برنامه نویسی نسل سوم[26]

۱) آ اس پی دات نت۲۷
۲) جاوا۲۸
۳) مایکروسافت دات نت۲۹

مهمترین بانک‌ها ی اطلاعاتی مورد استفاده در نرم افزارهای مالی

۱ اس کیو ال[30]
۲ اراکل[31]

ضرورت آموزش شناخت معیارهای انتخاب نرم افزار به دانشجویان رشته حسابدرای

با توجه به تعدد زبانهای برنامه نویسی و بانکهای اطلاعاتی و تفاوت فاحش هر یک از آنها از لحاظ کاربردی و امنیتی و همچنین سرعت تغییر کاربرد آنها با توجه به جدول مقایسه ای ارائه شده میتوان نتیجه گرفت برای آشنایی با نرم افزارهای حسابداری می‌بایست دانشجویان رشته حسابدرای نسبت به قابلیت، محاسن و معایب انواع زبانهای برنامه نویسی و بانکهای اطلاعاتی آگاهی داشته باشند.چرا که در صورت نداشتن چنین اطلاعاتی در زمانی که کلیه سازمانهای متوسط و بزرگ از سیستمهای رایانه ای و انواع مختلف نرم افزار استفاده می‌کنند دانشجویان رشته حسابدرای قادر به ادامه کار حرفه ای و تصمیم گیری صحیح نخواهند بود. که البته این مهم با توجه به واحدهای درسی و نحوه آموزش دانشجویان حسابداری درتمام مقاطع تحصیلی مورد توجه قرار نگرفته است و متاسفانه دانشجویان بعد از فارغ التحصیل شدن و ورود به بازار کار با مشکلات فراونی از جمله موارد ذیل روبرو می‌شوند.

۱) عدم توانایی انجام مناسب و به موقع امورات محوله با توجه به نداشتن دانش کامپیوتری لازم و عدم شناخت کافی از نرم افزارهای حسابداری
۲) بالا رفتن هزینه‌های آموزشی سازمانها به علت عدم آموزش دانشجویان در موقع تحصیل
۳) تبدیل شدن حسابداران به اپراتور جهت ورود اطلاعات به رایانه ونداشتن برتری به سایر کارکنان با توجه به تخصص مالی که در دوران تحصیل فرا گرفته اند.
۴) عدم توانایی ارائه اطلاعات مربوط و ضروری به مدیران ارشد و تبعیت بی چون و چرا از برنامه نویسان

با توجه مطالب فوق الذکر، ایجاد شناخت مختصر راجع به زبانهای برنامه نویسی، بانکهای اطلاعاتی و... و ضرورت آموزش آن به جمع بندی نظرات کارشناسان کامپیوتر در خصوص معیارهای عمده انتخاب نرم افزار حسابداری مناسب پرداخته می‌شود. علت این امر یعنی بیان نحوه انتخاب نرم افزار حسابداری مناسب برای ارائه حدود آموزش علوم کامپیوتری برای دانشجویان حسابداری این است که، شرط انتخاب درست یک نرم افزار کسب شناخت کافی در مورد علوم کامپیوتری است. البته از لحاظ علم منطق نیز داشتن شناخت کافی در مورد هر چیزی اولین لازمه اخذ تصمیم درست در مورد همان چیز است . لذا در این قسمت از مقاله برای ارائه حدود آموزش علوم کامپیوتری برای دانشجویان حسابداری به بیان چگونگی انتخاب یک نرم افزار حسابداری مناسب می‌پردازیم. برای اینکار باید معیارهای مختلفی را در نظر داشت که این معیارها رامی‌توان ازنظرکلی به دوگروه عمده تقسیم کرد : معیارهای فنی و معیارهای مدیریتی.

معیارهای فنی به ترتیب اهمیت عبارتند از:

۱) استفاده از زبان و بانک اطلاعاتی مناسب با توجه به نیازهای جاری و آتی
۲) سهولت بکارگیری،سرعت ورود داده، راحتی دسترسی به منوها واستفاده از کلیدهای میان بر ومهندسی مناسب طراحی آیتم‌های صفحه
۳) کارایی سیستم، قابلیت توسعه وتطبیق سیستم با نیازها و ا شرایط محیطی و شبکه
۴) امنیت شامل امنیت نرم افزار، امنیت بانک اطلاعاتی و امنیت شبکه
۵) معیارهای مدیریتی به ترتیب اهمیت عبارتند از :
۶) هزینه تهیه نرم افزار، هزینه خرید سخت افزارهای مورد نیاز نرم افزار انتخابی وهزینه نگهداری و توسعه
۷) اعتبار فروشندگان نرم افزار و سخت افزار و اطمینان از پشتیبانی و خدمات بعد از فروش آنها
۸) اطمینان از اینکه در تهیه نرم افزار از زبان و بانک اطلاعاتی دارای لیسانس استفاده شودو همچنین قابل خریداری بودن متن برنامه (سورس) با قیمت منصفانه در مواقع نیاز
۹) قابلیت گزارش دهی مناسب و با انعطاف

با توجه به معیارهای عنوان شده دانشجویان رشته حسابداری باید نسبت به انواع زبانهای برنامه نویسی و بانکهای اطلاعاتی شناخت مناسبی در حد موارد ذیل داشته باشند.

۱) قابلیت و معایب هریک از زبانهای برنامه نویسی و بانکهای اطلاعاتی علی الخصوص از لحاظ امنیت، هزینه‌های جاری وآتی، کارائی و سرعت انتقال اطلاعات.
۲) آشنایی با ساختار یک نرم افزار حسابداری مناسب.
۳) آشنایی با ساختار یک شبکه داخلی مناسب برای نرم افزارهای حسابداری.
۴) نحوه عمل و کارکرد یک نرم افزار حسابداری مناسب.

۲ ۲ انواع جرائم کامپیوتری

جرائم کامپیوتری به اشکال مختلفی صورت می‌گیرند. برخی روشهای ارتکاب جرائم کامپیوتری به طرز باور نکردنی ساده هستند. دیگر روشهای این کار چنان پیچیده هستند که تنها کارشناسان کامپیوتری و حسابداران حقوقی[۳۲] (حسابداران مجرب در امورحقوقی) می‌توانند از لابلای ده‌ها هزار اطلاعات ریز و درشت دقیقاً متوجه شوند که چه نوعی جرمی‌رخ داده و چه کسی این جرم را مرتکب شده است. در بسیاری از موارد، جرم کامپیوتری شبیه به جرم غیرکامپیوتری است، اما جرم کامپیوتری با استفاده از ابزارهای الکترونیکی صورت می‌گیرد نه ابزارهای سنتی.

این بخش به بررسی چندین دسته از جرائم کامپیوتری در سازمانها که غالباً توسط افرادی صورت می‌گیرد، می‌پردازد. سازمانها هیچ گونه کنترلی روی افرادی که از بیرون سازمان، مرتکب جرائم زیادی، مانند حملات تخریب خدمات یا شیادی از طریق ایمیل می‌شوند، ندارد، پس چنین جرائم کامپیوتری در مقاله مورد بحث قرار نمی‌گیرد. جرائم کامپیوتری در این مقاله به شش دسته مجزا طبقه بندی شده است، با اینکه می‌توان جرائم کامپیوتری را به گروههای متعدد دیگری نیز طبقه بندی نمود، اما طبقه بندی جرائم کامپیوتری در این مقاله با نام‌ها و تعاریف شناخته شده تری صورت گرفته است.

۱) برنامه‌های مخرب یا ویروسهای کامپیوتری[۳۳]

برنامه‌های تخریبی به اشکال مختلف و از جاهای متعددی وارد کامپیوترها می‌شوند. شاید شایع‌ترین اشکال آنها ویروس‌ها و کرمهای کامپیوتری باشند. در بسیاری موارد، چنین برنامه‌های تخریبی توسط افرادی خارج از سازمان تولید و توسعه می‌یابند. اما کارمندان هم می‌توانند این برنامه‌ها را در سازمان خودشان اجراء کنند.

تعاریف زیادی برای ویروس و کرم کامپیوتری وجود دارد، و افراد زیادی از این اصطلاحات به جای یکدیگر استفاده می‌کنند. عموماً، ویروس کامپیوتری را می‌توان اینگونه تعریف کرد: برنامه یا بخشی از برنامه ای که مخرب (ویروسی) بوده و اثر خود را به دیگر برنامه‌ها انتقال می‌دهد.و به سادگی قابل انتشار می‌باشد (هال ۲۰۰۴، «رومنی» و «استین بارت» ۲۰۰۳).[۳۴] در بسیاری از موارد ویروس تخریب کننده بوده، اما گاهی اوقات ویروسها بیشتر برای آزار و اذیت[۳۵] یک کامپیوتر یا شبکه کامپیوتری تولید می‌شوند و اثر تخریبی ندارند. ویروس کامپیوتری عموماً به این صورت تعریف می‌شود: برنامه ای که خود را در برنامه مجازی دیگری می‌گنجاند («هال» ۲۰۰۴، «رومنی» و «استین بارت» ۲۰۰۳). برخی کرمها هم مانند ویروسها تخریب کننده هستند، اما برخی نیز این گونه نیستند. کرمها غالباً از طریق پیامهای ایمیلی انتشار می‌یابند.

بمب منطقی[۳۶] نوعی ویروس شایع است. بمب منطقی کدی است که وارد سیستم عامل یا دیگر برنامه‌های نصب شده و هدف آن اجرای برخی از رویدادهای از پیش تعیین شده می‌باشد. بمبهای منطقی معمولاً ماهیتی تخریبی دارند. یکی از نمونه مشهور بمبهای منطقی، ویروس میکلانژ[۳۷] می‌باشدکه که تصور می‌شد که هر ساله در روز ۶ مارس (روز تولد این هنرمند) منتشر می‌شود. در سال ۱۹۹۲، این ویروس عمومیت بسیار زیادی پیدا کرد اما تأثیر بسیار اندکی در سراسر جهان داشت (vmyths.com ۲۰۰۴).

هر یک از این برنامه‌های تخریبی می‌توانند برای سازمان هزینه زا باشند. برای مثال، گزارش ارزیابیCSI/FBI در آمریکا نشان داد که ۸۲ درصد سازمانها مورد بررسی در سال ۲۰۰۳ وجود حملات ویروسی را گزارش کرده اند. مبلغ کل زیان این

حملات ویروسی بیش از ۲۷ میلیون دلار بود (گزارش ارزیابیCSI/FBI سال ۲۰۰۴).

۲) دسترسی غیرمجاز به سیستمهای اطلاعاتی

معمولاً به طرق مختلفی، اعم از داخلی یا خارجی، می‌توان به سیستم‌های اطلاعاتی دسترسی پیدا کرد. به افرادی که معمولاً این نوع جرائم کامپیوتری را مرتکب می‌شوند، هکر[۳۸] گفته می‌شود. در گذشته، هکرها داده‌ها را در طول مسیر انتقال تخریب ویا سرقت می‌کردند. لذا سازمانها شروع به رمزگذاری یا درهم ریختن داده‌ها[۳۹] نمودند، بنابراین هکرها برای دسترسی به این داده‌ها به روشهای دیگری روی آوردند. اساساً هکرها اغلب به صورت غیرقانونی وارد می‌شوند، اما این کار را با استفاده از کامپیوتر انجام می‌دهند. افراد غیرمجاز معمولاً به یکی از دو طریق ذیل به رمز عبور مورد نظر خود دسترسی پیدا می‌کنند.اول از طریق جستجوی رمز عبور[۴۰] با استفاده از برنامه ای که به صورت الکترونیکی شناسه و رمز عبور کاربر را حدس می‌زندو این عمل را تا زمانی که واقعاً رمز عبور مورد نظر را پیدا کند، ادامه می‌دهند. ودوم از طریق رد یابی رمز عبور[۴۱] که با ورود به سیستم اطلاعاتی از طریق ردیابی کاربرمجاز وباعبورازموانع امنیتی رمزموردنظر راپیداکند («لولفینگ» و همکاران ۲۰۰۳)[۴۲].

افراد به دلایل زیادی به سیستم‌های اطلاعاتی دسترسی غیرمجاز پیدا می‌کنند. برخی از افراد برای منافع شخصی یا به منظور سرقت داده‌های حساسی، نظیر شماره‌های تأمین اجتماعی، شماره‌های کارتهای اعتباری،یا شماره حسابهای بانکی، به این سیستم‌ها دسترسی پیدا می‌کنند. افراد دیگر نیز برای ایجاد اختلال در دسترسی‌های مجاز، به سیستم‌های کامپیوتری وارد می‌شوند، و برخی نیز تنها وب سایتها را تخریب کرده یا داده‌ها را از پایگاه داده‌ها حذف می‌کنند. در بسیاری از موارد، هکرهای خارجی تنها برای تفریح اقدام به هک کردن می‌کنند، یا اینکه تنها می‌خواهند از این موضوع لذت ببرند که آیا می‌توانند سیستم‌های کامپیوتری سازمانها را هک کنندیا خیر. اعم از اینکه دسترسی به صورت داخلی باشد یا خارجی، دسترسی غیرمجاز به سیستم‌های اطلاعاتی می‌تواند برای سازمان هزینه زا و زیان آور باشد.

۳) عملیات تخریب داده‌ها و خرابکاری فیزیکی [۴۳]

عملیات تخریب و خرابکاری چیزهای جدیدی نیستند و امکان ارتکاب آن هم توسط کارمندان سازمان و هم توسط افراد خارجی وجود دارد. اگر برنامه‌های مناسبی برای بازیابی اطلاعات وجود نداشته باشد، خسارت مربوط به سیستم فیزیکی کامپیوتری سازمان می‌تواند سرسام آور باشد. بیشتر سازمانها یاد گرفته اند که سیستمهای کامپیوتری را در محلهای قرار دهند که به سادگی برای کارکنان غیرمجاز قابل دسترسی نباشد. نمونه‌های واقعی زیادی از کارمندان ناراضی که به سخت افزار کامپیوتری شرکت آسیب رسانده اند، وجود دارد. با محدود کردن دسترسی فیزیکی به سیستم‌های اصلی کامپیوتری، سازمان می‌تواند آسیب فیزیکی وارده به کامپیوترها توسط کارمندانش را محدود سازد.

برخی مرتکبان اینگونه جرائم به جای وارد کردن آسیب فیزیکی به سخت افزار کامپیوتری، پایگاه داده‌ها یا وب سایتهای سازمان را تخریب می‌کنند.البته برای انجام این عملیات مجرم باید قادر باشد تا به منظور آسیب رساندن به فایلها، به فایلهای وب سایت یا پایگاه داده دسترسی پیدا کند. کنترل دسترسی به سیستم کامپیوتری اولین خط دفاعی برای چنین مواردی است. نمونه‌های متعددی برای اعمال خرابکاری در وب سایت سازمان وجود دارد. برای مثال، هکرها در بسیاری اوقات وب سایتهای دولتی را تخریب می‌کنند. وب سایتهای نیروی هوائی ایالات متحده، سازمان

اطلاعات مرکزی آمریکا، و ناسا همگی مورد هدف عملیاتهای تخریبی قرار گرفته اند. به علاوه، چندین وب سایت دولتی کانادا در سال ۱۹۹۹ تخریب شدند («سیلورتورن[۴۴]» ۱۹۹۷، «مک گیولیورای[۴۵]» ۲۰۰۰).

در برخی موارد، هکرها آدرس وب سایت سازمان را تغییر داده و پیام خود را به جای اطلاعات سازمان قرار داده و یا از وب سایت سازمانها برای مقاصد تحریف اطلاعاتی استفاده می‌کنند. برای مثال، کارمندان ناراضی یا هکرهای وارد وب سایت سازمان شده و اطلاعات نادرستی، نظیر اطلاعات نادرست مالی یا اخبار جعلی، را در مورد سازمان به جای اطلاعات اصلی قرار می‌دهند. چنین اطلاعات نادرستی می‌تواندبرای طرف قربانی پرهزینه و فاجعه آمیز باشد و منجر به خسارات جبران ناپذیری برای شهرت و آوازه سازمان گردد. جبران زیان حاصل از این تخریبها نیاز به زمان زیادی داردوگاهی ماهها طول می‌کشدودربرخی موارد مستلزم پیگرد قانونی است («مک گیولیورای» ۲۰۰۰). با وجودی که ممکن است افراد داخلی سازمان مرتکب چنین مواردی نشوند، اما باز هم به دلیل اینکه این افراد توان بالقوه ای جهت وارد

ساختن این نوع آسیبها دارند، برای سازمان مهم تلقی می‌شوند.

٤) سرقت اطلاعات محرمانه[٤٦]

یکی از اشکال سرقت اطلاعات محرمانه، معادل جاسوسی صنعتی می‌باشد که همان سرقت اطلاعات حساس یا مبادله اسرار محرمانه یک سازمان است. در بسیاری موارد، سرقت این اطلاعات توسط کارمندان مورد اعتماد صورت می‌گیرد که به این اطلاعات دسترسی دارند. چنین جرمی‌تواند به واسطه استفاده از تکنیک‌های پیچیده، نظیر هک کردن پایگاه داده‌ها یا نرم افزار و ضبط وکنترل اطلاعات دلخواه گرفته،تا تکنیکهای ساده ای، چون وارسی وبازیابی اطلاعات سطل زباله جهت استفاده غیر مجاز از آنها و یا ذخیره کردن در یک فایل مخفی، انجام گیرد. سرقت این اطلاعات می‌تواند برای سازمان مخرب باشد.برخی از کارکنان یا هکرها تلاش می‌کنند که اسرارتجاری را به سرقت ببرند و افشا چنین اطلاعاتی منجربه کاهش وضعیت رقابتی سازمان می‌شود.در برخی موارد،اطلاعات خصوصی حتی برای اخاذی یا تهدید سازمان مورد استفاده قرارمی‌گیرند(«ویتمن[۴۷]» ۲۰۰۳).

سرقت اموال فکری و نرم افزارهای یک سازمان نیز به عنوان سرقت اطلاعات محرمانه محسوب می‌شوند. سرقت اموال فکری و نرم افزاری به اشکال مختلفی مشاهده شده و می‌تواند به سادگی کپی کردن برنامه به صورت غیرقانونی یا هک کردن سیستم کامپیوتری سازمان و دزدیدن کد برنامه‌های مختلف باشد. اتحادیه تولید کننده‌های نرم افزارهای تجاری آمریکا[۴۸] برآورد می‌کند که ۲۳ درصد تمامی‌برنامه‌های نرم افزاری مورد استفاده به صورت غیرقانونی به دست آمده است.و زیان‌های اقتصادی حاصل از عدم رعایت قانون حق تالیف[۴۹] (کپی رایت) سالانه بین ۱/۸ میلیارد دلار تا ۹/۲ میلیارد دلار برآورد می‌شود. این زیانها شامل از دست رفتن درآمد ناشی از فروش، از دست رفتن مشاغل، دستمزدها، و درآمد مالیاتی می‌باشد. («هریس[۵۰]» ۲۰۰۳). اخیراً صنایع نرم افزاری و دیگر صنایع، به ویژه صنعت موسیقی، با انجام پیگردهای قانونی به دنبال مبارزه با این وضعیت هستند.این مورد در ایران با توجه به محکم نبودن قوانین مربوط به حق تالیف و عدم رعایت قوانین موجود بسیار شایع تر است. اما به علت اینکه اکثر نرم افزارها مورد استفاده در ایران خارجی هستند و مدافع ندارند مورد توجه قرار نمی‌گیرد.

٥) دستکاری داده‌ها و تقلب مالی[٥١]

یکی از اشکال دستکاری داده‌ها، به نام تحریف داده‌ها[٥٢]، شامل تغییر داده‌ها در یک پایگاه داده‌ها می‌باشد. دستکاری داده‌ها شامل افزودن، حذف نمودن

و یا تغییر داده‌ها در پایگاه داده‌هاست. عموماً چنین دستکاری توسط یکی از کارمندانی سازمان صورت می‌گیرد و هدف از انجام آن، تغییر داده‌های مالی است. تغییر داده‌های مالی منجر به ارائه صورتهای مالی نادرست یا دیگر گزارشهای مالی غیر واقعی می‌شود و این امر سبب می‌شود تا افراد زیادی اعم از درون سازمانی و یا برون سازمانی که از این اطلاعات برای اتخاذ تصمیمات مهم استفاده می‌کنند، دچار اشتباه شوند.شکل رایج دیگری از دستکاری داده‌ها، ورودی داده‌های تقلبی است. رویه‌های ورودی سیستم اطلاعات حسابداری خیلی حیاتی تلقی می‌شوند، زیرا هنگامی‌که داده‌های پر از خطا و تقلبی وارد سیستم اطلاعات حسابداری می‌شود خروجی این سیستم نیز نمی‌تواند مورد تأیید باشد. ارتکاب این نوع جرم تنها مستلزم مهارتهای کامپیوتری بسیار اندکی می‌باشد. در واقع تمام آنچه که جهت انجام این نوع از تخلفها مورد نیاز است آشنایی با چگونگی ورود معاملات (تراکنش‌ها)[۵۳] به درون سیستم کامپیوتری است.

٦) سرقت سخت افزار کامپیوتری [۵۴]

شکل دیگری از جرائم کامپیوتری، سرقت سخت افزار کامپیوتری است. طبیعتاً اگر سخت افزار کامپیوتری دزدیده شود، داده‌های این کامپیوتر هم به سرقت برده شده و ممکن است برای هرگونه برنامه کلاهبرداری و تقلب مورد استفاده قرار گیرد. با وجودی که سخت افزار کامپیوتری معمولاً توسط افراد خارج از سازمان دزدیده می‌شود،اما اطن خطر در مورد کارمندانی که غالباً سخت افزار کامپیوتری را امانت [۵۵] می‌گیرند، نیز وجود دارد.

سرقت سخت افزار کامپیوتری غالباً به شکل سرقت کامپیوترهای لپ تاپ صورت می‌گیرد. گزارش ارزیابی CSI/FBI در آمریکا نشان می‌دهد که سرقت لپ تاپ دومین شکل رایج برای کلاهبرداری کامپیوتری در سال ۲۰۰۳ بوده که ۴۷ درصد از پاسخ دهندگان اشاره کرده اند که سازمان آنها قربانی دزدیده شدن لپ تاپ شده است. (انجمن امنیت کامپیوتری ۲۰۰۳). با وجودی که جایگزینی یک لپ تاپ در برخی شرایط می‌تواند گران باشد، اما خطر سرقت لپ تاپ این است که فرد سارق لپ تاپ اکنون قادر است تا به شبکه‌های داخلی سازمان دسترسی پیدا کرده، و همچنین هرگونه فعالیت تقلبی و کلاهبرداری یا تخریبی را انجام داده و مشکلاتی را در سازمان به وجود آورد. دزدیدن لپ تاپ تنها شیوه سرقت سخت افزار کامپیوتری نمی‌باشد. واحدهای پردازشگر مرکزی[۵۶] (CPU)، آسیستان‌های دیجیتال شخصی [۵۷](PDA)، فلش مموری[۵۸]، و انواع دیگری از سخت افزارهای کامپیوتری غالباً اهداف آسانی برای دزدی محسوب می‌شوند. هر گونه ابزار قابل حمل کامپیوتری یا سخت افزار کامپیوتری که حرکت دادن آن آسان باشد، اهداف ساده ای برای سرقت سخت افزارهای کامپیوتری هستند. در هر حالتی که طی آن سخت افزار کامپیوتری مورد سرقت قرار می‌گیرد، ممکن است دسترسی به داده‌های حساس یا شبکه‌های کامپیوتری را موجب شود، که در هر حال می‌تواند برای سازمان هزینه زا باشد.

استفاده از فناوری برای جلوگیری و تشخیص جرائم کامپیوتری

جرائم و تقلب‌های کامپیوتری را می‌توان به طرقی مختلفی شناسائی و از ارتکاب آنها جلوگیری نمود. کنترلهای فیزیکی، نظیر قفل و دسترسی کنترل شده به مراکز کامپیوتری، سخت افزارها و اسناد مربوط به معاملات حسابداری، می‌توانند باعث جلوگیری از دسترسی مجرم به سیستم اطلاعات حسابداری شود. بیشتر سازمانها برخی از سطوح کنترل‌های فیزیکی را اعمال می‌کنند، اما سازمانهای زیادی نیز برای کمک به

جلوگیری و تشخیص جرائم کامپیوتری و تجاوز به حریم خصوصی شرکت، به استفاده از فناوری روی آورده اند. جلوگیری از جرائم کامپیوتری می‌تواند از اعمال کنترلهای ساده ای نظیر رمزهای عبور شروع شده، و تا سخت افزارهای پیچیده ای ادامه داشته باشد که سیستم اطلاعات را به منظور رخدادهای غیرمعمول یا تغییرات صورت گرفته در سیستم تحت مراقبت قرار می‌دهد. دانشجویان رشته حسابداری بایدجهت جلوگیری و تشخیص جرائم کامپیوتری نسبت به استفاده از فناوری، چه ساده و چه پیچیده، آگاه باشند، زیرا تقریباً تمامی‌سازمانها سیستم‌های اطلاعاتی خود را کامپیوتری کرده، و این سیستم‌ها به طور متنوعی از اشکال مختلف فناوری برای جلوگیری و تشخیص جرائم استفاده می‌کنند. دانشجوی حسابداری بدون داشتن دانش در زمینه این تکنیکها دچار نقصان اطلاعاتی می‌شوند.

این بخش به بررسی چندین تکنیک می‌پردازد که معمولاً برای جلوگیری از دسترسی به سیستم اطلاعاتی و نیز تشخیص تجاوز به حریم غیرمجاز در صورت وقوع، مورد استفاده قرار می‌گیرد. این فهرست از روشهای پیشگیری و تشخیص کامپیوتری جامع و فراگیر نمی‌باشد. بلکه این فهرست تنها برای ارائه ایده‌هایی از انواع کنترلهای مورد استفاده جهت جلوگیری از جرائم و کلاهبرداریهای کامپیوتری ارائه گردیده است.

۱) کنترل دسترسی به سیستم کامپیوتری [۵۹]

همانطور که در بالا اشاره شد، اولویت سازمانها جلوگیری از ایجاد جرائم کامپیوتری قبل از ارتکاب آن است. اولین خط دفاعی، دسترسی پیشگیرانه به سیستم کامپیوتری است که این کار برای جلوگیری از دسترسی فیزیکی به سیستم کامپیوتری صورت می‌گیرد. اما هنگامی‌که شخصی دسترسی فیزیکی پیدا می‌کند، خط دفاعی دیگری باید جهت ممنوعیت ورود به سیستم کامپیوتری اعمال گردد. از جمله تکنیکهایی که به طور رایج برای کنترل دسترسی به سیستم کامپیوتری مورد استفاده قرار می‌گیرند عبارتند از : قرار دادن رمز عبور[۶۰]، سیستم‌های بیومتریک[۶۱]، و دیواره آتشین[۶۲]. شاید شایع ترین نوع کنترل دسترسی فیزیکی به سیستم کامپیوتری، قرار دادن رمز عبور یا همان پسورد باشد. افراد باید برای دسترسی به یک سیستم کامپیوتری، ملزم به داشتن یک رمز عبور، به ویژه همراه با یک شناسه کاربری، می‌باشند. رمز عبور تا اندازه ای در برابر دسترسی غیرمجاز به سیستم کامپیوتری اطمینان ایجاد می‌کند، اما این روش هم به هیچ وجه شکست ناپذیر نیست. حدس زدن بسیاری از رمزهای عبور آسان بوده، و اگر هم حفاظتی را برای شرکت و سازمان ایجاد کنند، میزان آن چندان قابل توجه نخواهد بود. بنابراین، رمز عبور نباید به تنهائی به عنوان کنترل کامل برای دسترسی غیرمجاز مورد استفاده قرار گیرند.

روش دیگری که برای کنترل دسترسی به سیستم کامپیوتری به کار گرفته می‌شود سیستم بیومتریک است در این سیستم برای اجازه یا عدم اجازه دسترسی به سیستم کامپیوتری یا برخی بخشهای حفاظتی در یک ساختمان، از برخی مشخصه‌های فیزیکی استفاده می‌شود. ابزارهای بیومتریک سیستم‌هایی هستند که برای تشخیص افراد مجاز به ورود به قسمتهای خاصی از ساختمان که در آن سیستمهای کامپیوتری نگهداری می‌شوند، با استفاده از اسکنرها مشخصه‌های خاصی مانند اثر انگشت، صدا، الگوهای شبکیه چشم، و حتی امضا یا الگوهای صفحه کلید را کنترل می‌کنند (هال ۲۰۰۴). استفاده از سیستم‌های بیومتریک برای کنترل دسترسی به دلیل کاهش هزینه‌های این فناوری روز به روز شایع تر می‌شود. سازمانها نیز می‌توانند این سیستم‌ها را همراه با سیستم‌های دیگر استفاده کنند،

زیرا سیستم‌های بیومتریک همانند رمز عبور کاملاً بی عیب نمی‌باشند.

سیستم‌های دیواره آتشین به طور رایج برای جلوگیری از دسترسی غیرمجاز به سیستم‌های اطلاعاتی توسط افراد خارج از سازمان مورد استفاده قرار می‌گیرد. سیستم‌های دیواره آتشین به طور بارز ترکیبی از سخت افزار و نرم افزارهایی است که به عنوان سپری بین سازمان و دنیای خارج از آن، معمولاً اینترنت یا شبکه‌های داخلی[۶۳]، عمل می‌کنند («رومنی» و «استین بارت» ۲۰۰۳، «هال» ۲۰۰۴). سیستم دیواره آتشین در عمل به صورت فیلتری برای حفظ و جلوگیری از ارتباطات ناخواسته، چه از خارج به داخل و یا بالعکس، عمل می‌کند. برخی سازمانها نیز اطلاعاتی را که می‌خواهند دور از دسترس دیگران باشند، بر روی سرور اینترنتی جداگانه ای در پشت دیواره آتشین قرار می‌دهند. این سرور به عنوان سپر بین دنیای خارج و سیستم اطلاعاتی سازمان عمل می‌کند. اگر هکر به سرور اینترنتی دسترسی پیدا کند، تنها می‌تواند اطلاعات عمومی‌را تخریب کرده یا سرقت کند، زیرا اطلاعات محرمانه یا حساس در سرور جداگانه ای ذخیره شده اند که برای آنها از طریق دیواره آتشین محافظت بیشتری در برابر دنیای خارج ایجاد شده است.

۲) کنترل ورودی داده‌ها[۶۴]

همانطور که در بالا اشاره شد، فرآیند ورودی، حیاتی ترین فرآیند در سیستم اطلاعاتی یک سازمان است. داده‌هایی که وارد سیستم اطلاعاتی می‌شوند، همان چیزی هستند که پردازش شده و به صورت خروجی در می‌آیند. سیستم‌های اطلاعاتی کامپیوتری معمولاً از برخی از انواع روشهای تأیید ورودیها جهت بررسی داده‌های ورودی استفاده می‌کنند. این مسیرهای تأییدی می‌توانند به صورت ساده، مانند چک کردن انواع کاراکترهای ورودی در بخشهای خاص، یا به صورت پیچیده تر، مانند مسیرهایی که منطقی بودن داده‌های ورودی به این قسمتها را بررسی می‌کنند، باشند. از جمله دیگر نمونه‌های مسیرهای تأییدیه درسیستم‌های کامپیوتری می‌توان به بررسی صحت اطلاعاتی، بررسی امضا،بررسی کامل بودن، بررسی توالی ورودی،وبررسی سازگاری اطلاعاتی اشاره کرد(«موسکوف» وهمکاران[۶۵] ۲۰۰۳، «هال» ۲۰۰۴).

اگر شخص متخلف، همان فردی باشد که داده را وارد سیستم می‌کند، پس کنترل‌های مربوط به ورودی داده‌ها نمی‌تواند چندان مؤثر باشد. اگر شخص متخلف بتواند به ابزارهای ورودی داده‌ها دسترسی پیدا کند، پس وی قادر است تا به مسیرهای ورودی سیستم اطلاعاتی نیز دسترسی غیرمجاز داشته باشد. کنترلهای دسترسی و نیز مسیرهای تأیید صحت و سقم داده‌ها می‌تواند پایگاه دادها را در برابر چنین تقلب‌هائی محافظت نماید، اما این کنترلها نیز، همانند بسیاری از موارد کنترلی، صد در صد ایمن و شکست ناپذیر نمی‌باشند.

۳) کنترل خروجی داده‌ها از سیستم کامپیوتری[۶۶]

هدف از سیستم اطلاعاتی حسابداری اینست که قادر باشیم به اطلاعات مفیدی که برای تصمیم گیریهای ما مرتبط و ضروری می‌باشند، دسترسی پیدا کنیم. با وجودی که فرآیند ورودی داده‌ها می‌تواند اساسی ترین فرآیند در سیستم اطلاعاتی باشد، اما خروجیهای سیستم نیز باید کنترل شوند. بسیاری از مجرمان جرائم کامپیوتری برای یافتن اطلاعات حساس یا خصوصی، که می‌تواند برای ارتکاب جرائم شان مورد استفاده قرار گیرد، از اطلاعات سطل زباله کامپیوتر که به صورت مجازی پاک شده اند استفاده می‌کنند. با وجودی که سرقت اسناد از روی حافظه کامپیوتری را نمی‌توان به لحاظ فنی نوعی جرم کامپیوتری به حساب آورد، اما در هر حال خروجی سرقت شده از طریق سیستم اطلاعاتی کامپیوتری به

دست آمده است. روشهای کنترل خروجی از یک حافظه کامپیوتری عبارتند از : امحاء تمامی‌اسنادی که دیگر مورد نیاز نمی‌باشند، تهیه و استفاده از لیستهای کنترلی که نشان دهد چه کسانی ودر چه حدی می‌توانند گزارشات را دریافت کنند، ضمناً روشهای بایگانی اسناد و نحوه حفاظت از آنها از جمله این کنترلها هستند.

قطع ارتباطات الکترونیکی از دیگر روشهایی است که مجرمان برای سرقت خروجی کامپیوتری مورد استفاده قرار می‌دهند. این شکل از جرائم کامپیوتری شبیه به استراق سمع و ضبط مکالمات[۶۷] می‌باشد. شایع ترین روش برای پیشگیری از سرقت داده‌هایی که به طور الکترونیکی در حال انتقال هستند، کدگذاری یا رمزگذاری[۶۸] می‌باشد. رمزگذاری عبارتست از درهم ریختن داده‌هایی که از طریق خطوط ارتباطی انتقال داده می‌شوند («موسکوف» و همکاران، ۲۰۰۳، «هال» ۲۰۰۴). اگر این داده‌ها مورد سرقت قرار گیرند، شخص سارق تنها داده‌های درهم و برهمی‌را در اختیار دارد که نمی‌تواند از آنها استفاده نماید. شخصی که به طور مجاز از داده‌های رمزی استفاده می‌کند باید کلید رمز[۶۹] را در اختیار داشته باشد تا این داده‌ها را رمزگشائی نماید. این داده‌ها بدون در اختیار داشتن کلید رمز عملاً بی استفاده و بی فایده خواهند بود. همچنین برای رمزگذاری داده‌های ذخیره شده در پایگاه داده‌ها، از کدگذاری یا رمزگذاری استفاده می‌شود تا بدین وسیله از این داده‌ها در برابر حملات هکرها محافظت شود («هال» ۲۰۰۴).

٤) جلوگیری و تشخیص برنامه‌های تخریبی[۷۰] و از بین بردن آنها

گزارش ارزیابیCSI/FBI در آمریکا نشان می‌دهد که ۸۲ درصد سازمانها بررسی شده در این گزارش، نوعی حمله از طریق برنامه‌های تخریبی را گزارش کرده اند. به طرق زیادی می‌توان از حملات ویروس‌های کامپیوتری جلوگیری کرد. دو روش جلوگیری از آسیبهای ویروس کامپیوتری عبارتند از روشهای کنترلی آنتی ویروس[۷۱] (جلوگیری از ورود ویروس با استفاده از نرم افزار آنتی ویروس) و روشهای ویروس کشی با استفاده از نرم افزارهای ویروس کش. رویه‌های کنترلی برای هر دو روش مقابله با ویروس شامل نکاتی به شرح ذیل می‌باشد :

- خرید نرم افزار مورد نیاز از فروشندگان معتبر[۷۲]،
- اجتناب از خرید نسخه کپی شده نرم افزار،
- ممنوعیت دانلود کردن فایلهای نرم افزاری از طریق اینترنت،
- حذف پیامهای الکترونیکی از سوی منابع ناشناس بدون باز کردن آنها،
- عدم مبادله اطلاعات از طریق دیسکهای کامپیوتری،
- اجرای دوره ای ویروس اسکن (ویروس کشی) به وسیله نرم افزار آنتی ویروس معتبر («موسکوف» و همکاران ۲۰۰۳).

با وجودی که سازمانهای زیادی برنامه‌های آنتی ویروس را به کار گرفته اند، اما ویروسها و کرمهای کامپیوتری به صورت مداوم وارد سیستم کامپیوتری می‌شوند. نرم افزار آنتی ویروس، اقدام محافظتی خوبی در برابر چنین خرابکاری‌هائی می‌باشد. نرم افزار آنتی ویروس، ورودی و فایل‌های کامپیوتری یا شبکه را به لحاظ کد کامپیوتری که شبیه به کد ویروس‌های شناخته شده می‌باشد، را اسکن می‌کند. برنامه‌های آنتی ویروس عموماً دارای خصوصیتی هستند که می‌توانند به محض دانلود شدن ویروس از طریق ایمیل یا روشهای دیگر، آنها را حذف کنند. در این مورد، نرم افزار آنتی ویروس به عنوان کنترل پیشگیرانه عمل می‌کند. جلوگیری از ورود ویروسها بهترین راه برای محافظت از سیستم اطلاعاتی در برابر آسیبها می‌باشد،

اما اگر واقع بینانه تر بنگریم، کامپیوترها ویروسی می‌شوند. در این حالت، با استفاده از نرم افزار آنتی ویروس می‌توان ویروس را از بین برده و یا آن را در قرنطینه قرار داد.

رویه‌های کنترلی آنتی ویروس غالباً شیوه‌های پیشگیرانه بهتری، نسبت به نرم افزار آنتی ویروس که ویروس را از بین می‌برند می‌باشد. هر روزه ویروسهای جدیدی ایجاد شده، و بسیاری از فروشندگان نرم افزار آنتی ویروس برای به روز نگه داشتن مجموعه آنتی ویروسهای خود با مشکل روبرو هستند. در این حالت، ممکن است برخی ویروسها یا کرمها تا زمان به روز رسانی نرم افزار مربوطه، حذف نشوند. همچنین، سازمانهای زیادی مسئولیت اسکن کردن ویروسهای کامپیوتری را به کاربران شخصی کامپیوتری محول می‌کنند. این کاربران اغلب زمان لازم را برای اسکن نمودن ویروسها صرف نمی‌کنند که این امر می‌تواند احتمال آسیب دیدن شبکه سازمان به وسیله ویروسها را افزایش دهد. چنین آسیب بالقوه ناشی از برنامه تخریبی حتی می‌تواند برای بزرگترین سازمانها مشکل ساز و آسیب رسان باشد.

۵) شناسائی ورود غیر مجاز به حریم سیستم کامپیوتری [۷۳]

سازمانها به طور طبیعی می‌خواهند از ورودهای غیرمجاز و تعدی به سیستم اطلاعاتی شان جلوگیری به عمل آورند، اما هکرها می‌توانند بسیاری از این شیوه‌های کنترلی پیشگیرانه ای را که سازمانها اجرا می‌کنند، پشت سربگذارند. در چنین حالتی، سازمان باید قادر به تشخیص ورود غیرمجاز به حریم سیستم کامپیوتری باشد تا اقدام لازم جهت متوقف ساختن آن را انجام دهد. برای تشخیص تعدی به حریم غیرمجاز در سیستم اطلاعاتی کامپیوتری، چندین روش را می‌توان به کار گرفت. نمونه‌هایی از فناوریهای تشخیص ورود غیرمجاز که به کار گرفته می‌شوند عبارتند از: دروبین‌های مدار بسته[۷۴]، قرار دادن طعمه ای جهت حریص کردن فرد متخلف[۷۵]، و سیستم‌های تشخیص موارد غیرعادی[۷۶]. هنگامی‌که هر یک از این روشها ورود غیرمجاز به سیستم کامپیوتری را تشخیص دادند، سازمان می‌تواند موارد ذیل را شناسایی کند: چه کسی و به چه چیزی دسترسی پیدا کرده، زمان وقوع این دسترسی غیرمجاز، و اینکه آیا آسیبی وارد ساخته است یا خیر، و... با داشتن چنین اطلاعاتی سازمان می‌تواند برای جلوگیری از تکرار چنین تخلفاتی و ورودهای غیرمجاز در آینده، معیارهای پیشگیرانه لازم را به کار گیرد. یک روش برای ایجاد روشهای کنترلی جدید، استفاده از ابزارهای بررسی آسیب پذیری می‌باشد. از این ابزارها برای بررسی سیستم کامپیوتری درمواردی که ممکن است خطرات امنیتی بالقوه ای وجود داشته باشد، استفاده می‌شود. در حالیکه ابزارهای بررسی آسیب پذیری عموماً به عنوان معیارهای پیشگیرانه تلقی می‌شوند، اما غالباً از این ابزارها برای مراقبت و تشخیص الگوهای مشکوک کاربری و یا تغییرات موجود در ترکیباتی که ناشی از حمله هکرها می‌باشد، استفاده می‌گردد («لولفینگ» و همکاران ۲۰۰۳).

دوربین‌های مدار بسته در فواصل زمانی مشخص، عکسهایی[۷۷] (ضبط وضعیتهای کامپیوتر در یک لحظه) از مشخصه‌های کلیدی سیستم می‌گیرد. هنگامی‌که هکرها وارد سیستم کامپیوتری می‌شوند، به طور ناآگاهانه فایلها و مسیرها را تغییر می‌دهند. ابزارهای دوربین مدار بسته این تغییرات را تشخیص داده و به سازمان هشدار می‌دهد که تغییرات غیرمجازی در سیستم کامپیوتری ایجاد گردیده است. سیستم تشخیص موارد غیرعادی نیز شبیه به دوربین‌های مدار بسته هستند. این سیستمها نیز به بررسی سیستم‌های اطلاعاتی به لحاظ تغییرات اعمال شده در فعالیتهای پیش بینی شده می‌پردازند. این تغییرات سرنخ‌هایی را

نشان می‌دهند که یک تخلف کامپیوتری رخ داده است («لو لفینگ» و همکاران ۲۰۰۳).

قرار دادن طعمه ای جهت حریص کردن فرد متخلف در مواردی به کار برده می‌شود که هکر به اندازه کافی کار خود را ادامه داده است تا شناسائی و احتمالاً بازداشت او امکان پذیر باشد. در این روش پس از تشخیص ورود غیرمجاز به حریم سیستم کامپیوتری برخی از شواهد ورود غیرمجاز، که می‌تواند در پیگرد قانونی هکر در صورت دستگیر شدن مفید باشد، ذخیره می‌شود («لولفینگ» و همکاران ۲۰۰۳).

با وجودی که این روشها می‌توانند برای تشخیص ورودهای غیرمجاز مؤثر باشند، اما هیچیک از آنها صد در صد عاری از خطا یا شکست نمی‌باشند. این برنامه‌ها همانند هر برنامه دیگری نمی‌توانند دقیقاً به گونه ای که برنامه ریزی شده اند، عمل کنند. در برخی موارد، صرفاً به کارگیری سیستم تشخیص ورود غیرمجاز ممکن است کافی نباشد. تغییرات قانونی و مجاز می‌تواند سیستم را در تشخیص ورودهای غیرمجاز دچار اشتباه کند. همچنین، هکرهای باتجربه ممکن است قادر باشند تا به راحتی از پس این تکنیکهای شناسائی برآیند («لولفینگ» و همکاران ۲۰۰۳). البته داشتن این سیستمها علیرغم محدودیت‌هایشان، بهتر از آنست که اصلاً هیچ سیستمی‌برای تشخیص ورود غیرمجاز نداشته باشیم.

دانشجویان حسابداری نسبت به فراگیری علوم کامپیوتری ودانش شناسایی تقلب، شامل تقلب‌هایی که با استفاده از کامپیوتر صورت می‌گیرد، و نیز اخلاق حرفه ای، نیاز مبرم دارند. دانشجویان باید در مورد انواع جرائم کامپیوتری که روی می‌دهد، ارگانها یا افرادی که به پژوهش در مورد این جرائم می‌پردازند، و چگونگی تشخیص این جرائم، به ویژه اگر قصد کار کردن در حوزه فناوری را داشته باشد، آگاهی داشته باشند. هیچ واحد درسی حسابداری به تنهائی نمی‌تواند تمامی‌موارد اطلاعاتی فوق را برای دانشجویان حسابداری فراهم آورد. «کالون[۷۸]» و همکاران (۱۹۹۹) بر این باورند که واحددرسی اخلاق حرفه ای باید بخشی از برنامه آموزشی دانشگاهها باشد. این مقاله استفاده از چهار عنوان درسی برای آموزش دانشجویان رشته حسابداری در مورد فراگیری زبانهای برنامه نویسی و بانکهای اطلاعاتی،جرائم و تقلب‌های کامپیوتری، تشخیص تقلب، و موازین اخلاق حرفه ای و نحوه رعایت آن را پیشنهاد می‌کند. این چهار عنوان درسی عبارتند از آشنایی با مبانی زبان‌های برنامه نویسی و بانکهای اطلاعاتی ویژه حسابداری، سیستم‌های اطلاعاتی حسابداری، تشخیص تقلب و یا واحد حسابداری حقوقی، و موازین اخلاق حرفه ای حسابداری می‌باشند. البته، واحد درسی حسابرسی سنتی نیز می‌بایست مباحث تقلب و کنترلهای داخلی، به ویژه موارد رسوائی‌های مفتضحانه تقلب در حسابداری در چند سال گذشته، نظیر شرکت‌های «انرون»، «ورلدکام»، «آدلفیا»، و «تیکو»[۷۹]، رخ داده است را پوشش دهد. بنابراین، به مباحث واحدهای درسی حسابرسی باید مبحث آموزش دانشجویان حسابداری در زمینه اخلاق حرفه ای نیز افزوده شود.

۱) آشنایی با مبانی زبانهای برنامه نویسی و بانکهای اطلاعاتی ویژه حسابداری

دانشجویان حسابداری به دانش کاربردی قابل قبولی در زمینه آشنایی با زبانهای برنامه نویسی و بانکهای اطلاعاتی، نیاز دارند. معیارهای این آشنایی عبارتند بودند از معیارهای فنی به ترتیب اهمیت عبارتند از : استفاده از زبان برنامه نویسی و بانک اطلاعاتی مناسب با توجه به نیازهای جاری و آتی،سهولت بکارگیری نرم افزارحسابداری،کارایی سیستم بکارگرفته شده وامنیت آنها.

معیارهای مدیریتی به ترتیب اهمیت عبارتند از :هزینه تهیه نرم افزار، هزینه خرید سخت افزارهای مورد نیازسیستم نرم افزاری، اعتبار فروشندگان نرم افزار و سخت افزار واطمینان از پشتیبانی و خدمات بعد از فروش آنها و قابلیت گزارش دهی مناسب و با انعطاف .

با توجه به معیارهای فوق الذکر میتوان نتیجه گرفت که دانشجویان رشته حسابداری می‌بایست آشنایی کافی در مورد زبانهای برنامه نویسی، بانکهای اطلاعاتی داشته باشند ودر طول تحصیل نیز حداقل با چند نرم افزار حسابداری معتبر به صورت عملی کار کرده باشند، که البته این مهم با توجه به واحدهای درسی و نحوه آموزش دانشجویان حسابداری درتمام مقاطع تحصیلی مورد توجه قرار نگرفته است و متاسفانه دانشجویان بعد از فارغ التحصیل شدن و ورود به بازار کار با مشکلات فراونی روبرو می‌شوند.

تقریباً تمامی‌دانشگاهها در واحدهای درسی رشته حسابداری درس آشنایی با کامپیوتر و مبانی آن را، چه به صورت واحدهای الزامی‌و چه به صورت واحد اختیاری، در خود جای داده اند. اما عموماً پوشش این واحدهای درسی، چه به صورت معرفی کتاب یا به صورت جزوات استاد، شامل مباحثی در مورد آشنایی با کامپیوتر، مطالب عمومی‌و زبانهای قدیمی‌برنامه نویسی می‌شود. همچنین این واحدها شامل مباحث کلی در زمینه قالبهای عمومی‌مباحث مربوط به کامپیوترمی‌باشند. این واحدهای درسی با توجه به سرفصلهای مصوب جوابگوی نیاز فعلی دانشجویان حسابداری نمی‌باشد.. از این گذشته، کتب حاضر به ندرت مباحث اصلی مربوط سیستم حسابداری و کامپیوتری را با جزئیات کافی پوشش می‌دهند. بنابراین، برنامه آموزشی حسابداری باید واحدهای دیگری را نیز در خود جای دهد که به دانشجویان این اجازه را بدهد تا دانش بیشتری در حوزه زبانهای برنامه نویسی و بانکهای اطلاعاتی را به دست آورند.

سر فصلهایی پیشنهادی که برای این واحد درسی می‌تواند مفید باشد عبارتند از :

- معرفی انواع زبانهای برنامه نویسی و بیان نقاط قوت و ضعف هر یک از آنها
- معرفی انواع بانکهای اطلاعاتی و بیان نقاط قوت و ضعف هر یک از آنها
- بیان چارچوب کلی یک نرم افزار حسابداری
- معرفی چند نرم افزار حسابداری معتبر و برگزاری دوره عملی با همکاری شرکتهای نرم افزار نویسی به صورت متمرکز
- مصاحبه و دعوت به سخنرانی نرم افزار نویسان برای ایجاد ارتباط و ادبیات مشترک برای تعاملات آتی

۲) سیستم‌های اطلاعاتی حسابداری

دیگر واحد پیشنهادی واحد درسی AIS [۸۰](سیستم‌های اطلاعاتی حسابداری) است،تقریباً تمامی برنامه‌های آموزشی حسابداری، این واحددرسی را نیز، چه به صورت واحدهای الزامی‌و چه به صورت واحد اختیاری، در خود جای می‌دهند. عموماً پوشش واحد درسی AIS، چه به صورت معرفی کتاب یا به صورت جزوات استاد، شامل مباحثی در مورد تقلب، نظیر جرائم کامپیوتری، و کنترلهای داخلی می‌باشد. همچنین این واحدها شامل مباحث کلی در زمینه رعایت موازین اخلاق حرفه ای در حسابداری و سیستم‌های اطلاعاتی می‌باشند. واحدهای AIS نقطه شروع مناسبی برای برنامه آموزشی دانشجویان رشته حسابداری است، اما به دلیل تعدد مباحثی که در بیشتر واحدهای AIS گنجانده می‌شود، تدریس مبحث رعایت موازین اخلاق حرفه ای در محیط‌های کامپیوتری معمولاً به صورت

جامعی صورت نمی‌گیرد. برای مثال، در بسیاری از کتب مربوط به واحد AIS حداقل یک فصل را به مباحث تقلب و کنترلهای داخلی به کار رفته برای جلوگیری و تشخیص آن اختصاص داده اند، اما تنها بخشی از یک فصل از این کتابها معمولاً به مبحث رعایت موازین اخلاق حرفه ای در تجارت می‌پردازد. بنابراین، برنامه آموزشی حسابداری باید واحدهای دیگری را نیز در خود جای دهد که به دانشجویان این امکان را بدهد تا دانش بیشتری در حوزه تقلب کامپیوتری و رعایت موازین اخلاق حرفه ای به دست آورند. البته با توجه به اینکه این واحد درسی در کشور در مقطع کاردانی به کارشناسی ایجاد شده و دارای سرفصل مصوب می‌باشد پیشنهاد می‌شود برای دوره کارشناسی پیوسته نیز اجباری شود. وسرفصلهای آن نیز علی الخصوص در زمینه سیستمهای کامپیوتری حداکثر دو سال یکبار به روز رسانی شود.

۳) واحد کشف تقلب (حسابداری حقوقی)

دیگر واحد پیشنهادی، واحد کشف تقلب یا حسابداری حقوقی است. اگر فردی می‌خواهد جزئیات یک تقلب یا کلاهبرداری صورت گرفته را درک کند، باید انواع مختلف کلاهبرداریها و نیز چگونگی ارتکاب آنها را بلد باشد واحدکشف کلاهبرداری یا تقلب جائی منطقی برای تدریس این مباحث به دانشجویان حسابداری می‌باشد.

واحد درسی کشف کلاهبرداری باید به دقت چگونگی و دلیل روی دادن کلاهبرداریها و تقلبها را موردمطالعه قرار دهد.جرائم و کلاهبرداریهای کامپیوتری که با استفاده ازکامپیوتر صورت می‌گیرد، باید شامل مبحثی در این زمینه باشند، زیرا تمامی‌سازمانها عملاً سیستم اطلاعاتی کامپیوتری دارند.

همچنین در واحد حسابداری حقوقی یا کشف کلاهبرداری باید موضوع برحذر داشتن از انجام کلاهبرداری گنجانده شود. در همه جا این قضیه مطرح می‌شود، جلوگیری از ارتکاب کلاهبرداری بر تشخیص کلاهبرداری پس از آنکه به وقوع پیوسته است، اولویت دارد. واحدهای حسابرسی و AIS معمولاً شامل مباحثی ازکنترل‌های داخلی و جلوگیری از کلاهبرداری باشد، اما درک تکنیک‌های جلوگیری از تقلب می‌تواند در درک چگونگی ارتکاب اینگونه جرائم به دانشجویان حسابداری کمک کند.

سرانجام، واحد کشف کلاهبرداری باید شامل مبحثی از چگونگی پژوهش در مورد کلاهبرداریها و نیز چگونگی برطرف ساختن آنها باشد. در صورت امکان، مبحث سازمانهائی که معمولاً به پژوهش در مورد جرائم کامپیوتری می‌پردازند نیز باید در این واحد درسی گنجانده شود. مطالعات موردی، به دلیل حجم گسترده ای از اطلاعات در مورد کلاهبرداری در مقالات دانشگاهی برای واحد درسی مربوط به کشف تقلب مناسب می‌باشند. سخنرانان مدعو می‌توانند با در اختیار گذاشتن تجربیات خود در زمینه کشف کلاهبرداری مکملی برای این واحد درسی باشند به گونه ای که دانشجویان بتوانند میزان اهمیت این مبحث در حرفه حسابداری را درک نمایند. با در کنار هم قرار دادن دانش اساتید این رشته و تجربیات سخنرانان مدعو می‌توان محتوای ارزشمندی را برای این واحد درسی فراهم آورد.

سرفصلهای پیشنهادی که ممکن است در واحدهای درسی جلوگیری و کشف تقلب و کلاهبرداری گنجانده شوند، عبارتند از:

- طبقه بندی کلی تقلبها، یعنی تقلب در صورتهای مالی، اختلاس، تقلب مالیاتی،... و کلاهبرداریهای خاصی که در هر دسته جای می‌گیرند، شامل جرائم کامپیوتری در موارد کاربردی،
- بیان انگیزه‌های اشخاص متخلف،

- معرفی چارچوبهای کنترلی، به ویژه جهت جلو گیری از تقلبهای کامپیوتری،
- ابزارهای کشف کلاهبرداری وروشهای تشخیص آن، به ویژه در محیط‌های کامپیوتری،
- مصاحبه با پژوهشگران و بررسی کنندگان کلاهبرداریها، و
- معرفی سازمانهای تحقیق کننده در زمینه کلاهبرداریهاو بیان شیوه عمل آنها.

برخی دانشکده‌های حسابداری در آمریکا قبلاً واحدهای حسابداری حقوقی یا کشف کلاهبرداری را ارائه می‌کردند و برخی دیگر نیز ممکن است برنامه‌هایی برای ایجاد چنین واحدی جهت ارائه در آینده ای نزدیک داشته باشند. بسیاری از دانشگاهیان رشته حسابداری تجربیاتی در زمینه کشف تقلب در حسابداری دارند زیرا ممکن است بعضی از آنان قبل از روی آوردن به حوزه تدریس، حسابرس بوده اند. حسابرسان اغلب در معرض کشف و پژوهش در مورد کلاهبرداری در کارهایی که برای مشتریان خود انجام می‌داده اند، بوده اند. بنابراین، اساتید رشته حسابداری که تجربه عملی نیز دارند برای تدریس واحد کشف کلاهبرداری مناسب می‌باشند. بسیاری از گروههای حقوق جزاء واحدهای مشابهی در زمینه کلاهبرداری را به عنوان جایگزینی برای واحد کشف کلاهبرداری ارائه می‌نمایند، هرچند که چنین واحدهائی معمولاً به کلاهبرداری‌های حسابداری متمرکز نمی‌شوند و ممکن است چندان به جرائم کامپیوتری نیز نپردازند. برای برنامه‌های حسابداری که اساتید باتجربه ای در حوزه کشف کلاهبرداری ندارند یا اینکه در پی دیدگاه متفاوتی در این زمینه هستند، استفاده از واحد حقوق جزاء به عنوان مکملی برای آموزش حسابداری می‌تواند گزینه قابل قبولی باشد.

۴) موازین اخلاق حرفه ای در حسابداری

واحد دیگری که می‌تواند به آموزش دانشجویان رشته حسابداری کمک کند، واحد موازین اخلاق حرفه ای در حسابداری یا تجارت می‌باشد. همانطور که قبلاً اشاره شد، تقریباً تمامی‌واحدهای حسابداری مباحثی در مورد اخلاق حرفه ای را در خود جای داده اند. اما در بسیاری از موارد نیز این مباحث محدود بوده و ممکن است برای متقاعد ساختن دانشجویان در مورد اینکه رعایت موازین اخلاقی برای حرفه حسابداری و نیز در دنیای تجارت از اهمیت اساسی برخوردارند، کافی نباشد. به دنبال رسوائی‌های اخیر در حسابداری، اظهار نظرهائی در آمریکا مبنی بر این صورت گرفت که دانشجویان حسابداری باید واحد موازین اخلاق حرفه ای را به عنوان بخشی از آمادگی خود برای حرفه حسابداری اخذ نمایند.

واحد اخلاق حرفه ای ترجیحاً باید توسط اساتید رشته حسابداری تدریس شود، و این واحد درسی باید بیشتر به مباحث اخلاق حرفه ای در حسابداری و تجارت تا موازین اخلاقی به صورت عمومی‌بپردازد. گروههای فلسفی در بسیاری از دانشگاهها واحدهائی را در زمینه اخلاق حرفه ای ارائه می‌نمایند که این واحدها به بررسی مفاهیم اخلاق حرفه ای و تشخیص درست از غلط می‌پردازند. اما واحد اخلاق حرفه ای در رشته حسابداری یا تجارت بیشتر توجه خود را به محیط حسابداری یا تجارت معطوف می‌سازد، به گونه ای که دانشجویان می‌توانند مباحث اخلاقی را با آماده شدن برای حرفه حسابداری مرتبط سازند.

واحد درسی موازین اخلاق حرفه ای در حسابداری تا حد امکان شامل رویدادهای جاری می‌باشد. بررسی‌ها و آزمون‌های صورت گرفته در مورد کلاهبرداریهای جاری توسط افراد یا سازمانهایی که متهم به ارتکاب جرم هستند، در بسیاری از رسانه‌های عمومی‌ارئه می‌شوند. اخیراً مقالات دانشگاهی یا غیردانشگاهی زیادی در حوزه حرفه حسابداری و

آموزش دانشجویان حسابداری در مورد اخلاق حرفه ای نوشته شده است.

سرفصل‌های پیشنهادی که می‌تواند درزمینه اخلاق حرفه ای دراین درس گنجانده شود، عبارتند از:

- آئین نامه اخلاق و رفتارحرفه ای،
- اهمیت فرهنگ عمومی‌حسابداری در ارتقاء موازین اخلاق حرفه ای،
- قوانین، مقررات، و استانداردهای مربوط به اخلاق حرفه ای،
- نهادهای نظارتی که مسئول قانونی کردن استانداردهای اخلاق حرفه ای هستند،
- بررسی تفاوتهای اخلاق حرفه ای در میان گروههای مختلف، یعنی مشاغل جدید در برابر مشاغل قدیمی‌تر، اخلاق حرفه ای در برابر اخلاق غیرحرفه ای، و تحلیل تدریجی استانداردهای اخلاقی در سال‌های اخیر،
- مسئولیت حسابدار رسمی‌در قبال مشتری، عموم و حرفه حسابداری،
- چالش‌های پیش روی حسابداری رسمی‌برای حفظ اعتبار و اعتماد عمومی.

این چهارعنوان درسی باید دانشجویان حسابداری را به ساختن چارچوبی اخلاقی تشویق کنند. دانشجویان حسابداری باید دانش کافی در مورد علوم کامپیوتری و تقلب کامپیوتری داشته باشند تا بتوانند برای این حرفه مؤثر واقع شوند. و همچنین این چهار عنوان درسی باید بتواند دانشجویان برای مواجه شدن با کلاه برداری‌های که در طول دوران حرفه ای شان با آنان برخورد می‌کنند، آماده ساخته و اصول اساسی و کافی را در این زمینه در اختیار آنان قرار دهد.

٤ نتیجه‌گیری و بحث

حرفه حسابداری اخیراً با موارد متعددی از کلاهبرداری مواجه شده است که باعث سست شدن اصول و پایه‌های این حرفه گردیده است. برای مثال، شرکت «ورلدکام» و «انرون» هر دو درگیر کلاهبرداریهایی بوده اند که حسابرسان آنها دراین امر دخیل بوده، و شرکتهای «هیلات ساوت[٨١]» و «تیکو» نیز درگیر کلاهبرداریهایی بودند که مدیریت ارشد در آن نقش داشته است. زمانی «آرتور آندرسون»، در شرکت حسابداری «بیگ فایو[٨٢]»، به دلیل فراموشی اصول اخلاقی و صلاحیت اخلاقی اقدام به کلاهبرداری نمود، دیگر به فعالیت خود ادامه نداد. دانشجویان حسابداری باید آگاه باشند که چنین اقداماتی برای این حرفه و یا برای کل جامعه قابل قبول نمی‌باشد. دانشجویان باید در طول دوره تحصیل در برنامه‌های آموزشی حسابداری، تا حد امکان با مباحث اخلاق حرفه ای مواجه شوند. بیشتر واحدهای حسابداری شامل مباحثی در زمینه موازین اخلاق حرفه ای است، اما این مباحث محدود در مورد اخلاق حرفه ای ممکن است کافی نباشند.

این مقاله ضمن بیان حداقل دانش کامپیوتری مورد نیاز برای دانشجویان حسابداری به بررسی چندین نوع جرائم کامپیوتری و روشهای استفاده از فناوری برای جلوگیری و تشخیص جرائم کامپیوتری می‌پردازد. چهارعنوان درسی در این مقاله پیشنهاد می‌شوند که دانش خوبی را در زمینه دانش کامپیوتری،جرائم و اصول اخلاق حرفه ای برای دانشجویان حسابداری فراهم می‌آورند. این چهار واحد درسی عبارتند از: واحد آشنایی با مبانی زبانهای برنامه نویسی و بانکهای اطلاعاتی، واحد AIS، واحد کشف کلاهبرداری یا تقلب(حسابداری حقوقی)، و واحد اخلاق حرفه ای. این واحدها، که باتفاق یکدیگر مورد استفاده قرار می‌گیرند، دانش مورد نیاز را برای دانشجویان حسابداری در هنگام مواجهه با تقلبها یا تصمیمات اخلاقی در طول حرفه حسابداری شان را فراهم خواهد آورد.

فهرست منابع

۱) رحمانی، رضا، (۱۳۸۱)، راهنمای کامل برنامه نویسی،جلد اول و دوم، تهران، انتشارات داده پرداز.

۲) مختارانی، حسین، (۱۳۸۱)، کتاب مرجع برنامه نویسان سیستمهای PC، تهران، چاپ سوم، انتشارات ناقوس

۳) رضوی،سید امیر، (۱۳۸۵)، خود آموز استفاده از بانکهای اطلاعاتی، تهران، انتشارات دانشگاه شیراز.

۴) میرسمیعی،مسعود، (۱۳۸۵)، بکارگیری اکسس در حسابداری،تهران، انتشارات ترمه

۵) عادلی نیا، رحمتی، رضا، (۱۳۸۴)، آزمایشگاه پایگاه داده، تهران، انتشارات دیباگران.

۶) قلی زاده نوری، فرهاد، (۱۳۸۵)، راهنمای جامع ویژال فاکس پرو ۳، تهران، انتشارات علوم پیشگام.

۷) منتظر القائم، علیرضا، (۱۳۸۲)، کتاب آموزشی برنامه نویسی با BASIC، تهران، چاپ چهارم، انتشارات رسا

۸) مولاناپور،رامین،ADO.NETوASP.NET در DELPHI 2005 تهران،۱۳۸۳،انتشارات دیباگران.

۹) جزینی درچه، فرناز، (۱۳۸۲)، VISUAL LIPS برای برنامه نویسی CAD ، تهران، انتشارات رهنما.

۱۰) مولاناپور،رامین، (۱۳۸۲)، وب سایت‌های پویا با ASP.NET تهران، انتشارات علوم روز.

۱۱) یاقوتی، سمیه، (۱۳۸۶)، java برای برنامه نویسی شبکه ای ،تهران، انتشارات گل واژه.

۱۲) بسیاری، مهدی، (۱۳۸۱)، مدیریت سیستمهای اطلاعاتی، تهران نشر انتیستیتو ایز ایران.

۱۳) فارسانی ،حسینعلی، (۱۳۸۳)، Oracle زبانی برای بایدها و نبایدها، تهران، انتشارات علوم روز.

14) Boyce,J. (1996), Windows NT 4.0 Installation & Configuration Handbook, QUE.

15) O'Leary. T.J & O'Leary.L.I (2002), Microsoft Office XP (Volume 1), Mc Graw Hill\Irwin.

16) Sheldon,T. (1997), BASIC 2006 ,Osborn , Macgraw Hill.

17) Microsoft Technical Refrence, delphi & java , 2008 ,Audit &control.

18) perry.james (2000), T.&Schneider. Gary. Building Accounting System Access (VOLUME1) , P.(2001) ,Cover to cover publishing,Inc.

19) Ridly,J. (1994), Oracle Networking, John Wiley.

20) American Institute of Certified Public Accountants. (2004). Antifraud Resource Center accessed on 3/30/2004 at http://www.aicpa.org/antifraud/

21) Calhoun, C. H., M. E. Oliverio, and P. Wolitzer. (1999). Ethics and the CPA: Building Trust and Value Added Services. John Wiley & Sons, Inc.: New York, NY .

22) Casabona, P. and S. Yu. (1998). Computer Fraud: Financial and Ethical Implications. Review of Business

23) Computer Security Institute. (2003). CSI/FBI Computer Crime and Security Survey. Computer Security Institute: San Francisco, CA .

24) Hall, J. A. (2007), Accounting Information Systems, 4th Edition. South-Western College Publishing: Mason, OH .

25) Harris, S. (2003). Fighting Pirates. Government Executive 7-Luehlfing, M. S., C. M. Daily, T. J. Phillips, Jr., and L. M. Smith. Cyber Crimes , Intrusion, Detection ,and Computer Forensics. Internal Auditor .

26) McGillivray, G. (2000). Hazards of the Information Superhighway..Canadian Underwriter.

27) Moscove, S., M. Simkin, and N. Bagranoff. (2003). Core Concepts of

Accounting Information Systems, 8 th Edition. John Wiley & Sons: New York, NY .

28) Romney, M. and P. J. Steinbart. (2003). Accounting Information Systems, 9 th Edition. Prentice Hall: Upper Saddle River, NJ .

29) vmyths.com. (2000). The Worldwide Michelangelo Virus Scare of 1992. Accessed on 3/30/2004 at http://vmyths.com/fas/fas_inc.inc1.cfm. Journal Of Business & Economics Research – September 2005 Volume 3, Number 9

30) Whitman, M. E. (2003). Enemy at the Gates: Threats to Information Security. Communications of the ACM.

31) Zekany, K. E., L. W. Braun, and Z. T. Warder. (2004). Behind Closed Doors at WorldCom: 2001. Issues in Accounting Education

یادداشت‌ها

۱- آدرس وب سایت انجمن حسابداران رسمی آمریکا : http://www;aicpa.org/antifraud/homepage.htm.

[2] -Romney and Steinbart
[3] -Computer Security Institute
[4] -Federal Bureau of Invetigation
[5] - Theft of Proprietary Information
[6] -Denial of Service Attacks
[7] - Unauthorized Access
[8] - Sabotage
[9] - Casabona and Yu
[10] - Fortran
[11] - Cobol
[12] - Pascal
[13] - C
[14] - Dbase
[15] -Clipper
[16] - Paradox
[17] - Xbase
[18] - Foxpro
[19] - Basic
[20] - Visual foxpro
[21] - Client-server
[22] - Visual basic
[23] - Delphi
[24] - Vb. Net
[25] - Visual C# .Net
[26] - Web base
[27] Asp. Net
[28] - Java
[29] - Microsoft . Net
[30] - SQL
[31] - Oracle
[32] - Forensic Accountants
[33] - Destructive Or Malicioous Programs
[34] - Hall
[35] - Annoyance
[36] - Logic Bomb
[37] - Michelangelo
[38] - Hackers
[39] - Encrypting Or Scrambling The Data
[40] - Sniffing
[41] - Piggybacking
[42] - Luehlfing et al.
[43] - Sabotage And Vandalism
[44] - Silverthorn
[45] - McGullivray
[46] - Theft Of Proprietary Information
[47] - Whitman
[48] - The Business Software Alliance
[49] - Copyright
[50] - Harris
[51] - Data Manipulation And Financial Fraud
[52] - Data Diddling
[53] - Transactions
[54] - Theft Of Computer Hardware
[55] - Borrow
[56] - Central Processing Units
[57] - Personal Digital Assistants
[58] - Flash Memory
[59] - Controlling Access Into A Computer System
[60] - Passwords
[61] - Biometrics
[62] - firewall
[63] - Value Added Network (VAN)
[64] - Controlling Data Input
[65] - Moscove et al.
[66] - Controlling Output From The Computer System
[67] - Wiretapping
[68] - Encryption
[69] - Encryption Key
[70] - Preventing And Detection Destructive Programs
[71] - Antivirus
[72] - Reputable Vendors
[73] - Detecting Intrusions Into Computer Systems
[74] - Trip Wires
[75] - Honey Put Lures
[76] - Anomaly Detection Systems
[77] - Snapshots
[78] - Calhoun
[79] - Enron,WorldCom,Adelphia,And Tyco
[80] - Accounting Information Systems
[81] - HealthSouth
[82] - Big Five