

چالش‌ها و راهکارهای استقرار نظارت الکترونیک در سازمان بازرسی کل کشور^۱

دکتر بهزاد پورنقدی^۲

چکیده

نظارت الکترونیکی با هدف کاهش هزینه‌های نظارت سنتی و مراجعات حضوری و افزایش بهره‌وری و استفاده از ارتباطات الکترونیکی به دنبال سازو کارهای مناسب و کارآمد است. با تغییر نظام و ساختار نهادهای اجرایی، روشن است که روش‌های سنتی نظارت و کنترل از بازدهی و بهره‌وری لازم برخوردار نخواهند بود؛ لذا «نظارت الکترونیک» یکی از مفاهیم جدید در حوزه نظارت و بازرسی است که به عنوان مفهومی کارآمد در خدمت و تکمیل روندها و تسهیل نظارت، امروزه یکی از مهم‌ترین روش‌های نهادهای نظارتی شده است. با توجه به گسترش استقرار دولت الکترونیک یکی از مشکلات اساسی نظارت و بازرسی در ایران، استفاده از ابزارها و روش‌های قدیمی و سنتی نظارتی در کشف جرایم است. اجرای نظارت الکترونیک می‌تواند ابزاری مناسب و نظام‌مند برای پیشگیری، کشف و شناسایی جرایم به موازات تحقق دولت الکترونیک باشد. ضروری است سازمان بازرسی کل کشور با بهره‌گیری از نظارت الکترونیک، به پیشگیری و کشف سریع و دقیق جرایم پردازد که این امر موجب ارتقاء توانمندی سازمان در راستای تحقق اهداف و مأموریت‌های محوله و همچنین صرفه‌جویی اقتصادی در هزینه‌ها خواهد شد.

کلیدواژه‌ها: نظارت الکترونیک، سازمان بازرسی کل کشور، دولت الکترونیک، مقابله با فساد

۱. این مقاله بخشی از کتاب تألیفی «الزامات و راهکارهای نظارت الکترونیک بر جرایم رایانه‌ای از سوی سازمان بازرسی» است که با تصویب و حمایت

اداره کل بازرسی استان سمنان (سازمان بازرسی کل کشور) تدوین و منتشر شده است.

۲. دکترای مهندسی فناوری اطلاعات، استادیار دانشگاه آزاد اسلامی. behzad_pournaghdhi@yahoo.com

مقدمه

مهم ترین تحول در عرصه علم و دانش توسعه و گسترش علوم رایانه، الکترونیک و فناوری اطلاعات و ارتباطات است که در سال های اخیر شاهد پیشرفت های چشمگیری در این زمینه بوده ایم. امروزه این علم در خدمت و کمک رسانی به سایر علوم بر آمده و در تمامی ابعاد زندگی مردم و تکالیف روزمره ایشان دخیل و حائز اهمیت است (سکر، ۱۳۹۰). فناوری اطلاعات و ارتباطات در ابعاد گسترده ای وارد حیطه های مختلف کاری جوامع بشری شده است و سازمان بازرسی کل کشور و سایر نهادهای نظارتی نیز از این قاعده مستثنا نیستند. فناوری اطلاعات در راستای خدمت رسانی و تسریع روند انجام کارها و افزایش سرعت بهره وری و تبادل اطلاعات و ارتباطات، دنیا را متحول ساخته است.

جست و جوی سریع در بین انبوهی از اطلاعات، سرعت بالای عملیات ارتباطی و پردازش داده ها، از میان برداشتن محدودیت های جغرافیایی، اشتراک علم و دانش و یافته های علمی در میان ملل، تبادل فرهنگی، سهولت انجام کارهای روزانه، سهولت نظارت و انجام فرآیند بازرسی و... شماری از خدمات و نوآوری های این فناوری است. به طور کلی سیستم دستگاه های قضایی، نظارتی و بازرسی با به کارگیری فناوری اطلاعات و نظارت الکترونیک باعث افزایش توان اجرایی خود در تحقق اهداف و آرمان ها، پیشگیری، کشف و مقابله با جرایم و تخلفات و همچنین ارتقاء توان نظارتی خود در انجام مأموریت های محوله خواهند شد. مقاله حاضر به بررسی الزامات و راهکارهای نظارت الکترونیک بر جرایم رایانه ای از سوی سازمان بازرسی کل کشور و یافتن روش های جدید نظارت و بازرسی پرداخته و اهداف و چشم اندازهای آن را با کاربرد فناوری اطلاعات تعمیم می دهد. امکانات و دستاوردهای فراوانی که ابزار جدید نظارت الکترونیک در اختیار بازرسان سازمان بازرسی قرار می دهند کشف تخلف، پیشگیری از جرم و برخورد قانونی و هدفمند با متخلف را آسان تر می سازد.

یک سیستم بازرسی و نظارتی بدون در اختیار داشتن اطلاعات کافی، صحیح و به موقع نمی تواند نقش مؤثری در راستای اهداف و مأموریت های خود ایفا کند؛ بنابراین طراحی یک شبکه گسترده اطلاعاتی مبتنی بر ابزار الکترونیک که قادر است برای مسئولان نظارت و بازرسی اطلاعات لازم را فراهم سازد و این اطلاعات را به موقع در اختیار آنان قرار دهد، در فرآیند انجام کنترل و نظارت ضروری است. از آنجایی که نظارت دایمی و مستمر بر عملکرد افراد، کارکنان، یا فعالیت ها و

نحوه‌ی عملکرد سازمان‌ها و ادارات به دلایلی همچون صرف وقت و هزینه‌های زیاد امکان‌پذیر نیست، ضرورت تشکیل یک سیستم نوین نظارت و بازرسی الکترونیک با استفاده از تجهیزات و بسترهای فناوری اطلاعات کاملاً روشن و آشکار است؛ زیرا این امر موجب به دست آوردن نتایج بهتر و نظارت و کنترل گسترده‌تر و دقیق‌تر با صرف هزینه و وقت کمتر می‌شود. یکی از عوامل مؤثر در بهبود عملکرد نظارت سازمان و کاهش هزینه‌ها و صرفه‌جویی در منابع مالی و امکانات، بودجه، منابع انسانی و زمان سیستم نظارت الکترونیک است.

سیستم نظارت الکترونیک یک فرآیند نظارتی نوین است که با استفاده از تجهیزات و امکانات فناوری اطلاعات و ارتباطات و به منظور دستیابی به نتایج بهتر به کنترل و نظارت سازمانی می‌پردازد و این امر موجب حصول فرآیند بازرسی مؤثر، دقیق و کشف سریع فساد و تخلفات اداری می‌شود. یکی از مسائلی که در سیستم‌های نظارتی نقش مهم و اساسی دارد وجود اطلاعات گسترده و مناسب است؛ زیرا اطلاعات پراکنده، غیر مرتبط و ناقص برای فرآیند نظارت، کنترل و بازرسی یک تهدید و چالش جدی است. گاهی سیستم‌های نظارتی به دلیل حجم انبوهی از اطلاعات متفرقه و طبقه‌بندی نشده و یا عدم درجه‌بندی اطلاعات و اخبار بر حسب نیاز، نمی‌توانند به شناسایی و کشف موارد تخلف و فساد بپردازند که این مشکل با استفاده از سیستم‌های نوین نظارت الکترونیک و پردازش سیستمی و رایانه‌ای اطلاعات قابل حل است. حجم و درجه‌بندی اطلاعات دریافتی، جریان و یا عملکرد عادی یک سازمان با مقایسه شاخص‌ها و استانداردهای موجود باید به گونه‌ای باشد که قابل فهم بوده و از طرفی امکان تصمیم‌گیری و اقدامات اصلاحی را برای تشکیلات نظارتی ممکن سازد.

بنابراین، وجود چنین سیستمی تنها با به کارگیری یک مدل کارآمد نظارت الکترونیک امکان‌پذیر است که برای تحقق چنین سیستم نظارتی نیازمند به کارگیری و استفاده از سیستم‌های نظارت رایانه‌ای و الکترونیک هستیم. تعدد سازمان‌های نظارتی و عدم هماهنگی و ارتباط سیستمی و قانونمند میان سازمان‌های نظارتی موجب انجام فعالیت‌های موازی، تکراری و پرهزینه می‌شود. این ناهماهنگی‌ها و عدم ارتباط سبب شده تا حاصل اقدامات و نتیجه فعالیت دستگاه‌های نظارتی برای یکدیگر قابل بهره‌برداری و استفاده نباشد. هر چند ارتباطات مقطعی و غیرمتمرکزی میان آن‌ها وجود دارد اما این ارتباطات کافی نبوده و اهداف مورد نظر در زمینه‌ی نظارت و بازرسی را تأمین نمی‌کنند و باید در یک سیستم ارتباطی صحیح نتایج اقدامات نظارتی هر یک از سازمان‌های

نظارتی بر اساس یک راهبرد مشخص مورد بهره‌برداری قرار گیرد (عبداللهی، ۱۳۸۳).

بیان مسأله

«نظارت الکترونیك» یکی از مفاهیم جدید مدیریتی است که به‌عنوان مفهومی کارآمد در خدمت و تکمیل دولت الکترونیکی بسیار مورد استقبال واقع شده است. برنامه‌ریزی منابع سازمان، سیستمی است که می‌تواند با نظم دادن یکپارچه به تمامی اطلاعات تولیدشده و ثبت، دسته‌بندی و طبقه‌بندی، پردازش و ارایه گزارش‌های مدیریتی، تمامی این اطلاعات را در اختیار مدیران قرار دهد تا در نظام برنامه‌ریزی و نظارت مورد استفاده قرار گیرد (حسینی و فولادی طرقي، ۱۳۸۹، ص ۶۷۷). سرعت تحولات و توسعه دانش بشری فرصت تفکر و تدبیر را در زدودن تردید و وسواس می‌ریاید. عقب‌ماندگی از خیل عظیم جهان مجازی و فوق پیشرفته، خسروانی است که جبران آن بسیار دشوار است؛ لذا برای جبران یک‌جانبه‌نگری بودجه‌ریزان کشور، تدابیری اندیشیده شده که هر یک درخور توجه ویژه است.

برای آن که با خاستگاه‌ها و مظاهر فساد به‌صورت ریشه‌ای و هدفمند برخورد شود، درصد بازرسی‌های مستمر و از پیش برنامه‌ریزی شده افزایش یافت. برای کاهش تنش‌ها و ابهامات، به‌جای گزارش‌های محیطی بیشتر به گزارش‌های موضوعی روی آورده شد. با مجازی شدن مدیریت، سازمان و دولت رفته‌رفته به مجازی شدن جهان نزدیک می‌شویم. چنانچه اعمال مدیریت امروزی تنها منوط به حضور مدیر در محل مدیریت و سازمان مطبوع خود نیست و بخش اعظم آن با کنترل از راه دور (همانند روش‌های پیشگیری و درمان در امور پزشکی) انجام می‌شود. اعمال نظارت و بازرسی نیز می‌تواند با بهره‌گیری از دانش فنی روز، شدنی باشد. بدیهی است برای تحقق نظارت الکترونیکی ایجاد بسترهای فناوری اطلاعات و ارتباطات ضروری است و مستلزم این است که سازمان‌ها نیز به سمت الکترونیکی شدن گام بردارند (احمدی گر جی، ۱۳۸۶).

با توجه به گستردگی حجم اطلاعات و تولید دانش و گزارش‌ها سازمان نیازمند بهره‌مندی از سیستم‌های اطلاعات یکپارچه است؛ بنابراین توجه به نظام‌های یکپارچه اطلاعاتی در سازمان‌ها در همین راستاست و سیستم برنامه‌ریزی منابع سازمان^۱ یکی از طرح‌های اطلاعاتی و عملیاتی است که می‌تواند به‌صورت یکپارچه به تمامی اطلاعاتی که در حین عملیات تولید می‌شود نظم دهد و با ثبت، دسته‌بندی و طبقه‌بندی، پردازش و ارایه گزارش‌های مدیریتی تمامی این اطلاعات را در اختیار مدیران قرار دهد تا در نظام برنامه‌ریزی و نظارت و کنترل مورد استفاده قرار گیرد. سازمان‌های مدرن و مدیران آن‌ها برای نقش و جایگاه اطلاعات اهمیت ویژه‌ای قائل هستند. اطلاعات به‌عنوان

مواد خام سازمان، اطلاعات به‌عنوان دارایی، اطلاعات منبع ارزش افزوده، اطلاعات منبع راهبردی و اطلاعات یک منبع مهم تاکتیکی از جمله مواردی هستند که نظریه پردازان فناوری اطلاعات و ارتباطات جهت تبیین جایگاه و اهمیت اطلاعات در سازمان به آن‌ها اشاره دارند. برنامه‌ریزی منابع سازمان، فرهنگ سازمانی جدیدی است که با یکپارچه‌سازی سیستم‌ها و منابع اطلاعاتی سازمان با استفاده از شبکه‌های کامپیوتری، نظام تصمیم‌گیری و روند برنامه‌ریزی و حتی رفتار سازمان را تغییر می‌دهد. به نظر برخی اندیشمندان مدیریت و فناوری اطلاعات، برنامه‌ریزی منابع سازمان یک سیستم اطلاعاتی جامع برای یکپارچه‌سازی رفتارهای اطلاعاتی سازمان است (صرفی‌زاده، ۱۳۸۶).

بازرسان سایبری و الکترونیکی

بازرسان آینده مجبور خواهند بود فرآیند بازرسی و نظارت بر حسن اجرای قانون را با روش‌ها و تکنیک‌های بازرسی الکترونیکی اجرا کنند. امروزه بازرسان می‌توانند پرونده‌های مهمی را در زمینه‌ی کشف انواع فساد اداری و یا تخلفات سازمانی و جرایم رایانه‌ای بدون ترک دفتر کاری خود به سرانجام برسانند. همچنین در آینده‌ی نزدیک بازرسان و کارشناسانی که در مقابل انقلاب رایانه‌ای مقاومت می‌کنند، هرگز اقدامی را با حصول موفقیت به انجام نخواهند رساند.

جرایم سایبری طیف وسیعی از بزه‌کاری‌ها را شامل می‌شود و از انواع مزاحمت تا جرایم فاجعه‌آمیز را دربر می‌گیرد که در یک محیط مجازی به وجود می‌آیند. جرایم سایبری و مجازی قدمت کوتاهی دارند و تنها طی بیست سال اخیر این اصطلاح رواج یافته است و با ساده‌تر شدن کاربرد و استفاده از رایانه برای همگان و کاهش قیمت دسترسی به ابزار فناوری اطلاعات، معضلی نوین به نام جرایم سایبری در فضای مجازی پدید آمده است و نهادهای امنیتی، انتظامی و نظارتی را با چالش جدیدی مواجه ساخته است. جرایم سایبری که به جرایم نسل سوم رایانه و اینترنت وابسته است در محیط مجازی یا فضای سایبری قابل تحقق است. از این جهت رفتار مجرمان رایانه‌ای کاملاً متفاوت با مجرمان سنتی است. در این نوع از بزه، مرتکبان ناشناس در فضایی ناشناخته دست به اعمال مجرمانه می‌زنند. برخلاف جرم کلاسیک، جرم رایانه‌ای دارای فناوری برتر و وسایل پیشرفته‌تری است. مرتکبین این جرایم با استفاده از فناوری نوین و ابزارهای جدید به اهداف شوم خود دست پیدا می‌کنند، بدون آن‌که اثری همانند جرم کلاسیک از خود بر جای بگذارند. ویژگی دیگر این جرایم نامشخص بودن هویت مجرمان و همچنین عدم تشخیص درست طیف بزه‌دیدگان است؛ زیرا افراد و سازمان‌های متعددی می‌توانند هدف این مجرمان قرار بگیرند. این موضوع

نشان می‌دهد که مجرمان رایانه‌ای و مجازی فارغ از زمان و مکان بوده‌اند و این نوع از جرایم و تخلفات هم‌اکنون جنبه فراملی و فراسرزمینی به خود گرفته است. فناوری‌های نوین در این عرصه و پیشرفت تجهیزات ارتباطی، مخابراتی و الکترونیکی، سهولت وقوع جرایم رایانه‌ای در فضای مجازی متخلفان و مجرمان را قادر ساخته که فعالیت‌های خود را بدون داشتن ارتباطی خاص با یک محل معین و مشخص انجام دهند. پرواضح است که با وقوع این نوع از جرایم، خطری جدی برای جامعه بین‌المللی و جامعه داخلی یک کشور و سیستم اداری و تشکیلات سازمانی آن رقم می‌خورد. در شیوه جدید و جرایم نوین رایانه‌ای بیشترین مورد وقوع جرم در جرایم تجارت الکترونیکی و جرایم بانکداری الکترونیکی است (عالی پور، ۱۳۹۰، ص ۸۹).

در خصوص کشف جرایم و تخلفات رایانه‌ای و حفظ ادله الکترونیک، مراحل و روش‌های زیر برای آگاهی بازرسان سازمان بازرسی ارایه می‌شود. بدیهی است رعایت نکات فنی و تخصصی در این خصوص می‌تواند در اقدامات نظارتی و بازرسی درزمینه‌ی کشف فساد و جرایم مؤثر باشد:

۱. ضروری است مجموعه سازمان بازرسی کل کشور از اخبار مردمی و همکاری خبرگان و متخصصان علوم رایانه‌ای و فناوری اطلاعات و ارتباطات بهره‌مند شود.
۲. بازرسان، مسئولان فناوری اطلاعات و انفورماتیک ادارات و تشکیلات مورد بازرسی را جهت همکاری و مشاوره دعوت کنند.
۳. کارشناس جرایم رایانه‌ای و بازرسان الکترونیک می‌بایست از کلیه شواهد، اسناد، ادله الکترونیک و مدارک موجود به صورت کامل یک نسخه پشتیبان و یا به تعداد کافی کپی تهیه کنند.
۴. کارشناس جرایم رایانه‌ای کلیه شواهد، مدارک و مستندات را به آزمایشگاه تخصصی کشف جرم در سازمان بازرسی منتقل کند.
۵. بازرسان در صورت نیاز مدیران، مسئولان، کارشناسان و یا کارکنان ذی‌ربط را برای پاسخگویی فرابخوانند.
۶. ضروری است کارشناسان جرایم رایانه‌ای و بازرسان الکترونیک کلیه فایل‌ها را برای یافتن شواهد و مدارک مربوط به ارتکاب جرم آزمایش کنند و از صحت و اصالت اسناد، شواهد و مدارک به دست آمده مطمئن شوند.
۷. بازرسان پس از بررسی مدارک و انجام بازرسی‌های لازم گزارش مربوط به کارشناس جرایم رایانه‌ای را به صورت کامل مطالعه کرده و دفاعیات و شواهد را به صورت قابل قبول برای ارایه در

گزارش پیوست کنند.

استفاده از افرادی بی‌تجربه و غیرمتخصص در فرایند بازرسی و کشف آثار جرایم رایانه‌ای باعث نامعتبر شدن اثر جرم و شواهد و مدارک موجود خواهد شد؛ لذا لازم است همواره در این عرصه از افراد متخصص استفاده شود.

نظام بازرسی و ادله الکترونیکی

یکی از مباحث مهم و حساس در نظام‌های حقوقی ادله و نحوه استناد و پذیرش آن جهت اثبات یا رد دعوی خصوصی و جزایی است؛ به نحوی که می‌توان گفت بدون دلیل هیچ دعوی سرانجام ندارد. پس اسناد و مدارک ناشی از کارکردهای فناوری اطلاعات را نیز باید در همان فضا و به صورت الکترونیکی جست‌وجو کرد. اطلاعات و داده‌های مهمی در مورد افراد و مشاغل، سازمان‌ها و ادارات دولتی و خصوصی به صورت الکترونیکی ایجاد، ذخیره، پردازش و مبادله می‌شوند که می‌توانند نقش مؤثری در فرآیند دادخواهی یا تعقیب جزایی داشته باشند. اصولاً نسخه‌های الکترونیکی می‌توانند اطلاعات ارزشمندی را ارائه دهند که در نسخه‌های کاغذی و سنتی وجود ندارد. از آنجا که سازمان‌ها و اشخاص به طور گسترده‌ای به سیستم‌های رایانه‌ای خود وابسته شده‌اند توجه قانون‌گذار، نهادهای قضایی، نظارت و بازرسی و مجریان قانون به ذخایر ارزشمند اطلاعاتی که در این سیستم‌ها نگهداری می‌شوند معطوف شده است. این اشخاص به طور جدی جهت کشف و ارائه داده‌های الکترونیکی در تمامی دعاوی خود اهتمام می‌ورزند.

امروزه فناوری اطلاعات و علوم رایانه در زمینه‌ی نحوه مدیریت اطلاعات و روش‌های اداره مشاغل، انقلاب بزرگی به وجود آورده است. اطلاعات راجع به مشاغل مهم به سرعت در حال ایجاد، ذخیره‌سازی و برقراری ارتباط به روش الکترونیکی است. امروزه دیگر اطلاعات مختلفی که در دعاوی حقوقی یا پیگردهای جزایی نقش مهمی ایفا می‌کنند در پرونده‌های کاغذی ثبت و بایگانی نمی‌شوند بلکه در یک سیستم رایانه‌ای و یا به شکل قابل خواندن با رایانه، ذخیره و بایگانی می‌شوند. به همان نسبت که افراد، سازمان‌ها و شرکت‌ها اتکای خود را بر سیستم‌های رایانه‌ای افزایش داده‌اند بازرسان و نهادهای نظارتی نیز به ارزش ذخایر گرانبهای الکترونیکی پی‌برده‌اند؛ ذخایر محفوظ در سیستم‌های رایانه‌ای که به طور گسترده‌ای استناد به آن‌ها برای کشف و به جریان انداختن انواع دعاوی آغاز شده است. هر گونه داده یا نرم‌افزار یا سخت‌افزار الکترونیکی که بتواند اطلاعات ارزشمندی در راستای اثبات ادعا، دفاع، کشف جرم و یا استدلال قضایی به دست دهد، دلیل الکترونیکی محسوب می‌شود. این اطلاعات که ممکن است در اسناد کاغذی

موجود نباشد می تواند نقش مؤثری در فرآیند تعقیب کیفری، حقوقی یا دادرسی ایفا کند و با توجه به توسعه فناوری الکترونیک به ویژه فناوری اطلاعات و ارتباطات، یکی از ابزارهای مهم فن حقوق محسوب خواهد شد (حسینی و فولادی طرقي، ۱۳۸۹).

ادله الکترونیکی با توجه به گسترش استفاده از فناوری رایانه در زمینه مدیریت اطلاعات و افزایش بهره گیری از سیستم رایانه ای به جای پرونده های کاغذی و سیستم بایگانی سنتی، ذخایر ارزشمندی از اطلاعات را در سیستم های رایانه ای ایجاد می کنند که کشف و استناد به آن حائز اهمیتی خاص است. چنان که قریب به چند دهه است در دادگاه های کشورهای توسعه یافته به کار می آیند. مسأله و موضوع کشف ادله الکترونیکی را کشف رسانه الکترونیکی نیز می نامند. در پرونده های مختلفی از دعوی اخیر کشورهای توسعه یافته از جمله موارد آزار جنسی، نشر غیر مجاز، کلاهبرداری، اثبات ارتباط قربانی و متهم در موضوع قتل عمدی، اثبات سرقت اسرار تجاری و کاری و کشف دلیل و مدرک دال بر سایر اعمال مجرمانه و غیره از ادله الکترونیکی بهره برده اند (Jones, 2011).

جمع آوری ادله الکترونیک در نظارت و بازرسی الکترونیک

حفظ و نگهداری ادله الکترونیک در فرآیند نظارت و بازرسی یکی از مهم ترین اقدامات بازرسان الکترونیکی است؛ بنابراین توجه به موارد زیر در این راستا می تواند نسبت به حفظ و نگهداری ادله الکترونیک و استفاده از آنها مورد استفاده قرار گیرد.

الف) با توجه به این موضوع که در بازرسی ها یا تفتیش ها داده های الکترونیکی منبع ادله گرانبهایی به حساب می آیند، برخی نمونه های خاص که در این زمینه باید در نظر داشت عبارت اند از:

۱. داده های ذخیره شده در رسانه های مغناطیسی یا نوری قابل حمل؛
۲. پست الکترونیکی؛
۳. رویه های حسابرسی؛
۴. تصاویر دیجیتالی و ویدیویی؛
۵. داده های صوتی دیجیتالی؛
۶. پست صوتی و ...

ب) اطلاع رسانی و آگاه ساختن افراد یا سازمان بازرسی شونده از این موضوع که ممکن است با کاربری معمول از سیستم رایانه ای یا دیگر تجهیزات الکترونیکی بدون اجرای اقدامات فوری یا

محافظت از آن‌ها، ادله الکترونیک خاصی تخریب شود.

ج) حتی‌المقدور بازرسان انواع اطلاعاتی که باید محافظت شوند را تعیین کنند و مکان‌هایی که احتمال می‌رود این دلایل وجود داشته باشد، مشخص شوند.

در راستای توسعه و گسترش نظام کنترل، نظارت و بازرسی الکترونیکی و کشف ادله و داده‌های الکترونیکی اجرای مراحل و اقدامات زیر ضروری است:

۱. تهیه پرسش‌نامه‌ای رسمی در چارچوب قوانین حاکی از بازجویی جهت کسب اطلاعات غنی و لازم در رابطه با روش‌ها و سیستم‌های رایانه‌ای سازمان و دستگاه بازرسی شونده (این فرآیند باید در صورت اجازه قوانین حوزه قضایی ذی‌ربط انجام گیرد)؛

۲. پیگیری فرآیند نظارت و بازرسی از طریق کشف شفاهی (گزارش مردمی و یا شهادت کارکنان)، بازرسی و بازجویی کارکنان سازمان و یا بازرسی سیستم‌های اطلاعاتی و رایانه‌ای سازمان در صورت عدم محدودیت قانونی و اجازه قوانین ذی‌ربط؛

۳. کسب اطمینان از این که در مراحل بازرسی سازمان، تمامی درخواست‌های تولید و ارایه ادله موردنظر علاوه بر اسناد کاغذی بر اسناد الکترونیک نیز تصریح شده است؛

۴. جست و جوی نسخه‌های الکترونیکی داده‌هایی که از طرف کارشناسان گواهی دهنده در سازمان مطبوع تقاضا و احراز شده است؛

۵. توجه بازرسان به این موضوع که آیا ارزیابی یا تفتیش سیستم کامپیوتری موردنظر لازم خواهد شد و یا امکان دارد که به ادله الکترونیک ارایه شده توسط کارکنان و یا سیستم اداری سازمان بازرسی شونده اعتماد کرد؟

برای این که کارشناسان و بازرسان، تفتیش و بازرسی جامعی از ادله الکترونیکی به عمل آورند، لازم است بدانند که به دنبال چه چیزی هستند و باید آن‌ها را کجا بیابند. بازرسان باید معین کنند که کدام سیستم‌های رایانه‌ای و کدام برنامه‌های نرم‌افزاری موجود و یا سیستم‌های ذخیره‌سازی الکترونیکی، شامل محتوای داده‌های الکترونیکی موردنیاز هستند. همچنین لازم است تمامیت داده‌های الکترونیکی کشف شده نیز به اثبات برسد که در ادامه این بخش به برخی روش‌های جمع‌آوری ادله الکترونیک اشاره شده است. برای جمع‌آوری ادله الکترونیک در فرآیند بازرسی می‌باید بازرسان افراد کلیدی و جریان کاری بین آن‌ها را کشف و شناسایی کنند. همچنین فهرستی از همه فایل‌ها و یا اسناد تولید یا اصلاح شده توسط افراد ذی‌ربط در یک دوره معین درخواست شود (قدمی، ۱۳۸۳) سپس هویت افرادی که به اسناد مربوط دسترسی دارند مشخص شود. همچنین

هویت اشخاص ثالثی که نسخه‌های این اسناد را در اختیار دارند تعیین شود. در ادامه فرآیند بازرسی لازم است بازرسان موارد احتمالی و چگونگی تخریب اطلاعات و اسناد نگهداری شده و ادله الکترونیکی را شناسایی کرده و در خصوص جلوگیری از چنین مشکلی تدابیر لازم را بیندیشند. تولید و توزیع چندین نسخه از ادله الکترونیک کار آسانی است و معمولاً از داده‌ها و اطلاعات سازمان‌ها به‌طور منظم و دوره‌ای نسخه‌های پشتیبان^۱ گرفته و ذخیره می‌شود؛ بنابراین در بسیاری از موارد این نسخه‌ها در مکان‌های متعددی وجود دارند. به‌طوری‌که حتی اگر سازمان بازرسی شونده یا کارکنان پاسخگو معتقد باشند همه نسخه‌ها قبلاً پاک شده‌اند، می‌توان یک نسخه کپی یا نسخه‌های دیگری از آن ادله موردنیاز را کشف کرد. بازرسان و متخصصان نظارت الکترونیک برای این که بتوانند استراتژی کشف داده‌های الکترونیکی را اجرا کرده و تدوین و توسعه دهند، لازم است همه مکان‌هایی که احتمال می‌رود نسخه‌ای از اطلاعات مربوط در آنجا باشد را در نظر داشته باشند. برخی از این مکان‌ها عبارت‌اند از: کامپیوترهای شخصی اداره یا سازمان، دیسک‌ها، حافظه‌های فلش قابل حمل و دیسک‌های USB، سرور^۲ فایل‌های شبکه یا سیستم‌های رایانه‌ای بزرگ، کامپیوترهای شخصی موجود در منزل کارکنان، کامپیوترهای مشترک اداری قابل حمل^۳، منابع کامپیوتری تحت کنترل خارج از مجموعه، سرویس‌های پست الکترونیکی^۴ و سایر موارد.

چالش‌ها و موانع گردآوری و تحلیل ادله الکترونیک

درخواست‌های ارایه‌شده بازرسان در خصوص اسناد باید مشخص و عاری از هرگونه ابهام باشد و لازم است که در آن‌ها به همه منابع احتمالی ادله الکترونیک مرتبط اشاره شود. این منابع شامل مکان‌های مختلف ذخیره‌ساز، کامپیوتر و منابع نسخه‌های پشتیبان، فایل‌های حذف‌شده اما قابل بازیابی، بخش‌های آخر نوارها و غیره است. درخواست‌کننده باید این آمادگی را داشته باشد که در صورت لزوم هم سازمان بازرسی شونده و هم سازمان مطبوع خود را در خصوص موضوعات فنی مربوط به ذخیره‌سازی و بازیابی ادله الکترونیک توجیه کند.

۱. محرمانگی داده‌های سازمانی

اگر لازم باشد که بازرس و کشف‌کننده اقدام به کنترل و بازرسی منبع الکترونیکی کند سازمان بازرسی و محاکم قضایی می‌توانند از سازمان یا نهاد مورد بازرسی در برابر محرمانه بودن

1. Backup
2. Server
3. Laptop
4. E-Mail

مطالب غیر قابل کشف و هزینه‌های مربوط به آن حمایت کنند. دستور حمایتی محاکم قضایی و یا مقام بازرسی فقط می‌تواند به بازرسان، کارشناسان و یا نمایندگان منتخب طرفین، اجازه بازرسی و افشای اطلاعات را بدهد (جلالی فراهانی، ۱۳۸۹).

۲. حجم اطلاعات و اسناد الکترونیکی

یکی دیگر از مشکلات و معضلات فراروی بازرسان الکترونیک، حجم گسترده و انبوهی از اطلاعات الکترونیک است؛ به طوری که حجم اطلاعاتی که به شکل الکترونیکی ذخیره می‌شوند بسیار زیاد است. از آنجایی که قیمت فضای ذخیره‌ساز دیسک سخت کامپیوتر به سرعت در حال کاهش است، هزینه نگهداری اطلاعات قدیمی نسبت به صرف وقت یک کارمند جهت حذف اطلاعاتی که دیگر مورد نیاز نیستند، پایین تر بوده و هرروزه این هزینه به طور فزاینده‌ای رو به کاهش است. جدا از آسیبی که به طور بالقوه بر اطلاعات ذخیره‌شده الکترونیکی وارد می‌آید، هنگام رسیدگی قضایی به چنین مقادیر بزرگی از دلایل و مدارک انباشت شده، حجم زیاد آن‌ها نیز موجب بروز خسارت مضاعف بر آن‌ها می‌شود.

۳. عدم سازماندهی و دسته‌بندی داده‌های الکترونیکی

عموماً اطلاعات رایانه‌ای و الکترونیکی نسبت به اطلاعات و مدارک کاغذی و سنتی کمتر سازماندهی و دسته‌بندی می‌شوند. معمولاً اسناد کاغذی به صورت پرونده‌های شماره‌بندی شده بایگانی می‌شوند و هر یک دارای کارت شناسایی مخصوص هستند و نسخه مالی اضافی نیز در پرونده‌هایی جداگانه و مرتبط نگهداری می‌شود؛ ولی در بسیاری موارد اطلاعاتی که در سیستم‌های رایانه‌ای سازمان‌ها و ادارت ذخیره می‌شود، به خوبی سازماندهی و دسته‌بندی نمی‌شود. معمولاً نسخه‌های الکترونیکی پشتیبان اطلاعات به طور کامل فهرست‌بندی نمی‌شوند. شاید بتوان نسخه‌های پشتیبان را بر اساس تاریخ تولیدشان تعیین و دسته‌بندی کرد، اما تشخیص این که کدام حامل داده‌ای حاوی چه فایل پشتیبانی است، امری غیر ممکن است. بازرسان و یا کارشناسانی که اسناد و مدارک تولیدشده در جریان کشف را دریافت می‌کنند، باید آن‌ها را سازماندهی و ثبت و ذخیره کنند (جاوید نیا، ۱۳۸۸). سازماندهی یا طبقه‌بندی اسناد و مدارک با توجه به میزان مفید و مرتبط بودن آن‌ها با مورد یا موارد مطروحه است. همچنین بازرسان می‌توانند در بررسی و بازمینی حجم عظیمی از ادله الکترونیک از کمک سیستم‌های رایانه‌ای نیز بهره‌مند شوند و موارد مورد نیاز را با توجه به کلمات کلیدی ضروری مورد جستجو و بازمینی قرار دهند.

۴. رمز گذاری و فشرده سازی ادله الکترونیکی

یکی دیگر از مشکلات احتمالی بازرسان در خصوص جمع آوری ادله الکترونیکی مواجه شدن با قالب اختصاصی فشرده سازی و رمز گذاری اطلاعات و مستندات است. بسیاری از برنامه های کاربردی داده ها را در قالب یک فایل اختصاصی ذخیره می کنند تا علاوه بر صرفه جویی در فضای ذخیره سازی اطلاعات، دسترسی سریع تر به داده ها را نیز فراهم کنند؛ بنابراین رمزگشایی و خارج کردن ادله از حالت فشرده سازی یکی از دشواری های فرآیند بازرسی الکترونیک خواهد بود.

۵. بررسی صحت و اصالت اسناد الکترونیکی

ادله الکترونیک نسبت به اسناد و مدارک کاغذی سنتی بیشتر در معرض نابودی، تغییر، دستکاری و یا دسترسی غیرمجاز قرار دارند. تاریخ و زمان مربوط به ادله الکترونیکی که توسط سیستم های عامل رایانه ای ایجاد و نگهداری می شود، به آسانی قابل تغییر است. این موضوع یکی دیگر از چالش های سیستم نظارت و بازرسی الکترونیک خواهد بود؛ زیرا با تغییر زمان ایجاد و ثبت داده های الکترونیکی استنادپذیری ادله های الکترونیکی نیز از بین می رود و یا با مشکل روبه رو خواهد شد (پرنیان، ۱۳۸۳).

۶. عدم تولید و بایگانی اسناد الکترونیک در دستگاه ها

در پرتو کشف تخلفات، جرایم و نظارت بر اطلاعات الکترونیکی یک سازمان باید کلیه کارکنان خود را به تهیه پیش نویس کلیه مدارک و مستندات به ویژه پیام های الکترونیکی تشویق و توصیه کند؛ زیرا ممکن است در آینده و در جریان تحقیقات و بازرسی یکی از نهادهای نظارتی، هنگام رسیدگی بازرسان به اطلاعاتی در این خصوص نیاز باشد که ضمن ارایه آن به فرآیند نظارت الکترونیکی و همچنین سازو کار و ساختار خود کنترل سازمانی کمک کنند. به ادارات، نهادها، ارگان ها و سازمان ها توصیه می شود ضمن حفاظت از اسناد و داده های الکترونیکی خود از نبود شرایط و عوامل خطر ساز غیر ضروری در سیستم بایگانی الکترونیکی خود اطمینان حاصل کنند. مدارک و اسناد داخلی سازمان ها باید به درستی ثبت و ذخیره شوند و فعالیت های انجام شده توسط سازمان را برای کنترل و نظارت به نهادهای نظارتی ارایه دهند. باید همواره دقت کافی به عمل آید تا از به کارگیری افراد فاقد مهارت یا افرادی که آموزش لازم و تخصص مناسب را در رابطه با سیستم بایگانی و ثبت اسناد الکترونیکی ندارند، خودداری شود. یکی از راهبردهای کاربردی که می تواند از هزینه های بررسی شمار زیادی از اسناد الکترونیکی در مورد درخواست

تهیه یک سند در جریان نظارت و بازرسی بکاهد، استفاده از برنامه‌های پیشرفته بایگانی اسناد است (احمدی گرجی، ۱۳۸۶).

در برنامه بایگانی اسناد اصل بر این است که فقط اسناد مفید (اسناد و مدارک راجع به فعالیت‌های شغلی و موضوعات قانونی که شرکت با آنها مواجه می‌شود) برای مدت زمان محدودی که بایگانی آنها لازم است، حفظ و نگهداری شوند. یک برنامه بایگانی که خوب طراحی شده باشد می‌تواند به عنوان یک ابزار قانونی بازدارنده از فساد اداری و تخلفات سازمانی به کار رود. همچنین این سیستم می‌تواند موجب حذف هزینه سنگین نگهداری مدارک غیر ضروری و منسوخ شود و از هزینه‌های مالی و هزینه بررسی دوباره اسناد در پاسخ به درخواست‌های کاری، بازرسی‌های دولتی و قضایی و نهادهای نظارتی بکاهد.

راهکارهای رفع موانع نظارت و ارزیابی الکترونیک

به منظور غلبه بر موانع نظارت و ارزیابی در سازمان‌ها راهکارهایی پیش‌بینی شده است که برخی از این راهکارها در زیر بیان می‌شوند:

۱. خودنظارتی را در افراد و سازمان‌ها توسعه دهیم: در سازمان‌های اجتماعی بهترین نوع نظارت آن است که فرد نظارت را از خودش شروع کند و خودنظارتی معمول شود. منظور از خودنظارتی این است که فرد تقریباً آزاد است و آزادی فرد تا جایی است که به آزادی حقوق و اموال دیگر افراد لطمه نزند. نظارتی که درباره خود اجرا می‌کنیم ساخته خودمان است.

۲. شناخت روشنی از مسئولیت‌ها به افراد و سازمان‌ها بدهیم: چنانچه کارکنان و مدیران سازمان شناخت روشنی از مسئولیت‌های خود برای انجام تعهدات داشته باشند، می‌توان انتظار داشت تا خودنظارتی به بهترین نحو بر رفتار آنان در سازمان اثر گذاشته و از بروز ناهنجاری و فساد جلوگیری کند.

۳. در تدوین استانداردهای نظارتی، افراد و سازمان‌های مورد نظارت را دخالت دهیم. در صورتی که هنگام وضع استانداردهای نظارتی نظر افراد، گروه‌ها و یا سازمان‌های مورد نظارت را نیز جویا شویم به میزان زیادی مقاومت‌هایی را که در مورد فرآیند نظارت به وجود خواهد آمد از بین می‌بریم. همچنین می‌باید به افراد، کارکنان و سازمان‌هایی که مورد نظارت قرار می‌گیرند به طور مستمر بازخورد داده شود. افراد و سازمان‌های تحت نظارت حق دارند تا به طور مستمر در مورد عملکرد خود بازخورد بگیرند و سازمان‌های نظارتی نیز در حقیقت موظف به ارایه چنین بازخوردی هستند پس باید به طور مستمر به نظارت شوندگان بازخورد داده شود تا موجب بهبود و

اثربخشی نظارت شود (صادقپور، ۱۳۷۸، ص ۱۹).

۴. لازم است تشکیلات نظارتی از امکانات، فناوری و دانش روز برای کنترل، نظارت و بازرسی بهره‌مند شوند. همچنین ضروری است سازمان بازرسی کل کشور در فرآیند اجرای امور پیشرفت و بهبود داشته باشد و به ایجاد و استفاده از سیستم نظارت الکترونیک اقدام کند.

۵. به وضع قوانین و تعیین ضوابط صریح و روشن همراه با ضمانت اجرایی قوی پردازیم. به منظور حل مسایل و مشکلات مبتلا به سازمان‌ها از نظر فساد و تبعیض و موارد دیگر می‌بایست قوانین و ضوابط صریح و روشنی تصویب شوند که مسیر را برای نظارت شفاف هموار کنند و از طریق وضع قوانین و تعیین ضوابط و ضمانت اجرایی مناسب سیستم نظارت کمی و کیفی و همچنین نظارت مالی و فنی و اجرایی در سازمان‌ها فراهم شود.

۶. به تربیت نیروی انسانی متخصص و متعهد برای نظارت و ارزیابی پردازیم. سازمان‌های نظارتی در کشور بایستی به تربیت نیروی انسانی ورزیده، مؤمن و کارشناس پردازند تا بتوانند با دقت کامل به اعمال نظارت بر سازمان‌های کشور پرداخته و موجب اثربخشی سیستم کنترل و نظارت در کشور شوند (اصلاتی، ۱۳۷۸، ص ۶۵).

۷. به بازبینی در ساختار نظارتی کشور و ایجاد هماهنگی بین سازمان‌های نظارتی پرداخته شود. همان‌طور که در بخش موانع ساختاری مطرح شد در حال حاضر سازمان‌های نظارتی فراوانی در کشور ما به امر نظارت و بازرسی مشغول‌اند؛ اما در میان این سازمان‌ها هماهنگی لازم وجود ندارد؛ لذا باید به منظور ایجاد هماهنگی بین این نهاد‌های نظارتی نوعی تشکیلات هماهنگ‌کننده ایجاد و شرح وظایف هر یک از بخش‌های نظارتی کشور را دقیقاً مشخص شود تا از موازی کاری و همچنین عدم نظارت در برخی از موارد جلوگیری به عمل آید.

۸. توجه به نظارت پیش‌نگر: موضوع بااهمیت در امر بازرسی و نظارت این است که پیشگیری همیشه بهتر از درمان است. در صورتی که ما در امر انتصاب و انتخاب مدیران سازمان‌ها دقت لازم را کرده و افراد امین و کارآمد را در پست‌های مدیریتی منصوب کنیم تا حد زیادی از نیاز به نظارت‌های بعدی و همچنین نیاز به تلاش برای کشف فساد و جرم در مراحل بعدی نظارت کاسته خواهد شد. بدین منظور مکانیسم‌های انتخاب و انتصاب مدیران دولتی باید به گونه‌ای تغییر کند که شایسته‌سالاری و به‌گزینی جایگزین رابطه مداری شود.

نتیجه‌گیری و پیشنهاد

در عصر نوین دانش و فناوری اطلاعات نیاز جوامع انسانی به رایانه و اینترنت هر روز افزایش

یافته است. این موضوع به افراد فرصت طلب و سودجو امکان می‌دهد تا مقاصد و اهداف شوم خود را در فضای سایبری دنبال کنند. علاقه به ارتکاب جرم در فضای سایبر به دلیل نامحدود بودن و احتمال ردگیری و شناسایی پایین مجرمان توسط نهادهای امنیتی، بازرسی، نظارتی و قضایی افزایش یافته است. با توجه به گسترده‌گی دستگاه‌های اجرایی و تخصصی شدن فعالیت‌های اجرایی منحصر کردن نظارت و بازرسی به شیوه‌های سنتی و به عبارتی دستی و فیزیکی همانند آن است که در انبار کاه به دنبال سوزن بگردیم؛ بنابراین در چنین اوضاعی تنها راه حل، اعمال شیوه مدیریت و نظارت الکترونیکی است. شیوه‌ای که ما را در جهت قانون‌گرایی رهنمون می‌سازد؛ زیرا تحقق قانون‌گرایی در گرو توسعه نظارت و توسعه نظارت نیز وابسته به مدیریت نظارت است که این مهم تنها با اجرای سیستم یکپارچه نظارت الکترونیک محقق خواهد شد. بدیهی است برای تحقق نظارت الکترونیکی، ایجاد بسترهای فناوری اطلاعات و ارتباطات ضروری است و مستلزم این است که سازمان‌ها نیز به سمت الکترونیکی شدن گام بردارند.

توجه به نظام‌های یکپارچه کنترل و نظارت در سازمان‌ها نیز در همین راستا بوده و سیستم برنامه‌ریزی منابع سازمان^۱ یکی از طرح‌های مدیریتی و عملیاتی است که می‌تواند به صورت یکپارچه به تمامی اطلاعاتی که در حین عملیات تولید می‌شود نظم دهد و با ثبت، دسته‌بندی و طبقه‌بندی، پردازش و ارائه گزارش‌های مدیریتی تمامی این اطلاعات را در اختیار مدیران قرار دهد تا در نظام برنامه‌ریزی و نظارت و کنترل مورد استفاده قرار گیرند.

در خصوص الزامات نظارت الکترونیک بر جرایم رایانه‌ای پیشنهادهاى کاربردی ارائه می‌شود:

۱. آموزش و تسلط کارشناسان و بازرسان سازمان بازرسی به علوم کامپیوتر و فناوری اطلاعات؛

۲. برگزاری میزگردها، نشست‌ها، همایش‌ها و سمینارهای درون سازمانی برای بررسی و معرفی

طرح نظارت و بازرسی الکترونیکی؛

۳. اطلاع‌رسانی درون سازمانی و فرهنگ‌سازی و بسترسازی به منظور توجیه و آموزش کلیه

مدیران و همکاران سازمان بازرسی؛

۴. تعیین راهکارهای قانونی، اداری یا علمی و ضرورت آموزش تمامی مدیران دستگاه‌های

اجرایی کشور نسبت به استفاده از ابزار رایانه‌ای و فناوری اطلاعات؛

۵. تجهیز بخش‌های اداری و عملیاتی سازمان بازرسی به ابزار پیشرفته رایانه‌ای و بسترسازی

ارتباطات شبکه‌ای و راه‌اندازی سیستم نظارت و بازرسی الکترونیک در سازمان بازرسی؛

۶. آموزش تکمیلی کارشناسان سازمان بازرسی در بخش ستاد خبری و برقراری ارتباط

شبکه‌ای آن با بخش‌های مدیریتی مرتبط؛

۷. برگزاری سمینارها و میزگردهای مشترک سازمان بازرسی با هر یک از دستگاه‌های اجرایی در خصوص اجرایی شدن طرح نظارت و بازرسی الکترونیک؛
۸. برگزاری میزگردهای علمی و سمینارهای برون‌سازمانی در خصوص موضوع‌های زیر در راستای تحقق طرح:

- ۱- ۸. جایگاه نظارت و بازرسی الکترونیک در کشف و کاهش فساد و تخلفات اداری؛
- ۲- ۸. جایگاه نظارت و بازرسی الکترونیک در کاهش هزینه‌های نظارت و بازرسی؛
- ۳- ۸. چگونگی نظارت و بازرسی در مدیریت مجازی و الکترونیک؛
- ۴- ۸. دولت الکترونیک و نقش و جایگاه نظارت و بازرسی در آن (احمدی گرجی، ۱۳۸۶).

منابع و مأخذ

- احمدی گرجی، حسینعلی (۱۳۸۶)، طرح نظارت الکترونیک (دیجیتالی یا مجازی).
- اصلاتی، رشید (۱۳۷۸)، نظارت طرح‌های عمرانی، وظیفه‌ای فراموش شده در دولت، مقالات سی‌امین سالگرد تأسیس مرکز آموزش مدیریت دولتی، مجموعه یازدهم، ۱۳۸۷.
- پرنیان، حمیدرضا (۱۳۸۳)، ارتباطات و فناوری اطلاعات و نقش آن در نظارت کارآمد، مجموعه مقالات سومین همایش نظارت کارآمد.
- جاویدنیا، جواد (۱۳۸۸)، جرایم تجارت الکترونیک، تهران: نشر خرسندی.
- جلالی فراهانی، امیرحسین (۱۳۸۹)، کنوانسیون جرایم سایبر و پروتکل الحاقی آن، چاپ اول.
- حسینی، میرزا حسن و فولادی طرقي، مهدی (۱۳۸۹)، بررسی موانع و محدودیت‌های اجرای نظارت الکترونیکی، فصلنامه مطالعات مدیریت انتظامی، سال پنجم، شماره چهارم.
- رحیمیان، نظام‌الدین (۱۳۷۷)، نقش فناوری اطلاعات در حسابرسی، ماهنامه حسابدار، سال سیزدهم، شماره ۱۳۱.
- سکر، جین (۱۳۹۰)، یادگیری الکترونیکی و کتابخانه دیجیتال، ترجمه اکبر مجیدی. تهران: کتابدار.
- صادقی‌پور، ابوالفضل (۱۳۷۸)، نظارت یا کنترل کردن، مرکز آموزش مدیریت دولتی، کتابچه مقالات سی‌امین سالگرد تأسیس مرکز آموزش مدیریت دولتی، مجموعه یازدهم.

- صراف‌زاده، اصغر (۱۳۸۶)، فناوری اطلاعات در سازمان، انتشارات میر.
- عبداللهی، جواد (۱۳۸۳)، موانع و محدودیت‌های اعمال نظارت کارآمد، مجموعه مقالات سومین همایش نظارت کارآمد.
- قدمی، محسن (۱۳۸۳)، نظارت کارآمد و فراگیر در سازمان‌های نوین، مجموعه مقالات سومین همایش نظارت کارآمد.
- کریمیان، محمد وزین (۱۳۸۰)، نظارت شکلی - نظارت ماهوی، دومین همایش علمی و پژوهشی نظارت و بازرسی.
- کونتز و همکاران (۱۳۹۲)، اصول مدیریت، ترجمه: طوسی و همکاران، جلد دوم.
- Peter. Jones, "Combating Fraud & corruption in the public sector", chapman & Hall, 2011.