کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی

کارگاه آنلاین آشنایی با پایگاه های اطلاعات علمی بین المللی و ترفند های جستجو

کارگاه آنلاین
پروپوزال نویسی و پایان نامه نویسی

کارگاه آنلاین
بررسی مقابله ای متون (مقدماتی)

رتبه بندی عوامل کلیدی موفقیت در پیاده سازی سیستم مدیریت امنیت اطلاعات

علی اکبر عیسی زاده

کارشناس ارشد شبکه و ممیز داخلی سیستم مدیریت امنیت اطلاعات، اداره کل بنادر و دریانوردی استان گیلان ، ایران

eisazadeh@anzaliport.ir

چکیده

امروزه استفاده از خدمات الکترونیکی و دیجیتالی به عنوان امری بدیهی در زندگی ما انسانها جای خود را باز کرده است و تقریبا زندگی بدون استفاده از فن آوری به موضوعی تقریبا غیرممکن تبدیل شده است. در عصری که از خرید مایحتاج زندگی گرفته تا انجام عمل های جراحی فوق پیچیده و از راه دور به واسطه پیشرفت های الکترونیکی و از بستر اینترنت امکانپذیر شده است، می توان به اهمیت استفاده از خدمات فوق پی برد. به تناسب الکترونیکی شدن امور بیش از بیش مقوله امنیت اطلاعات اهمیت فوق العاده ای پیدا کرده است که مورد توجه کلیه مدیران قرار دارد. در آشفته بازار انفجار اطلاعات و شفافیت اطلاعاتی سازمانهایی که نتوانند با فراهم آوردن امنیت لازم ، اطمینان مشتریان خود را جلب نمایند با کاهش مشتری و به سوی نیستی گام خواهند برداشت. در این رهگذر پیاده سازی سیستم مدیریت امنیت اطلاعات تا حد زیادی می تواند امنیت اطلاعات را به ارمغان آورد و نشان دهنده فراهم شدن حداقل امنیت اطلاعات دیجیتالی باشد. عوامل کلیدی موفقیت در پیاده سازی سیستم مدیریت امنیت اطلاعات را می توان به عوامل فن آوری ، عوامل برون سازمانی و عوامل درون سازمانی تقسیم نمود که در این مقاله سعی شده است عوامل فوق رتبه بندی شود تا مشخص گردد کدامیک از عوامل کلیدی فوق الذکر در حین پیاده سازی سیستم مدیریت امنیت اطلاعات از اهمیت بیشتر و کدامیک از اهمیت کمتری برخوردارند.روش انجام پژوهش مطالعه موردی و تعیین پرسش نامه به روش دلفی بوده و برای تحلیل داده ها از نرم افزار اکسل استفاده شده است.

واژگان کلیدی: امنیت اطلاعات، مدیریت اطلاعات،مدیریت امنیت اطلاعات، سیستم مدیریت امنیت اطلاعات

۱- مقدمه

هر سازمانی جهت انجام امور جاری و آتی خود دارای یک سری از فرآیندها ، دستورالعمل ها و روالهای کاری مختص به خود می باشد که به تناسب ظهور فناوری های جدید نحوه انجام فرآیندها نیز دچار تغییرات اساسی می شود . استفاده از فن آوری های جدید باعث می شود تا در حالت نرمال علیرغم گستردگی تغییراتی که در فرایندها و فعالیت ها وجود دارد، انجام آنها در زمان کمتر و بهینه تر انجام گیرد. در این مقوله روشهای حفاظت از اطلاعات نیز با تغییر فن آوری ها دستخوش تغییرات اساسی می گردد و اصل حفاظت از اطلاعات در همه اعصار امری انکار نشدنی است. در این راستا ایجاد یک سیستم امنیتی قوی می تواند برای حفظ امنیت اطلاعات هر سازمان موثر باشد.بدیهی است سیستم مذکور باید علاوه بر کمک برای پیاده سازی بهینه روشهای مناسب حفاظت اطلاعات به گونه ای طراحی شود تا بتوان موارد امنیتی را کنترل و بهبود داد . از اینرو بحث طراحی و پیاده سازی سیستم مدیریت امنیت اطلاعات (**ISMS**) به عنوان ابزاری مناسب جهت طراحی و کنترل سطح امنیت اطلاعات و بهبود امنیت در سازمان مطرح می شود. در پیاده سازی سیستم مدیریت امنیت اطلاعات عوامل فراوانی دخیل هستند ، در واقع پیاده سازی هر سیستمی نیازمند زیر ساخت های خاصی است که بدون وجود آنها امکان پیاده سازی وجود ندارد از جمله زیر عوامل لازم و کلیدی می توان به عواملی مانند فن آوری، درون سازمانی و برون سازمانی نام برد که به بررسی میزان تاثیر هر یک خواهم پرداخت. لیکن در ابتدا مفاهیم اطلاعات، امنیت اطلاعات، حفاظت اطلاعات و سیستم مدیریت امنیت اطلاعات تعریف و تحقیقات پیشین مورد بررسی قرار می گیرد.

۲- مروری بر امنیت اطلاعات ، مدیریت امنیت اطلاعات و سیستم مدیریت امنیت اطلاعات و تحقیقات پیشین

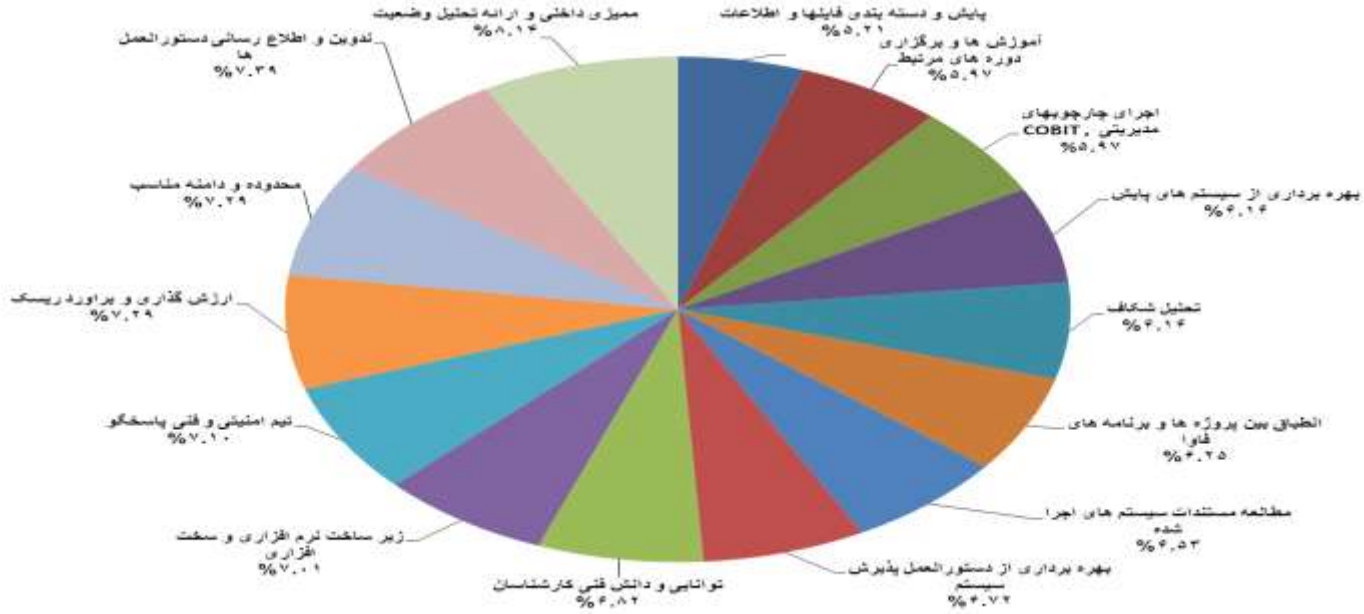
تعاریف گوناگونی برای امنیت اطلاعات وجود دارد که می توان به موارد زیر اشاره کرد: امنیت اطلاعات عبارت است از حفاظت اطلاعات و به حداقل رساندن دسترسی غیر مجاز به آنها [۳] . همچنین علم مطالعه روشهای حفاظت از داده ها در رایانه ها و نظام های ارتباطی در برابر تغییرات غیر مجاز است [۴] . از طرفی امنیت اطلاعات حفاظت از محرمانگی ، تمامیت و دسترس پذیری اطلاعات است. علاوه بر این ها سایر ویژگی ها از قبیل اصالت ، قابلیت جوابگویی ، اعتبار ، انکار ناپذیری و قابلیت اطمینان اطلاعات نیز می توانند مشمول این حفاظت باشند.مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف ، امنیت و بررسی موانع سر راه رسیدن به این اهداف و ارائه راهکارهای لازم را بر عهده دارد [۱] .

مفهوم سیستم مدیریت اطلاعات عبارت است از : بخشی از سیستم مدیریت کلی و سراسری در یک سازمان است که بر پایه ی رویکرد مخاطرات کسب و کار قرار داشته و هدف آن پایه گذاری ، پیاده سازی ، بهره برداری ، نظارت ، بازبینی ، نگهداری و بهبود امنیت اطلاعات است[۲] .

خطرهای تهدید کننده ی امنیت اطلاعات را می توان در دو دسته خطرات عمدی و طبیعی تقسیم نمود. برای مقابله با تهدیدات فوق می بایست یک سیستم مدیریت امنیت اطلاعات طراحی گردد که فازهای تضمین امنیت اطلاعات در آن عبارتند از: - تعریف دامنه و محدوده – ارزیابی تهدیدات – ارزیابی آسیب پذیری ها –ارزیابی ریسک – استراتژی مدیریت ریسک و نقشه امنیتی – پیاده سازی نقشه امنیتی – ارزیابی ،بازبینی و ممیزی امنیتی[۵] .اجرای سیستم مدیریت امنیت اطلاعات در صورت تحقق سه شرط اطمینان، دقت و قابلیت دسترسی بشرح ذیل قابل بررسی است: الف- اطمینان : از سلامت اطلاعات چه در زمان ذخیره و چه به هنگام بازیابی و ایجاد امکان برای افرادی که مجاز به استفاده از اطلاعات هستند. ب)دقت : اطلاعات چه از نظر منبع ارسالی و چه در هنگام ارسال و بازخوانی آن باید از دقت و صحت برخوردار باشند و ایجاد امکاناتی در جهت افزایش این دقت ضرورت خواهد داشت. ج) قابلیت دسترسی : اطلاعات برای افرادی که مجاز به استفاده از آن می باشند باید

در دسترس بوده و امکان استفاده در موقع لزوم برای این افراد مقدور باشند [۶] . در ارتباط با پیاده سازی سیستم مدیریت امنیت اطلاعات و بررسی عوامل موثر در پیاده سازی آن پیش تر نیز تحقیقاتی صورت پذیرفته است.

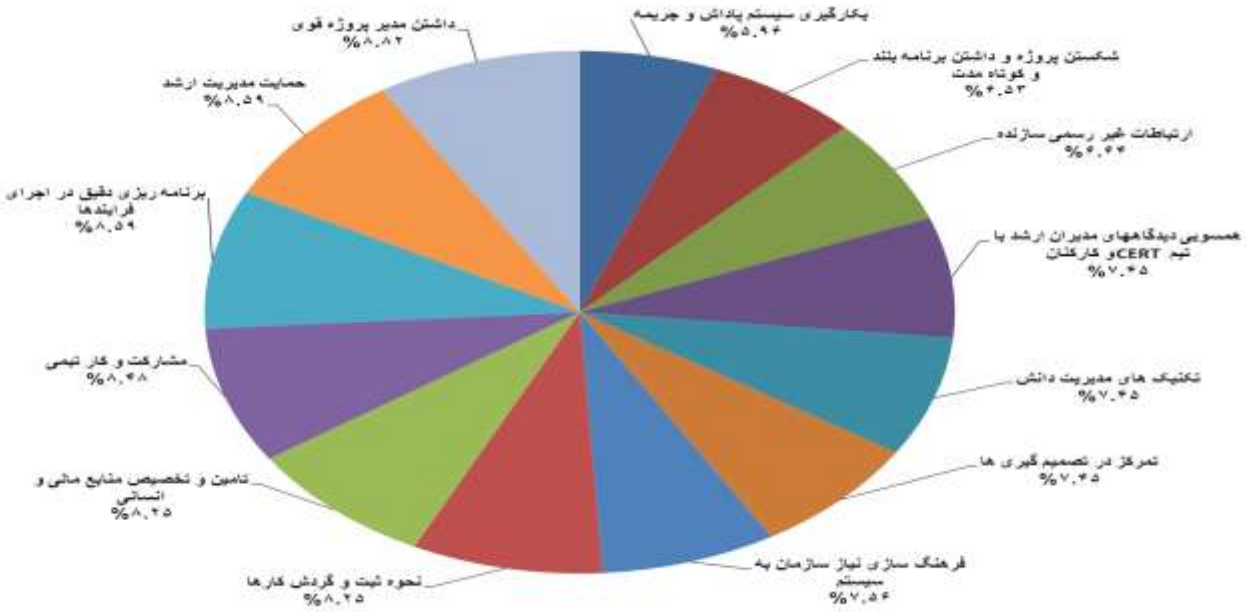
در مقاله ای تحت عنوان " شناسایی و رتبه بندی عوامل فن آوری موثر در پیاده سازی سیستم مدیریت امنیت اطلاعات" به قلم اینجانب ، ۱۵ عامل از عوامل فن آوری به ترتیب وجود ممیزین داخلی بمنظور تحلیل وضعیت، تدوین و اطلاع رسانی مناسب دستورالعمل ها، انتخاب دامنه و محدوده مناسب، ارزش گذاری و برآورد مناسب ریسک، وجود تیم فنی و امنیتی پاسخگو، زیر ساخت های نرم افزاری و سخت افزاری مناسب، توانایی و دانش فنی کارشناسان، بهره برداری از دستورالعمل پذیرش سیستم، مطالعه مستندات سیستم های اجرا شده، انطباق بین پروژه ها با اسناد بالا دستی و برنامه های فاوا، تحلیل شکاف ، بهره برداری از سیستم های پایش، اجرای چارچوب های مدیریتی موجود مانند **COBIT, ITIL, …** ، آموزش و برگزاری دوره های مرتبط و دسته بندی و پایش اطلاعات و فایل ها رتبه بندی گردید [۷] .شکل ۱ نمودار دایره ای رتبه بندی عوامل فن آوری موثر در پیاده سازی ISMS را نشان می دهد.



شکل ۱: نمودار دایره ای رتبه بندی عوامل فن آوری موثر در پیاده سازی ISMS

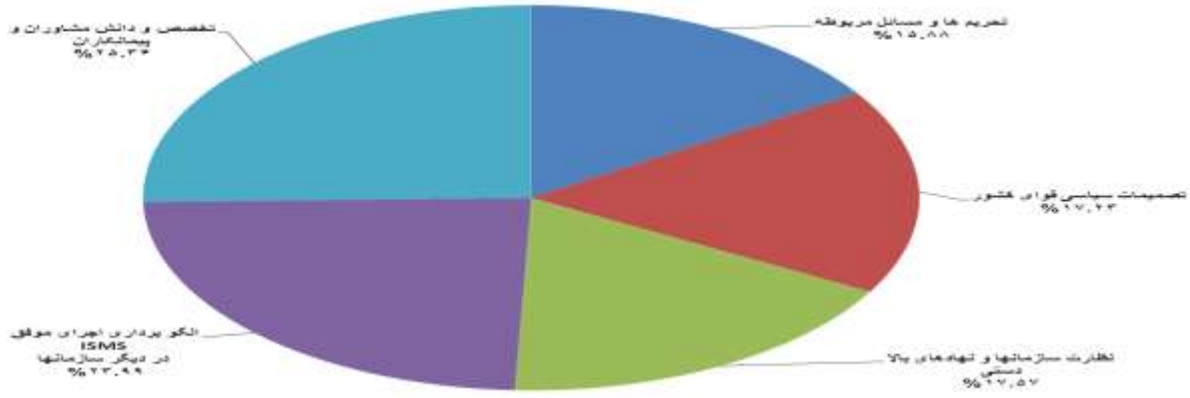
در مقاله ای دیگر تحت عنوان " شناسایی و رتبه بندی عوامل درون سازمانی موثر در پیاده سازی سیستم مدیریت امنیت اطلاعات" به قلم اینجانب ، ۱۳ عامل از عوامل درون سازمانی به ترتیب داشتن مدیر امنیت اطلاعات قوی ، حمایت مدیران ارشد سازمان از تیم پیاده ساز به همراه برنامه ریزی دقیق در اجرای فرآیندها و ایجاد روحیه مشارکت و انجام کار تیمی به عنوان سه عامل اصلی درون سازمانی موثر در پیاده سازی ISMS می باشند و موارد همچون تامین و تخصیص منابع مالی و انسانی، نحوه ثبت و گردش کارها، فرهنگ سازی سازمانی به منظور پذیرش سیستم، تمرکز در تصمیم گیریها و همسویی دیدگاه های مدیران با کارکنان به همراه استفاده از تکنیک های مدیریت دانش در رتبه های بعدی قراردارند. همچنین مشخص گردیدکه عوامل درون سازمانی همچون ارتباطات غیر رسمی سازنده، و داشتن برنامه های کوتاه و بلند مدت و بکارگیری سیستم پاداش و جریمه کمترین تاثیر درون سازمانی در پیاده سازی سیستم مدیریت امنیت اطلاعات در محدوده مورد مطالعه

را داشته و در سه رتبه آخر رتبه بندی قرار گرفته اند. شکل ۲ نمودار دایره ای رتبه بندی عوامل درون سازمانی موثر در پیاده سازی ISMS را نشان می دهد.



شکل ۲: نمودار دایره ای رتبه بندی عوامل درون سازمانی موثر در پیاده سازی ISMS

در مقاله ای دیگر تحت عنوان " شناسایی و رتبه بندی عوامل برون سازمانی موثر در پیاده سازی سیستم مدیریت امنیت اطلاعات" به قلم اینجانب ، ۵ عامل از عوامل برون سازمانی به ترتیب استفاده از دانش و تخصص مشاوران مجرب و پیمانکاران متخصص به همراه الگو برداری اجرای موفق سیستم مدیریت امنیت اطلاعات در دیگر سازمانها به عنوان دو عامل اصلی و مهم و نظارت سازمانها و نهادهای بالا دستی، تصمیمات سیاسی قوای کشور و از همه مهمتر تحریم ها کمترین تاثیر برون سازمانی در پیاده سازی سیستم مدیریت امنیت اطلاعات در محدوده مورد مطالعه را داشته اند. شکل ۳ نمودار دایره ای رتبه بندی عوامل برون سازمانی موثر در پیاده سازی ISMS را نشان می دهد.



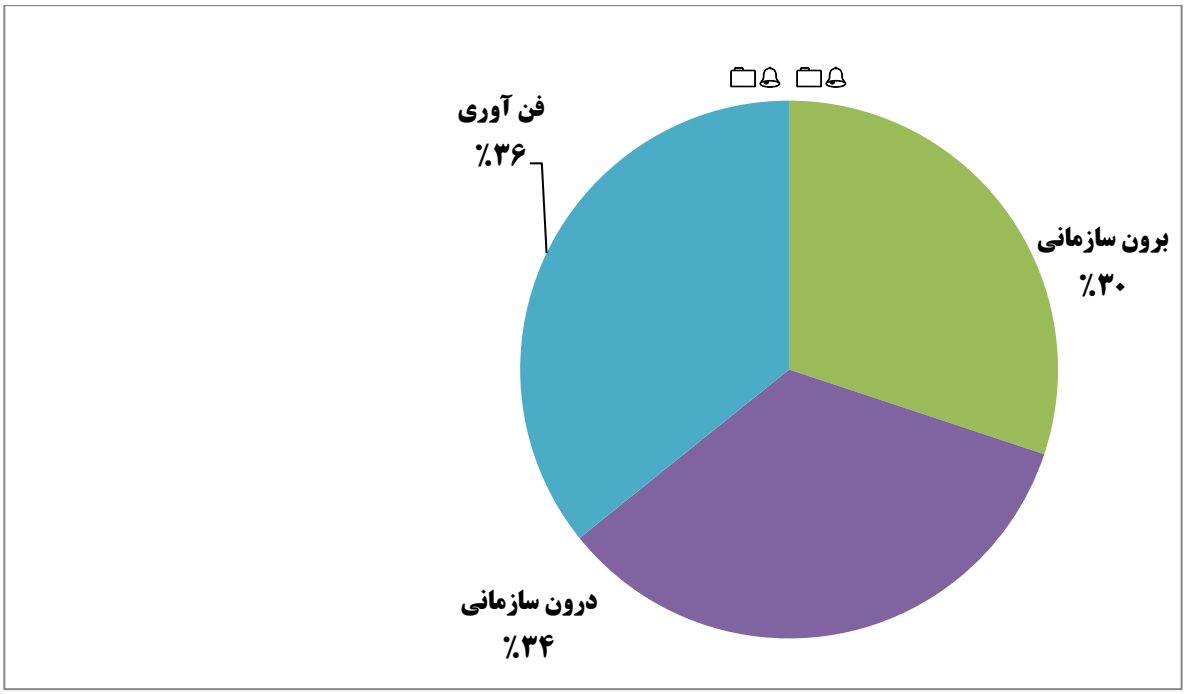
شکل ۳: نمودار دایره ای رتبه بندی عوامل برون سازمانی موثر در پیاده سازی ISMS

در این مقاله از دیدگاه کلی به رتبه بندی عوامل کلیدی موفقیت در پیاده سازی سیستم مدیریت امنیت اطلاعات پرداخته شده است.

۳- عوامل کلیدی موفقیت در پیاده سازی سیستم مدیریت امنیت اطلاعات

در تحقیق انجام شده ۳ عامل به عنوان عوامل کلیدی موفقیت در پیاده سازی سیستم مدیریت امنیت اطلاعات شناسایی شده است که عبارتند از عوامل فن آوری ، درون سازمانی و برون سازمانی. بمنظور اینکه نتایج تحقیق به واقعیت نزدیک تر باشد سعی شده است پرسشنامه ها در یک سازمانی که موفق به پیاده سازی سیستم مدیریت امنیت اطلاعات شده است و در بین افرادی که در پیاده سازی سیستم مدیریت امنیت اطلاعات تاثیر مستقیم داشته اند (کارگروه راهبری سیستم، مدیران و کارشناسان حوزه فناوری اطلاعات، مشاوران سیستم) – پخش شود و سپس با استفاده از روشهای موجود به تجزیه و تحلیل اطلاعات پرداخته شود و در نهایت نتایج اعلام گردد.

با توجه به نتایج مطالعات و تحقیقات انجام شده قبلی و همانگونه که در شکل ۴ نمودار دایره ای رتبه بندی عوامل کلیدی موفقیت در پیاده سازی ISMS مشاهده میگردد، عوامل فن آوری مهمترین عامل موفقیت در پیاده سازی سیستم مدیریت امنیت اطلاعات در سازمانهاست و میزان تاثر آن ۳۶ درصد بوده است. این در حالی است که محاسبات نشان می دهد عوامل درون سازمانی ۳۴ درصد در موفقیت پیاده سازی سیستم مدیریت امنیت اطلاعات نقش داشته است و عوامل برون سازمانی با ۳۰ درصد تاثیر، کمترین نقش را ایفا نموده است.



شکل ۴: نمودار دایره ای رتبه بندی عوامل کلیدی موثر در پیاده سازی ISMS

۴-نتیجه گیری

با انجام تحقیق فوق ۳ عامل کلیدی موفقیت در پیاده سازی سیستم مدیریت امنیت اطلاعات بررسی شد. اگر چه نتایج و میزان تاثیر هر کدام نزدیک بهم هستند اما مشخص شد که عوامل فن آوری به عنوان مهمترین عامل کلیدی موفقیت در پیاده سازی ISMS می باشد و عوامل درون سازمانی در رتبه دوم و مهمتر از عوامل برون سازمانی می باشد و عوامل برون سازمانی در رتبه سوم و آخر از عوامل کلیدی موفقیت در پیاده سازی سیستم مدیریت امنیت اطلاعات در محدوده مورد مطالعه قرار

گرفته اند. با توجه به نتایج فوق پیشنهاد می شود مدیران قبل از پیاده سازی سیستم مدیریت امنیت اطلاعات نسبت به فراهم نمودن بسترهای لازم فن آوری ، درون سازمانی و در نهایت برون سازمانی اقدام نمایند و با برنامه ریزی مناسب و اختصاص بودجه های لازم ، امر پیاده سازی سیستم مدیریت امنیت اطلاعات را تسهیل نمایند.

منابع :

۱.اسعدی شالی ، عادله، مرداد ۱۳۸۴ ، مدیریت سیستمهای امنیت اطلاعات ، مجله الکترونیکی مرکز اطلاعات و مدارک علمی ایران ، شماره چهارم ، دوره چهارم

۲.پورمند ، علی ، استانداردی برای امنیت اطلاعات ، ماهنامه تدبیر، سال هفدهم، شماره ۱۷۸

۳.جعفری ، نیما ، سیستم مدیریت امنیت اطلاعات از طرح تا اصلاح ، ماهنامه تدبیر ، شماره ۱۸۹

۴.عبد اللهی ، محمد ، طراحی و پیاده سازی سرویسهای امن برای شبکه های کامپیوتری ، پایان نامه کارشناسی ارشد ، دانشگاه صنعتی شریف

۵.ذاکرالحسینی، علی؛ ملکیان،احسان،۱۳۹۰، امنیت داده ها، نسخه سوم، نص

۶.کورنگی ، حیدر علی ، تیرماه ۱۳۸۷ ، پنجمین سمینار آموزشی شبکه علمی غرب آسیا ، دانشکده مهندسی برق و کامپیوتر دانشگاه شهید بهشتی

۷.عیسی زاده، علی اکبر،۱۳۹۳، شناسایی و رتبه بندی عوامل فناوری و تکنولوژی موثر در پیاده سازی سیستم مدیریت امنیت اطلاعات، همایش بین المللی مدیریت، تهران، موسسه سفیران فرهنگی مبین

۸.عیسی زاده، علی اکبر، ۱۳۹۴، شناسایی و رتبه بندی عوامل درون سازمانی موثر در پیاده سازی سیستم مدیریت امنیت اطلاعات، کنفرانس بین المللی پژوهش های کاربردی در فناوری اطلاعات، کامپیوتر و مخابرات ، تربت حیدریه، دانشگاه آزاد تربت حیدریه و شرکت مخابرات خراسان رضوی

۹.عیسی زاده، علی اکبر، ۱۳۹۴، شناسایی و رتبه بندی عوامل برون سازمانی موثر در پیاده سازی سیستم مدیریت امنیت اطلاعات، کنفرانس بین المللی اقتصاد، مدیریت و حسابداری با رویکرد ارزش آفرینی، شیراز، موسسه آموزشی مدیران خبره نارون

کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی

کارگاه آنلاین آشنایی با پایگاه های اطلاعات علمی بین المللی و ترفند های جستجو

کارگاه آنلاین
پروپوزال نویسی و پایان نامه نویسی

کارگاه آنلاین
بررسی مقابله ای متون (مقدماتی)