فصلنامه مطالعات مدیریت فناوری اطلاعات سال چهارم، شماره ۱۶، تابستان ۹۵
صفحات ۱۴۷ تا ۱۷۶

ارائه چارچوبی برای بررسی عوامل درون‌سازمانی مؤثر بر امنیت سامانه‌های اطلاعاتی با استفاده از روش تحلیل سلسله مراتبی فازی

علیرضا پیکام *
خداکرم سلیمی فرد **

چکیده

یکی از زیر بخش‌های فناوری اطلاعات که به‌رغم جدید بودن موضوع آن دارای اهمیت فراوانی در ایجاد اطمینان و رشد کاربرد سامانه‌های اطلاعاتی است، امنیت سامانه‌های اطلاعاتی است. گرچه در سالیان اخیر جنبه‌های فنی موضوع امنیت موردتوجه فراوان پژوهشگران و متخصصان حوزه فناوری اطلاعات قرارگرفته، بنابراین کمتر به ابعاد مدیریتی و سازمانی آن توجه شده است. برای بررسی عوامل ایجاد و حفظ امنیت سامانه‌های اطلاعاتی، این پژوهش عوامل درون‌سازمانی تأثیرگذار بر امنیت سامانه‌های اطلاعاتی را شناسایی می‌کند و با تهیه پرسش‌نامه و با استفاده از فرآیند تصمیم‌گیری سلسله مراتبی فازی وزن هر یک از شاخص‌ها را به دست می‌آورد و در پایان آن‌ها را

* کارشناس ارشد مدیریت صنعتی، دانشکده ادبیات و علوم انسانی، دانشگاه خلیج فارس، بوشهر. (نویسنده مسئول)؛ Peykam.alireza67@gmail.com
** استادیار گروه مدیریت صنعتی، دانشکده ادبیات و علوم انسانی، دانشگاه خلیج فارس، بوشهر.
تاریخ دریافت: ۹۴/۰۵/۳۰ تاریخ پذیرش: ۹۵/۰۷/۰۵

رتبه‌بندی می‌کند. نتایج به‌دست‌آمده نشان می‌دهد، عامل نیروی انسانی مهم‌ترین عامل درون‌سازمانی تأثیرگذار بر امنیت سامانه‌های اطلاعاتی و نیز در این شاخص، زیر شاخص عدم اطلاع از میزان ارزش اطلاعات با اهمیت‌ترین زیر شاخص شناخته‌شده است.

کلیدواژگان: امنیت اطلاعات، عوامل درون سازمانی، سامانه اطلاعاتی، تحلیل سلسله‌مراتب فازی

مقدمه

تاکنون نقش سامانه‌های اطلاعاتی و فناوری اطلاعات در کسب‌وکارها و رساندن آن‌ها به عرصه‌ی رقابت بسیار موردبحث قرارگرفته است. استفاده از سامانه‌های اطلاعاتی و فناوری اطلاعات برای کسب‌وکارها، مزیت رقابتی به وجود می‌آورد (مانیان و همکاران، ۱۳۹۳). یکی از سرمایه‌های مهم واصلی برای هر سازمانی اطلاعات آن است که تحت هر شرایطی باید محفوظ بماند و تدابیر امنیتی خاصی برای آن لحاظ شود. این تدابیر شامل ایمن‌سازی فیزیکی و منطقی اطلاعات، جلوگیری از نفوذ بیگانگان، آسیب‌ها و تهدیدات است که از سخت‌ترین وظایف هر سازمانی است. تمامی موارد عنوان‌شده مبین اهمیت فوق‌العاده امنیت اطلاعات است. از سوی دیگر به دلیل آنکه امروزه نیازها، کسب‌وکار، تجارت، امور مالی و بانکی توسط شبکه جهانی اینترنت مرتفع می‌شوند و روزبه‌روز بر استفاده از این شبکه افزوده می‌شود، بنابراین اهمیت امنیت اطلاعات دوچندان می‌شود. ازآنجاکه ضروری است اطلاعات از جهت‌های مختلف ایمن شود پس امنیت اطلاعات عملی یک‌سویه نیست و باید آن را مدیریت کرد؛ بنابراین لازم است یک سیستم مدیریتی را برای آن در نظر گرفت تا بتوان توسط آن امنیت که جزء جدایی‌ناپذیر اطلاعات است را تضمین کرد (جدّی و همکاران، ۱۳۹۰). از فناوری اطلاعات می‌توان به‌عنوان بزرگ‌ترین فناوری در طول تاریخ یادکرد که توانسته بین رشته‌های مختلف علوم، ارتباط برقرار کند. این فناوری با به‌کارگیری تمام علوم توانسته است اطلاعات موردنیاز پژوهشگران، صنعتگران، بازرگانان و همچنین قشرهای مختلف جامعه را در کمترین زمان و بهترین وجه فراهم کند، به‌طوری‌که می‌توان ادعا کرد امروزه فناوری اطلاعات، مرزهای کشورهای مختلف را درنوردیده و ملت‌ها را در یک جامعه جهانی گرد هم آورده است.

گفتن و شنیدن از مزایای فناوری اطلاعات و امکاناتی که برای بشر به ارمغان آورده همواره لذت‌بخش است؛ اما این فناوری همانند سایر فناوری‌ها همچون سکه دو رو دارد: «فرصت» و «تهدید» و اگر به همان اندازه که به توسعه و فراگیری آن توجه می‌شود

به امنیت آن توجه نشود می‌تواند به یک تهدید و مصیبت بزرگ تبدیل شود. حجم بالای اطلاعات در هر سازمان در قالب طرح‌ها، نقشه‌ها، سیاست‌ها، بخشنامه‌ها، مکاتبات بازرگانی، مستندات پروژه‌های پژوهشی و سایر اطلاعاتی که سازمان برای ذخیره‌سازی و پردازش در اختیار این فناوری قرار می‌دهد، سازمان را بر آن می‌دارد تا به فکر حفاظت از آن نیز باشد. اطلاعات یادشده مهم‌ترین دارایی و کلید رشد و موفقیت هر سازمان است. اگر سازمان نتواند این دارایی مهم را از دسترس تهدیدها حفظ کند، به‌شدت آسیب می‌بیند. پژوهشگران بر این باورند که اکثر سازمان‌ها بدون توجه به تهدیدات فناوری اطلاعات، هزینه‌های بسیاری برای توسعه این فناوری صرف می‌کنند و اغلب با اجرای راهبردهای مقطعی (مانند نصب آنتی‌ویروس، دیوار آتش و...) سعی دارند تا سازمان و اطلاعات خود را حفظ کنند. بسیار مشاهده‌شده است سازمان‌ها خسارت شدیدی را از این بابت متحمل شده‌اند، اما متأسفانه همین روش را هم چنان ادامه می‌دهند (محمود زاده و همکاران، ۱۳۸۵). ضرورت این پژوهش ازآنجا احساس می‌شود که در عصر حاضر سازمان‌ها باارزش‌ترین دارایی خود را جهت پردازش و ذخیره‌سازی در اختیار تجهیزات فناوری اطلاعات قرار داده‌اند. وابستگی به این فناوری باعث شده است تا اگر در ارائه خدمات خللی پیش آید سازمان‌ها نتوانند به کار خود ادامه دهند. بدین ترتیب حیات سازمان‌ها ارتباط نزدیکی با سامانه‌های اطلاعاتی آن‌ها دارد. سامانه‌های اطلاعاتی نیز همواره درخطر سرقت اطلاعات، تغییر اطلاعات و ایجاد وقفه در ارائه خدمات می‌باشند. ازاین‌رو سازمان‌ها برای ایمن ماندن از این آسیب‌ها باید به فکر امنیت اطلاعات باشند.

هدف از انجام این پژوهش، بررسی و شناسایی عوامل درون‌سازمانی مؤثر بر امنیت سامانه‌های اطلاعاتی است که در این راستا ادبیات نظری مرتبط مطالعه و شاخص‌های تأثیرگذار استخراج می‌شود. سپس با استفاده ازنظر خبرگان و صاحب‌نظران این حوزه شاخص‌ها تعدیل و تجمیع شده و پرسش‌نامه‌ی مرسوم AHP تهیه و بین خبرگان دانشگاهی و متخصصان سازمان‌های دولتی شهر بوشهر توزیع‌شده است و در پایان وزن

شاخص‌ها با استفاده از روش تحلیل سلسله مراتبی فازی به دست می‌آید.

پیشینه پژوهش

تا دهه ۷۰، فعالیت‌های مربوط به دسترسی و محافظت از اطلاعات در سازمان‌ها و شرکت‌ها محدود به محل‌های نگهداری این اطلاعات شامل آرشیو اسناد و شبکه‌های محلی رایانه‌ای بود. در چنین محیط‌هایی، حفاظت فیزیکی، امنیت سامانه‌های اطلاعات را تا حد بسیار بالایی تأمین می‌کرد. درواقع تا اوایل دهه ۸۰ میلادی امنیت را فقط با دیدگاه فنی مشاهده و برقراری آن را منوط به امنیت رایانه و دستگاه‌های جانبی می‌دانستند؛ اما باگذشت زمان متوجه شدند که بیشتر تجاوزهای امنیتی از طریق مسائلی همچون ضعف‌های مدیریتی (ازلحاظ امنیتی) و عوامل انسانی (به دلیل عدم آموزش) است؛ بنابراین از اواسط دهه ۸۰ میلادی تا اواسط دهه ۹۰ میلادی بحث مدیریت امنیت اطلاعات مطرح شد که آن را منوط به خط‌مشی امنیت اطلاعات و ساختارهای سازمانی می‌دانستند. از اواسط دهه ۹۰ میلادی پارامترهای دیگری چون تعریف استراتژی‌های امنیتی و خط‌مشی امنیتی بر اساس نیازهای اصلی سازمان و مدیریت آن مطرح شد که این پارامترها مؤلفه‌هایی چون استانداردهای امنیت اطلاعات، گواهی‌نامه‌های بین‌المللی، فرهنگ‌سازی امنیت اطلاعات در سازمان و پیاده‌سازی معیارهای ارزیابی دائمی و پویای امنیت اطلاعات را نیز شامل می‌شود (قاسمی شبانکار و همکاران، ۱۳۸٦). در استاندارد ISO /IEC ۱۷۷۹۹ که روش استقرار امنیت اطلاعات در سازمان را ارائه می‌دهد،۱۰ عامل که در مدیریت امنیت اطلاعات مؤثرند به‌صورت زیر بیان‌شده‌اند: ۱ـ سیاست امنیت اطلاعات ۲ـ امنیت سازمانی ۳ـ کنترل و دسته‌بندی سرمایه ٤ـ امنیت کارکنان ۵ـ امنیت محیطی و فیزیکی ٦ـ مدیریت عملیات و تولید ۷ـ کنترل دسترسی ۸ـ امنیت سامانه‌های اطلاعاتی ۹ـ مدیریت حیات و دوام سازمان ۱۰ـ سازگاری (مؤسسه‌ی استاندارد و تحقیقات صنعتی ایران). در کتاب فرآیند آموزش اجرای یک سیستم مدیریت امنیت اطلاعات، نویسنده از اجزای زیر به‌عنوان تهدیدهای سیستم اطلاعاتی و عواملی که باید

کنترل بشوند نام‌برده است: سند سیاست امنیت اطلاعاتی، بازبینی و ارزیابی، محکمه‌ی امنیت اطلاعات ـ مدیریت، هماهنگی امنیت اطلاعاتی، تخصیص مسئولیت‌های امنیت اطلاعات، فرآیند اختیارات برای تسهیلات فرآیند اطلاعات، مشاوره‌ی امنیت اطلاعات تخصصی، لحاظ کردن امنیت در مسئولیت‌های شغلی، گزینش افراد، توافق‌های محرمانه، ضوابط استخدام، آموزش امنیت اطلاعات، فرآیند انضباطی، تفکیک وظایف و ممانعت سوءاستفاده از تسهیلات اطلاعاتی. جیم کلینچ، امنیت اطلاعات را در ٤ بعد با زیر شاخص‌هایش دسته‌بندی می‌کند که عبارت‌اند از: افراد (ارتباطات ـ آگاهی ـ آموزش ـ تصدیق) فرآیندها (مدیریت ریسک ـ مدیریت رویداد و مدیریت اطلاعات) محصولات / فنّاوری (فایروال ـ فیلترهرزنامه و...) شرکا / تأمین‌کنندگان (فروشندگان ـ تولیدکنندگان ـ آژانس‌ها) (کلینچ[1]، ۲۰۰۹). دیزازالی و همکاران[2]، دورنمای امنیت اطلاعات و سطح بلوغ در سازمان‌های خدمات عمومی مالزی را با استفاده از جمع‌آوری پرسش‌نامه، بررسی کرده‌اند. آن‌ها در مطالعات خود، تهدیدات زیر را برای امنیت اطلاعات برشمرده‌اند: ناشناسی هویت کاربر، خطاهای ارسال و انتقال، دسترسی غیرمجاز به کامپیوتر، اطلاعات، خدمات و کاربردها، خطای نگهداری، نقص نرم‌افزار، نقص تجهیزات و خدمات ارتباطی، خطای کاربر، نقص تأمین (قدرت، تهویه‌ی مطبوع) (دیزازالی و همکاران، ۲۰۰۹). بوجانس و جرمن بلاسیک[3] یک رویکرد مدل‌سازی اقتصادی برای مدیریت ریسک امنیت اطلاعات ارائه داده‌اند. آن‌ها در این مقاله تهدیدات امنیت اطلاعات را به دودسته‌ی کلی حادثه‌های طبیعی و فعالیت‌های انسانی تقسیم کرده‌اند. آن‌ها سرقت، دستیابی غیرمجاز به خدمات شبکه، نفوذ کدهای مخرب، افشای اطلاعات شخصی و سازمانی را نمونه‌ای از تهدیدات انسانی برمی‌شمارند (بوجانس و جرمن بلاسیک، ۲۰۰۸). رن وی فانگ و همکاران[4]، تغییرات غیرمجاز برای فاش یا انحراف اطلاعات،

1. Clinch
2. Dzazali et al.
3. Bojanc & Jerman-Blazic
4. Ren-Wei Fung et al.

غفلت کاربران و فساد اطلاعات، نرسیدن یا رسیدن ناقص اطلاعات، عدم پذیرش خدمات و برگشت اطلاعات را به‌عنوان تهدیدات سامانه‌های اطلاعاتی معرفی می‌کنند (رن وی فانگ و همکاران، ۲۰۰۳). فارن و همکاران[1]، تهدیدات امنیت اطلاعات را به سه دسته‌ی فنّاوری، افراد و عملیات تقسیم می‌کنند (فارن و همکاران، ۲۰۰۸). دوهرتی و فولفرد[2] رابطه‌ی بین سیاست امنیت اطلاعات و برنامه‌ریزی سامانه‌های اطلاعاتی استراتژیک را بررسی کرده‌اند. آن‌ها استفاده‌ی شخصی از سامانه‌های اطلاعاتی، افشای اطلاعات، امنیت فیزیکی زیرساخت‌ها و اطلاعات، تخطی و نقض امنیت، ممانعت از ویروس‌ها و هکرها، مدیریت دسترسی کاربر، محاسبه‌ی سیار، توسعه و نگهداری نرم‌افزار، رمزدار کردن و برنامه‌ریزی مستمر را از مؤلفه‌های سیاست امنیت اطلاعات معرفی کرده‌اند (دوهرتی و فولفرد، ۲۰۰۶). کرامرو همکاران[3]، در پژوهشی عامل‌های انسانی و سازمانی امنیت اطلاعات و کامپیوتر را بررسی کرده‌اند. آن‌ها عوامل را در ۹ دسته طبقه‌بندی کرده‌اند: نفوذ از خارج، خطای انسانی، مدیریت، سازمان، مدیریت منابع، مدیریت عملکرد، مسائل سیاست‌گذاری، فنّاوری و آموزش (کرامر و همکاران، ۲۰۰۹). کیم و همکاران[4]، در پژوهش خود تأثیر امنیت اطلاعات هتل را بر قابلیت اطمینان سیستم بررسی کرده‌اند. آن‌ها انواع امنیت اطلاعات را در ۹ دسته طبقه‌بندی کرده‌اند: امنیت شبکه، امنیت سازمان، امنیت ریسک محیطی، امنیت کامپیوتر، امنیت اینترنت، استمرار و تداوم کسب‌وکار، امنیت کنترل ثبت، کنترل دسترسی به سیستم و مدیریت قفل‌گذاری که برای هرکدام نیز عواملی را مطرح می‌کنند (کیم و همکاران، ۲۰۱۲). ایفیندو[5] در مطالعه‌ای پذیرش سیاست‌های امنیت اطلاعات از دیدگاه‌های نظری پیوند اجتماعی، نفوذ اجتماعی و پردازش شناختی را بررسی کرده است. در نتایج مطالعه‌ی وی بیان می‌شود که یکی از دلایل ادامهٔ حوادث امنیتی سیستم‌های اطلاعاتی، سوء استفاده‌ها و

1. Farn et al.
2. Doherty & Fulford
3. Kraemer et al.
4. Kim et al.
5. Ifinedo

تخریب برای ضربه زدن به سازمان‌ها، این است که کارمندان ضعیف‌ترین حلقه‌ی ارتباطی در تأمین امنیت سیستم‌های اطلاعاتی هستند و برای سازمان تهدید داخلی به شمار می‌روند؛ پس نگرش این است که سازمان‌ها باید بر ذهنیت کارمندان و رفتارهای آن‌ها برای حفاظت از منابع تمرکز کنند (ایفیندو، ۲۰۱٤). وی و همکاران[1] نیز در پژوهشی به ارزیابی امنیت سیستم‌های اطلاعاتی بر اساس سیستم‌های پویا پرداخته‌اند. نویسندگان با استفاده از سیستم‌های پویا به دنبال شناسایی ریسک‌های بالقوه در امنیت سیستم‌های اطلاعاتی هستند که با استفاده از روش‌های سنتی شناسایی این ریسک‌ها غیرممکن است. آن‌ها با استفاده از نتایج پژوهش خود بیان می‌کنند که ریسک انسانی به دلیل غیرقابل‌پیش‌بینی بودن انسان به‌مراتب بیشتر از ریسک محیطی است که اغلب قابل پیش‌بینی و بدون تغییر است. همچنین ریسک‌های سخت‌افزار، نرم‌افزار و داده نیز در حال افزایش هستند (وی و همکاران، ۲۰۱۵).

در ایران نیز مطالعاتی در زمینه امنیت سامانه‌های اطلاعاتی صورت گرفته که تعدادی از آن‌ها به شرح زیر است: محمود زاده و رادرجبی در مطالعه‌ی خود به‌مرور پژوهش‌های پیشین در زمینه عوامل تأثیرگذار بر امنیت اطلاعات پرداختند و مدلی ارائه داده‌اند که در آن امنیت نیروی انسانی، امنیت فیزیکی و امنیت فنی عوامل مؤثر بیان‌شده‌اند. اعتبار مدل با طراحی و اجرای پرسش‌نامه موردسنجش قرارگرفته است. نتایج حاصل از پژوهش نشان می‌دهد مؤلفه‌ی عدم آگاهی کاربران بالاترین تهدید و پس‌ازآن امنیت نیروی انسانی دومین تهدید برای امنیت اطلاعات سامانه‌های رایانه‌ای است. مؤلفه‌های امنیت فیزیکی و امنیت اطلاعات به ترتیب در رتبه‌های بعدی قرار دارند (ابراهیم محمود زاده و همکاران، ۱۳۸۵). اسعدی شالی در پژوهش خود اشتباه‌های انسانی، خطرات ناشی از عوامل طبیعی، ایرادات سامانه‌ای و فعالیت‌های خرابکارانه را انواع خطرهای تهدیدکننده‌ی سیستم اطلاعاتی معرفی می‌کند. او برای مقابله با این تهدیدات انجام اعمالی مانند تعیین سیاست امنیتی اطلاعات، اعمال سیاست‌های مناسب، بررسی بلادرنگ وضعیت امنیت

1. Wei et al.

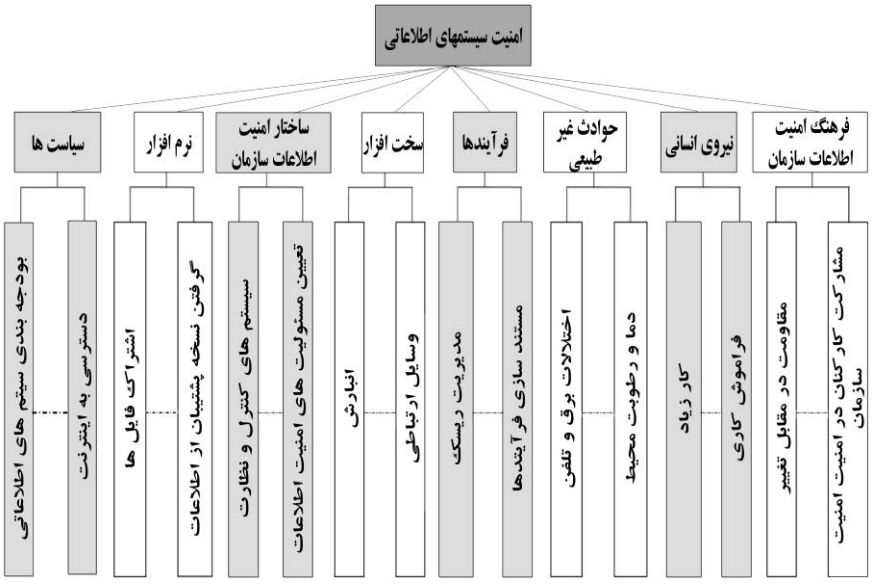
اطلاعاتی بعد از اعمال سیاست امنیتی، بازرسی و آزمون امنیت اطلاعاتی و بهبود روش‌های امنیت اطلاعاتی سازمان را پیشنهاد می‌کند (عادله اسعدی شالی، ۱۳۸٤). قاسمی شبانکاره و همکاران، تهدیدات موجود در پیش روی سامانه‌های امنیت اطلاعاتی را به ۳ دسته تقسیم می‌کنند: افشای اطلاعات محرمانه، صدمه به یکپارچگی اطلاعات (دست‌کاری) و موجود نبودن اطلاعات. آن‌ها افشای اطلاعات را مهم‌ترین تهدید امنیت اطلاعات می‌دانند. آن‌ها عواملی را به‌عنوان خطرهای تهدیدکننده‌ی سیستم معرفی می‌کنند که عبارت‌اند از: اشتباه‌های انسانی، بلایای طبیعی، ایرادات سامانه‌ای، فعالیت‌های خرابکارانه، اتخاذ سیاست‌های امنیتی (شبانکاره و همکاران، ۱۳۸٦). الهی و همکاران نیز در پژوهش خود چارچوب جدیدی برای عوامل انسانی مرتبط در امنیت سیستم‌های اطلاعاتی ارائه داده‌اند که آن را مسئله انسانی و مسئله سازمانی می‌نامند. این الگو بر امنیت اطلاعات رفتاری تمرکز دارد و در آن بر این نکته که کاربران و در کل عوامل انسانی، ضعیف‌ترین و سست‌ترین عنصر آسیب‌پذیر در مدل‌های امنیت سیستم‌های اطلاعاتی مطرح‌اند تأکید می‌شود. هدف این پژوهش، به‌طور خاص شناسایی و مدل‌سازی سازه‌های مدیریتی حیاتی و اساسی مؤثر بر اثربخشی امنیت سیستم‌های اطلاعاتی است. در این راستا، سازه‌های حمایت مدیریت عالی، آموزش امنیتی، فرهنگِ امنیتی، مهارت امنیتی، تقویت خط‌مشی امنیتی، تجربیات و خودباوری افراد به‌عنوان فاکتورهای مؤثر بر اثربخشی امنیت سیستم‌های اطلاعاتی معرفی می‌شوند (الهی و همکاران، ۱۳۸۸). اشاره به این نکته ضروری است که فرهنگ‌سازمانی نیز از طریق میزان پشتیبانی مدیریت ارشد (کناپ و همکاران[1]، ۲۰۰٦) مقاومت در مقابل تغییر، جوابگویی و مسئولیت‌پذیری (رویقاور و همکاران[2]، ۲۰۰۷) و مشارکت کارکنان در امنیت سازمان (کرامر و همکاران، ۲۰۰٦) بر سامانه‌های امنیت اطلاعات اثر می‌گذارد. در بررسی سامانه‌های اطلاعاتی توجه به هزینه و بودجه‌بندی برای سامانه‌های اطلاعاتی یکی از مهم‌ترین عواملی است که باید مدنظر

1. Knapp et al.
2. Ruighaver et al.

مدیران سازمان باشد (کرامر و همکاران، ۲۰۰۹).

مدل مفهومی عوامل مؤثر بر امنیت سامانه‌های اطلاعاتی

با توجه به گفته‌های ادبیات نظری و مفهوم امنیت سامانه‌های اطلاعاتی می‌توان ساختار سلسله مراتبی عوامل مؤثر بر امنیت سامانه‌های اطلاعاتی را به‌صورت شکل ۱ رسم کرد. در این مقاله سعی شده است اهمیت هر یک از ابعاد مدل مفهومی با توجه به متغیرهای مربوط، با استفاده از فرآیند تحلیل سلسله مراتبی فازی بررسی‌شده و وزن‌های هرکدام در پایان گزارش شود. در شکل ۱ ساختار سلسله مراتبی موردنظر به‌طور مختصر نشان داده‌شده است.



شکل ۱. شاخص‌های تأثیرگذار بر امنیت اطلاعات

هر یک از این شاخص‌ها دارای زیر شاخص‌هایی هستند که به دلیل تعداد زیاد آن‌ها وعدم توانایی نشان دادن آن‌ها در شکل ۱، در جدول ۱ به آن‌ها اشاره‌شده است.

جدول ۱. معرفی شاخص‌ها و زیر شاخص‌های مؤثر بر امنیت اطلاعات

شاخص	زیر شاخص	شاخص	زیر شاخص
سیاست امنیت اطلاعات سازمان	بودجه‌بندی سامانه‌های اطلاعاتی	نیروی انسانی	فراموش‌کاری کارکنان
	امنیت فیزیکی زیرساخت‌ها و اطلاعات		کوتاهی و بی‌مسئولیتی کارکنان
	تخطی و نقض امنیت اطلاعات		نداشتن انگیزه در انجام کار
	ممانعت از ورود ویروس‌ها و بدافزارها		عدم اطلاع از میزان ارزش اطلاعات
	رایانش موبایلی[1]		تداخل مسئولیت‌ها
	مدیریت دسترسی کاربر به سیستم اطلاعاتی		نداشتن مهارت کافی
	دسترسی به اینترنت		کار زیاد و خستگی ناشی از آن
سیاست امنیت اطلاعات سازمان	توسعه و نگهداری نرم‌افزارها و تجهیزات	فرهنگ امنیت اطلاعات سازمان	مشارکت کارکنان در امنیت اطلاعات
	رمزگذاری		مقاومت در مقابل تغییر
	شرایط و ضوابط استخدام		پشتیبانی مدیریت از طرح‌های امنیت اطلاعات
	برنامه‌ریزی مستمر سامانه‌های اطلاعاتی		جوابگویی و مسئولیت‌پذیری
	شرایط پاداش و تنبیه	سخت‌افزار	انبارش (فایل‌های کاغذی و...)
	استفاده شخصی از سامانه‌های اطلاعاتی		دستگاه‌های خروجی (پرینتر، پلاتر و...)
نرم‌افزار	اشتراک فایل‌ها		دستگاه‌های ورودی (اسکنر و...)
	سیستم‌عامل		کامپیوترها
	کرم‌های شبکه		وسایل ارتباطی (خط‌های تلفن، مودم و...)
	اسب‌های تراوا	حوادث غیرطبیعی	اختلالات برق و تلفن
	ویروس‌ها		ترکیدگی لوله آب
	نرم‌افزارهای جاسوسی		دما و رطوبت محیط
	گرفتن نسخه پشتیبان از اطلاعات		
فرآیندهای سازمانی	مدیریت ریسک پروژه‌های سیستم اطلاعاتی	ساختار امنیت اطلاعات سازمان	تعیین مسئولیت‌های مربوط به امنیت اطلاعات در سازمان
	مدیریت رویدادها		
	مدیریت اطلاعات		هماهنگی فعالیت‌های مربوط به امنیت اطلاعات
	مستندسازی فرآیندهای سازمانی		
	ممیزی سیستم مدیریت امنیت اطلاعات		سامانه‌های کنترل و نظارت بر امنیت سامانه‌های اطلاعاتی
	مدیریت تغییر		

1. Mobile Computing

امنیت سامانه‌های اطلاعاتی

با توجه به این‌که امروزه داده‌ها در قالب‌های الکترونیکی و رویه‌های غیر مشهود و خودکار جریان دارند (لادون و همکاران[1]، ۲۰۰۶) و نیز با توجه به رشد روزافزون استفاده از سامانه‌های اطلاعاتی، شرکت‌ها با مخاطرات فراوانی در استفاده از این سامانه‌ها روبرو هستند. امنیت اطلاعات را می‌توان حفاظت از سامانه‌های اطلاعاتی در مقابل خطرات و تهدیدهای موجود نامید. امنیت اطلاعات رشته‌ای تخصصی در حوزه علوم رایانه است که هدف آن تجزیه‌وتحلیل راهکارها و ارائه روش‌های مناسب جهت پاسخ به تهدیدهای سامانه‌های اطلاعاتی است (سعیدی و همکاران، ۱۳۸۶). در تعریف دیگری امنیت، علم مطالعه روش‌های حفاظت از دادها در رایانه‌ها و سامانه‌های ارتباطی در برابر دسترسی و تغییرات غیرمجاز معرفی‌شده است. از دیدگاه دیگر امنیت مجموعه‌ای از تدابیر، روش‌ها و ابزار برای جلوگیری از دسترسی غیرمجاز در سامانه‌های رایانه‌ای و ارتباطی تعریف گردیده است (جعفری و همکاران، ۱۳۸۶). بی شاپ امنیت رایانه را بر محرمانگی اطلاعات، جامعیت و دسترسی‌پذیری متکی می‌داند (اندرسون[2]،۲۰۰۳). جامعیت، بدین معنا که اطلاعات نمی‌توانند توسط افراد غیرمجاز ساخته، تغییر و یا حذف گردند. محرمانگی، یعنی اطمینان از این‌که اطلاعات تنها برای افراد مجاز قابل‌دسترسی است. دسترس‌پذیری، یعنی اطمینان از این‌که کاربران مجاز، به اطلاعات و دارایی‌های مرتبط در زمان نیاز دسترسی دارند (اندرسون،۲۰۰۳)(فارن و همکاران[3]،۲۰۰۴). درواقع هدف از ایمن‌سازی اطلاعات نیز تضمین جامعیت، محرمانگی و دسترس‌پذیر بودن آن است. می‌توان گفت، امنیت به سیاست‌ها، رویه‌ها و اشاره دارد که از دسترسی غیرمجاز، سرقت، تغییر دادها یا آسیب فیزیکی به سامانه‌های اطلاعاتی جلوگیری می‌کند.

---

1. Laudon et al.
2. Anderson
3. Farn et al.

ساختار امنیت اطلاعات سازمان

هر سازمان باید بداند که چه چیز را به چه دلایلی و در برابر چه خطراتی محافظت کند. سازمان‌ها در سطوح حساسیت متفاوتی از یکدیگر نسبت به اطلاعاتشان قرار دارند (جعفری و همکاران، ۱۳۸٦) و همین موضوع نشان‌دهنده‌ی ساختار سازمانی مناسب برای امنیت اطلاعات است و نسبت به حساسیت سازمان برای امنیت اطلاعات است که ساختار کنترلی فعالیت‌های سازمانی، هماهنگی این فعالیت‌ها و تعیین مسئولیت‌های سازمان شکل می‌گیرد.

سیاست‌های امنیتی سازمان

همان‌طور که اشاره شد امنیت یکی از اجزای اصلی زیرساخت‌های فناوری اطلاعات به شمار می‌رود. به همین دلیل برای پیاده‌سازی امنیت در سامانه‌های اطلاعاتی و شبکه‌ها، علاوه بر ایمن‌سازی سخت‌افزاری، نیاز به تدوین سیاست‌های امنیتی در حوزه فناوری اطلاعات و امنیت سامانه‌های اطلاعاتی در یک سازمان است. سیاست‌های امنیتی، استانداردها و سطوح امنیتی را تعیین می‌کند. درواقع سیاست امنیتی تعیین می‌کند که از جنبه امنیتی چه‌کارهایی مجاز و چه‌کارهایی غیرمجاز است (لادون و همکاران[1]، ۲۰۰٦)(پست و کاگان[2]، ۲۰۰۷). سیاست‌های امنیتی سازمان متناسب با نیازهای سازمان مخاطرات پیش رو را برآورد کرده و بر اساس آن طراحی و تدوین می‌گردد (سیپانن و همکاران[3]، ۲۰۰۹).

فرآیندهای سازمانی

در یک جمله یک فرآیند، مجموعه‌ای از فعالیت‌های مرتبط و ساختاریافته‌ای است که به

1. Laudon et al.
2. Post & Kagan
3. Siponen et al.

تولید محصول و یا ارائه خدماتی متناسب با نیاز مشتریان منجر می‌شود. فرآیند مجموعه فعالیت‌های متوالی و مرتبط بوده که محصول خاصی را به وجود می‌آورد و برای ایجاد این محصول به درون دادهای خاصی نیاز دارد که زمینه را برای درست عمل کردن به آن فراهم می‌سازند. هرکسی که حداقل دریکی از مراحل عملکرد فرآیند درگیر باشد، صاحب فرآیند محسوب می‌گردد. فرآیندهای موجود در هر سازمان برای دستیابی به مأموریت سازمان طراحی‌شده‌اند؛ تا با عملکرد بهتر نیازهای اساسی مردم را تأمین نمایند.

فرهنگ امنیت اطلاعات سازمان

در یک نگاه کلی امنیت اطلاعات شامل فرآیندهای مختلفی می‌شود که عملکرد صحیح بسیاری از آن‌ها تا حد زیادی به رفتارها و همکاری انسانی وابستگی دارد. کارکنان یک سازمان، چه به‌صورت عمد و یا به دلیل سهل‌انگاری ناشی از عدم آگاهی و دانش کافی، خود بزرگ‌ترین تهدید برای امنیت اطلاعات سازمان هستند به‌طوری‌که بسیاری از روش‌های و راه‌حل‌های امنیتی بدون مشارکت و همکاری کارکنان ثمربخش نبوده و به نتیجه نخواهند رسید. بر اساس پژوهش‌های انجام‌شده استقرار یک فرهنگ نهفته در سازمان برای امنیت اطلاعات به‌عنوان کلید مدیریت عامل‌های انسانی در بحث امنیت اطلاعات به‌طور گسترده‌ای پذیرفته‌شده است. با ایجاد این فرهنگ کارکنان بجای اینکه تهدید امنیتی در نظر گرفته شوند به‌عنوان یک دارایی امنیتی محسوب خواهند شد. البته حتی با ایجاد این فرهنگ‌سازمانی مزایا و معایب و تضاد منافع همچنان وجود خواهد داشت که این مسئله باید به‌طور جداگانه‌ای مدیریت و رسیدگی شود (ون نیکرک و ون سالمس[1]، ۲۰۱۰).

امنیت کارکنان

شامل شناسایی اطلاعات در حوزه‌های فردی و نحوه ایمن‌سازی آن‌ها، آموزش کارکنان، تدوین، پذیرش و امضاء توافقنامه‌های حفظ محرمانگی اطلاعات می‌شود. عدم ارائه

1. Van Niekerk & Von Solms

آموزش‌های مناسب و عدم آگاهی و روزآمدسازی اطلاعات توسط کاربران و گاه بی‌توجهی آن‌ها در کار موجب تحمیل هزینه‌های سنگین بر سازمان می‌شود؛ که با آموزش مناسب بخش مهمی از مسائل مربوط به کاربران اطلاعاتی حل خواهد شد. بی‌دقتی و بی‌توجهی کارمندان نسبت به مسائل امنیتی نیز گاه موجب بروز مشکلات می‌شود. نوع دیگر از خطراتی که توسط کاربران متوجه سازمان است شکل عمدی داشته و در این حالت سازمان باید با تعیین دقیق حدود اطلاعات و نیز دقت در انتخاب کاربران اطلاعاتی صدمات آن را تا حد امکان کاهش دهد. کارمندان خوب، وجود روابط مناسب و خوب در محیط کاری تا اندازه زیادی موجب کاهش این خطرات می‌شود (پیپکین[1]، ۲۰۰۰).

نرم‌افزار

نرم‌افزار، مجموعه از دستورالعمل‌های دقیق و مرحله‌به‌مرحله است که هدف خاصی را دنبال می‌کند. ظاهراً، اولین بار جان تاکی در سال ۱۹۵۸ این واژه را به این معنا به‌کاربرده است. احتمالاً این واژه در مقابل سخت‌افزار به‌کاربرده‌اند که بسیار پیش از پیدایش رایانه (به معنای اسباب و اشیاء) به کار می‌رفته است.

سخت‌افزار

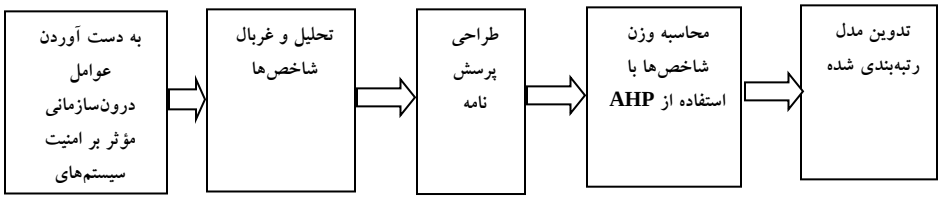
سخت‌افزار بخش مادی، قابل‌لمس و ابزاری هر مجموعه یا سیستم است.

روش‌شناسی پژوهش

روش تحقیق این پژوهش از نوع کاربردی است. در این پژوهش برای رتبه‌بندی عوامل درون‌سازمانی تأثیرگذار بر امنیت سامانه‌های اطلاعاتی، ابتدا مطالعات گسترده‌ای روی

1. Pipkin

مدل‌های موجود در این حوزه انجام شد که هرکدام دریک حوزه ویژه مانند امنیت فیزیکی و امنیت کارکنان، این موضوع را بررسی کرده بودند؛ در پایان با بررسی این مدل‌ها و با کمک خبرگان و صاحب‌نظران این حوزه، مجموعه‌ای از شاخص‌ها استخراج و بسیاری از شاخص‌ها باهم تجمیع شدند و درنهایت پرسشنامه‌ی مرتبط با شاخص‌های استخراج‌شده تهیه شد. پرسشنامه‌ها توسط خبرگان دانشگاهی و متخصصان سازمان‌های دولتی شهر بوشهر پاسخ داده شدند. میانگین این پرسشنامه‌ها، محاسبه و با گرد کردن این اعداد به نزدیک‌ترین مقدار زبان‌شناسی، داده‌های ورودی را برای تجزیه‌وتحلیلAHP فازی تشکیل داده‌شده است (ازآنجاکه در این بررسی، ارزیابی با شاخص‌های چندگانه و کیفی و به‌صورت گام‌به‌گام صورت می‌گیرد،AHP روش مناسبی برای این منظور است و ازآنجایی‌که غالباً افراد ترجیحات و نظرات خود را به‌صورت اصطلاحات زبانی به‌جای مقادیر عددی بیان می‌کنند؛ ازاین‌رو در اولویت‌بندی عوامل از یک چارچوب AHP فازی استفاده‌شده است). این مراحل در نمودار شماره (۲) نشان داده‌شده است.



نمودار۲. روش پژوهش

بر اساس نمودار ۲ در گام اول تعدادی از مقالاتی که به‌نوعی با امنیت سامانه‌های اطلاعاتی مربوط بودند بررسی و یک سری از عوامل درون‌سازمانی مؤثر بر امنیت سامانه‌های اطلاعاتی، استخراج‌شده است؛ بسیاری از شاخص‌ها باهم ادغام شدند و برخی از شاخص‌ها زیرمجموعه‌ی دیگر شاخص‌ها قرار گرفتند. در گام بعد پرسشنامه مقایسات زوجی برای شاخص‌های غربال‌شده تهیه گردیده و در اختیار پاسخ‌دهندگان قرارگرفته است. ازآنجاکه در این تصمیم‌گیری ممکن است تصمیم‌گیرنده با معیارهای مختلفی مواجه شود، در چنین شرایطی باید از روش‌های مطرح در این زمینه بهره جوید. یکی از

این روش‌ها فرآیند تحلیل سلسله مراتبی است. روش تحلیل سلسله مراتبی یکی از معروف‌ترین فنون تصمیم‌گیری چندمنظوره است که در سال ۱۹۸۰ توسط توماس ساعتی ابداع شد. این روش هنگامی‌که عمل تصمیم‌گیری با چند گزینه رقیب و معیار تصمیم‌گیری روبه‌رو است می‌تواند استفاده شود. فرآیند تحلیل سلسله مراتبی ترکیب معیارهای کیفی همراه با معیارهای کمی را به‌طور هم‌زمان امکان‌پذیر می‌سازد .اساس روش تحلیل سلسله مراتبی بر مقایسه زوجی یا دودویی گزینه‌ها و معیارهای تصمیم‌گیری است .برای چنین مقایسه‌ای نیاز به جمع‌آوری اطلاعات از تصمیم‌گیرندگان است و این امر به تصمیم‌گیرندگان این امکان را می‌دهد تا فارغ از هرگونه نفوذ و مزاحمت خارجی تنها روی مقایسه دو معیار یا گزینه تمرکز کنند. افزون بر مقایسه دودویی، به دلیل اینکه پاسخ‌دهنده تنها دو عامل را نسبت به هم می‌سنجد و به عوامل دیگر توجه ندارد، اطلاعات ارزشمندی را برای مسئله موردبررسی فراهم می‌آورد و فرآیند تصمیم‌گیری را منطقی می‌سازد؛ کیفیت تصمیم‌گیری با تجزیه‌وتحلیل نظرات مختلف مورداستفاده قرار می‌گیرد (ساعتی[1]، ۱۹۸۹).

تئوری مجموعه‌های فازی که نخستین بار پرفسور لطفی زاده آن را ارائه کرد، در حل مسائلی که نمی‌توان پارامترها و کمیت‌ها را به‌طور دقیق بیان کرد، استفاده شد. فازی بودن به انواع مختلف ابهام و عدم اطمینان و به‌خصوص به ابهامات مربوط به بیان زبانی و طرز فکر بشری بستگی دارد و با عدم اطمینانی که به‌وسیله نظریه احتمال بیان می‌شود، فرق دارد. رویکرد فازی ابزار بسیار مناسبی برای برخورد و کنار آمدن با عدم اطمینان و مدل‌سازی متغیرهای زبانی است. منطق فازی هدفش این است که اساسی را برای استدلال گری تقریبی با استفاده از تئوری مجموعه فازی فراهم آورد. با توجه به اینکه تصمیم‌گیری انسان با مفاهیم نادقیق و مبهم همراه است، این مفاهیم بیشتر به‌صورت متغیرهای زبانی بیان می‌شوند. بر اساس منطق فازی این عناصر نادقیق عوامل مهمی در هوشمندی انسان به

1. Saaty

شمار می‌روند (وانگ و بای[1]، ۲۰۰۲).

در این پژوهش از دیدگاه FAHP مطابق با روش تجزیه‌وتحلیل توسعه‌ای چانگ[2] برای ارائه‌ی قضاوت‌های تصمیم‌گیرندگان استفاده می‌شود تا عوامل درون‌سازمانی مؤثر بر امنیت سامانه‌های اطلاعاتی را اولویت‌بندی کنیم. در این بررسی، مقایسات تصمیم‌گیرنده با واژه‌های زبان‌شناسی توصیف‌شده است و با اعداد فازی بیان می‌شود.

پرسشنامه‌ها توسط خبرگان دانشگاهی و متخصصان سازمان‌های دولتی شهر بوشهر پاسخ‌داده‌شده است. میانگین این پرسش‌ها، محاسبه و با گرد کردن این اعداد به نزدیک‌ترین مقدار زبان‌شناسی، داده‌های ورودی را برای تجزیه‌وتحلیل AHP فازی تشکیل دادیم.

در ادامه خلاصه‌ی روش تحلیل توسعه‌ای چانگ ارائه می‌شود که منطبق بر اصول فازی به کمک فرایند تحلیل سلسله مراتبی است. مراحل اجرای روش به‌صورت زیر است:

مرحله‌ی ۱: ترسیم درخت سلسله مراتبی: ابتدا ساختار سلسله مراتبی تصمیم با استفاده از سطوح هدف، معیار و زیر معیار تشکیل داده می‌شود.

مرحله‌ی ۲: تشکیل ماتریس مقایسات زوجی: ماتریس‌های توافقی را مطابق با درخت تصمیم و با استفاده از نظرات خبرگان تشکیل داده، نرخ ناسازگاری آن‌ها حساب می‌شود (در این مقاله نرخ ناسازگاری پرسشنامه‌ها با نرم‌افزار Expert choice محاسبه شد و چون از ۰/۱ کمتر است، می‌توان گفت ماتریس مقایسات از سازگاری برخوردار است).

مرحله‌ی ۳: میانگین حسابی نظرات: میانگین حسابی نظرات تصمیم‌گیرندگان را محاسبه کرده تا ماتریس زیر حاصل شود.

---

1. Kwong & Bai
2. Chang

$$\tilde{A}=\begin{bmatrix} 1 & \tilde{M}_{12} & \dots & \tilde{M}_{1n} \\ \tilde{M}_{21} & 1 & \dots & \tilde{M}_{2n} \\ . & . & . & . \\ . & . & . & . \\ \tilde{M}_{n1} & \tilde{M}_{n2} & \dots & 1 \end{bmatrix}$$

میانگین حسابی نظرات تصمیم‌گیرندگان از رابطه‌ی (۲) به دست می‌آید.

رابطه (۱) $SUM=\sum_1^N A_{ij} i,j=1,2,...,n \qquad Mean=SUM/n$

سپس با استفاده از اعداد مثلثی فازی حد بالا و پایین هر ستون ماتریس و معکوس آن را دست می‌آوریم. فرض کنید $\widetilde{A_{IJ}}=\{\tilde{M}_{ij}\}$ یک ماتریس میانگین مقایسه زوجی فازی باشد که به‌صورت بالا تعریف می‌شود. آنگاه رابطه‌ی (۲) برقرار خواهد بود.

رابطه (۲) $\tilde{M}_{IJ}=1/\tilde{M}_{ij}$

مرحله‌ی ٤: استفاده از روش تحلیل توسعه‌ای[1] (EA)برای بی مقیاس کردن:

درروش تحلیل توسعه‌ای برای هر یک از سطرهای ماتریس زوجی، ارزش S_K که خود یک عدد فازی مثلثی است و به‌صورت رابطه‌ی ۳ محاسبه می‌گردد.

رابطه (۳) $S_K=\sum_{j=1}^{n} M_{ij}\otimes[\sum_{i=1}^{m}\sum_{j=1}^{n} M_{ij}]^{-1}$

که در آن k بیانگر شماره‌ی سطر و i و j به ترتیب نشان‌دهنده گزینه‌ها و شاخص می‌باشند.

مرحله‌ی (۵): در این روش پس از محاسبه‌ی S_K ها باید درجه بزرگی آن‌ها نسبت به هم را به دست آورد. به‌طورکلی اگرM_1 و M_2 دو عدد فازی مثلثی باشند، درجه بزرگی M_1 بر M_2 به‌وسیله‌ی رابطه‌ی ٤ و جدول ۱ (هاست و همکاران[2]، ۲۰۰٤) به دست می‌آید.

اگر$M_1 \geq M_2$ باشد داریم:

رابطه (٤)
$$\begin{cases} V(M_1 \geq M_2)=1 \\ V(M_1 < M_2)=hgt(M_1 \cap M_2) \end{cases}$$

1. Extent Analysis Methods
2. Host et al.

جدول ۲: تابع عضویت متغیرهای زبانی تعیین وزن معیارها (چانگ[1]، ۱۹۹۲)

ارجحیت سطر به ستون			ارجحیت ستون به سطر		
متغیر زبانی	عدد فازی معادل		متغیر زبانی	عدد فازی معادل	
اهمیت یکسان	۱	۱	اهمیت یکسان	۱	۱
یکسان تا نسبتاً مهم‌تر	۲/٦۷	۱/۳۳	یکسان تا نسبتاً مهم‌تر	۰/۷۵	۰/۵	۰/۳۷
نسبتاً مهم‌تر	۳/٦۷	۲/۳۳	نسبتاً مهم‌تر	۰/٤۳	۰/۳۳	۰/۲۷
نسبتاً تا بسیار مهم‌تر	٤/٦۷	۳/۳۳	نسبتاً تا بسیار مهم‌تر	۰/.۳۰	۰/۲۵	۰/۲۱
بسیار مهم‌تر	۵/٦۷	٤/۳۳	بسیار مهم‌تر	۰/۲۳	۰/۲۰	۰/۱۸

در غیر این صورت داریم:

رابطه (۵)
$$hgt(M_1 \cap M_2) = \frac{U_1 - L_2}{(U_1 - L_2) + (m_2 - m_1)}$$

میزان بزرگی (v) یک عدد فازی مثلثی از k عدد فازی مثلثی دیگر نیز از رابطه (٦) به دست می‌آید:

رابطه (٦)
$$V(M_1 \geq M_2, ..., M_k) = Min[V(M_1 \geq M_2), ..., V(M_1 \geq M_k)]$$

مرحله‌ی ٦ محاسبه وزن شاخص‌ها به‌صورت بی مقیاس شده: برای محاسبه‌ی وزن شاخص‌ها در ماتریس مقایسات زوجی از رابطه (۷) می‌کنیم:

رابطه (۷)
$$w'(x_i) = \min\{V(S_i \geq S_k)\} \qquad k = 1, 2, 3, ..., n, k \neq i$$

بنابراین بردار وزن شاخص‌ها که همان بردار ضرایب غیر بهنجار است طبق رابطه (۸) خواهد بود:

رابطه (۸)
$$w' = [w'(x_1), w'(x_2), ..., w'(x_n)]^t$$

سپس برای به دست آوردن بردار هنجار نیز طبق رابطه‌ی (۹) عمل می‌کنیم:

رابطه (۹)
$$w(x_k) = \frac{w'(x_k)}{\sum_{k=1}^{n} w'(x_k)}$$

1. Chang

این مراحل برای تمام جداول انجام‌شده است تا وزن‌های به هنجار شده آن‌ها نیز به دست آید (آذر و همکاران، ۱۳۸۹).

جمع‌آوری و تجزیه‌وتحلیل داده‌ها

بر اساس مفهوم امنیت سامانه‌های اطلاعاتی و مروری بر ادبیات مربوط، یک نمودار سلسله مراتبی امنیت سیستم اطلاعاتی طبق شکل ۳ به‌دست‌آمده است. پرسش‌نامه‌ای با فرمت مرسوم AHP (مقایسه زوجی) بر اساس سلسله‌مراتب مذکور تهیه گردید. ۱۵ پرسش‌نامه بین نخبگان دانشگاهی و متخصصان سازمان‌های دولتی شهر بوشهر توزیع شد که نرخ بازگشت پرسش‌نامه ۱۰ عدد بوده است. داده‌هایی که از ۱۰ پرسش‌نامه جمع‌آوری‌شده است، پس از محاسبات مربوط به فرآیند سلسله مراتبی فازی (FAHP) به‌صورت جداول زیر نشان داده‌شده است.

جدول ۳. وزن زیر معیارهای مربوط به معیار سیاست امنیت اطلاعات سازمان

ردیف	زیر شاخص	وزن
۱	بودجه‌بندی سامانه‌های اطلاعاتی	۰/۱۹۸
۲	امنیت فیزیکی زیرساخت‌ها و اطلاعات	۰/۱۶۹
۳	ممانعت از ورود ویروس‌ها و بدافزارها	۰/۱۲۸
٤	برنامه‌ریزی مستمر در مورد امنیت سامانه‌های اطلاعاتی	۰/۱۲۷
٥	تخطی و نقض امنیت اطلاعات	۰/۱۲۰
٦	مدیریت دسترسی کاربر به سیستم اطلاعاتی	۰/۱۱۳
۷	توسعه و نگهداری نرم‌افزارها و تجهیزات	۰/۰٦٤
۸	رایانش موبایلی	۰/۰۳۰
۹	دسترسی به اینترنت	۰/۰۲۲
۱۰	شرایط پاداش و تنبیه	۰/۰۱٤
۱۱	رمزگذاری	۰/۰۰۹
۱۲	شرایط و ضوابط استخدام	۰/۰۰٥
۱۳	استفاده شخصی از سامانه‌های اطلاعاتی	۰/۰۰۳

جدول ۳ نشان‌دهنده وزن زیر معیارهای مربوط به معیار سیاست امنیت اطلاعات سازمان است. همان‌طور که ملاحظه می‌شود، زیر شاخص بودجه‌بندی سامانه‌های اطلاعاتی مهم‌ترین زیر شاخص شناخته‌شده است.

جدول ٤. وزن زیر معیارهای مربوط به معیار نرم‌افزار

ردیف	زیر شاخص	وزن
۱	ویروس‌ها	۰/۳۲٤
۲	نرم‌افزارهای جاسوسی	۰/۲۷۹
۳	کرم‌های شبکه	۰/۱٦۹
٤	اسب‌های تراوا	۰/۱۲٥
٥	سیستم‌عامل	۰/۰٦۲
٦	اشتراک‌گذاری فایل‌ها	۰/۰۲٤
۷	گرفتن نسخه پشتیبان از اطلاعات	۰/۰۱٦

جدول ٥. وزن زیر معیارهای مربوط به معیار نیروی انسانی

ردیف	زیر شاخص	وزن
۱	عدم اطلاع از میزان ارزش اطلاعات	**۰/۲٦۸**
۲	نداشتن مهارت کافی	**۰/۲٦٦**
۳	کوتاهی و بی‌مسئولیتی کارکنان	**۰/۲۱۲**
٤	کار زیاد و خستگی ناشی از آن	**۰/۱۲۳**
٥	نداشتن انگیزه در انجام کار	**۰/۱۱٤**
٦	تداخل مسئولیت‌ها	**۰/۰۱٦**
۷	فراموش‌کاری کارکنان	**۰/۰۰۲**

جدول ٤ و ٥ به ترتیب نشان‌دهنده وزن زیر معیارهای مربوط به شاخص‌های نرم‌افزار و نیروی انسانی است. همان‌طور که ملاحظه می‌شود در شاخص نرم‌افزار زیر شاخص ویروس‌ها بیش‌ترین اهمیت رادارند و برای حفظ امنیت سامانه‌های اطلاعاتی باید توجه

زیادی به آن شود. بعلاوه در شاخص نیروی انسانی، زیر شاخص عدم اطلاع از میزان ارزش اطلاعات دارای بیش‌ترین اهمیت است.

جدول ٦: وزن زیر معیارهای مربوط به معیار فرآیندهای سازمانی

ردیف	زیر شاخص	وزن
۱	ممیزی سیستم مدیریت امنیت اطلاعات	۰/۳۳۱
۲	مدیریت اطلاعات	۰/۲۹۲
۳	مستندسازی فرآیندهای سازمانی	۰/۲٤۸
٤	مدیریت ریسک پروژه‌های سیستم اطلاعاتی	۰/۰٦٤
٥	مدیریت رویدادها	۰/۰۳۸
٦	مدیریت تغییر	۰/۰۲۷

جدول ٦ نشان‌دهنده وزن زیر معیارهای مربوط به معیار فرآیندهای سازمانی است. همان‌طوری که مشخص است، زیر معیار ممیزی سیستم مدیریت امنیت اطلاعات با وزنی برابر با ۰/۳۳۱ دارای بیش‌ترین اهمیت است.

جدول ۷: وزن زیر معیارهای مربوط به فرهنگ امنیت اطلاعات سازمان

ردیف	زیر شاخص	وزن
۱	جوابگویی و مسئولیت‌پذیری کارکنان و مدیران	۰/٥۷٥
۲	پشتیبانی مدیریت ارشد از طرح‌های امنیت اطلاعات	۰/۳۱٤
۳	مقاومت کارکنان و مدیران در مقابل تغییر	۰/۰۹۷
٤	مشارکت کارکنان در امنیت اطلاعات سازمان	۰/۰۱٤

جدول ۷ نشان‌دهنده وزن زیر معیارهای مربوط به معیار فرهنگ امنیت اطلاعات سازمان است. همان‌طور که مشخص است زیر معیار جوابگویی و مسئولیت‌پذیری کارکنان و مدیران سازمان با وزنی برابر ۰/٥۷٥ دارای بیش‌ترین اهمیت در فرهنگ امنیت اطلاعات سازمان است. به‌عبارت‌دیگر برای حفظ امنیت سازمان باید کارکنان و مدیران سازمان

حس مسئولیت‌پذیری و جوابگویی بالایی نسبت به کاری که انجام می‌دهند داشته باشند.

جدول ۸. وزن‌های زیر معیارهای مربوط به ساختار امنیت اطلاعات سازمان

ردیف	زیر شاخص	وزن
۱	سامانه‌های کنترل و نظارت بر امنیت سامانه‌های اطلاعاتی	۰/۷۷۸
۲	هماهنگی فعالیت‌های مربوط به امنیت اطلاعات	۰/۱٤٦
۳	تعیین مسئولیت‌های مربوط به امنیت اطلاعات در سازمان	۰/۰۷٦

جدول ۸ نشان‌دهنده وزن زیر معیارهای مربوط به معیار ساختار امنیت اطلاعات سازمان است. همان‌طور که در جدول مشخص است، زیر معیار سامانه‌های کنترل و نظارت بر امنیت سامانه‌های اطلاعاتی مهم‌ترین زیر معیار با وزن ۰/۷۷۸ است که نشان می‌دهد سازمان برای حفظ و افزایش امنیت اطلاعات سازمان نیاز به داشتن سامانه‌های کنترل و نظارت بر عملکرد سامانه‌های اطلاعاتی دارد.

جدول ۹. وزن زیر معیارهای مربوط به معیار سخت‌افزار

ردیف	زیر شاخص	وزن
۱	وسایل ارتباطی (خط‌های تلفن، مودم و...)	۰/٤۷۹
۲	کامپیوترها	۰/۳۵۰
۳	دستگاه‌های ورودی (اسکنر و...)	۰/۰٥٤
٤	دستگاه‌های خروجی (پرینتر، پلاتر و...)	۰/۰٥۹
٥	انبارش (فایل‌های کاغذی و...)	۰/۰٥۸

جدول ۹ نشان‌دهنده وزن زیر معیارهای مربوط به معیارهای سخت‌افزار است. همان‌طور که مشخص است، زیر معیار وسایل ارتباطی با وزن ۰/٤۷۹ دارای بیش‌ترین اهمیت است. به‌عبارت‌دیگر خلل و نقصی در وسایل ارتباطی می‌تواند باعث بروز آسیب‌های جبران‌ناپذیری به امنیت سامانه‌های اطلاعاتی سازمان شود.

جدول ۱۰. وزن زیر معیارهای مربوط به معیار حوادث غیرطبیعی

ردیف	زیر شاخص	وزن
۱	اختلالات برق و تلفن	۰/۵۹۰
۲	دما و رطوبت محیط	۰/۲۱۳
۳	ترکیدگی لوله آب	۰/۱۹۶

جدول ۱۰ نشان‌دهنده وزن زیر معیارهای مربوط به حوادث غیرطبیعی است. همان‌طور که مشخص است، اختلالات برق و تلفن با وزنی برابر ۰/۵۹۰ دارای بیش‌ترین اهمیت در حوادث غیرطبیعی است.

جدول ۱۱. وزن معیارهای مؤثر بر امنیت سامانه‌های اطلاعاتی

ردیف	معیارهای تأثیرگذار بر امنیت سامانه‌های اطلاعاتی	وزن
۱	نیروی انسانی	۰/۲۹۲
۲	سیاست امنیت اطلاعات سازمان	۰/۲۵۳
۳	ساختار امنیت اطلاعات سازمان	۰/۱۸۲
٤	نرم‌افزار	۰/۱۱۱
٥	سخت‌افزار	۰/۰٦۲
٦	فرهنگ امنیت اطلاعات سازمان	۰/۰٤۷
۷	فرآیندهای سازمانی	۰/۰٤۱
۸	حوادث غیرطبیعی	۰/۰۱۱

همان‌طور که در جدول ۱۱ مشخص است، نیروی انسانی با وزنی برابر ۰/۲۹۲ بااهمیت‌ترین معیار امنیت سامانه‌های اطلاعاتی است. این جدول نشان می‌دهد که متخصصان و مدیران سازمان و کسانی که به‌گونه‌ای با سامانه‌های اطلاعاتی در ارتباط‌اند و امنیت این سامانه‌ها برای آن‌ها موردتوجه است، باید به انسان که همان کاربران سیستم هستند بیش‌ترین توجه را بکنند تا بتوانند امنیت سیستم سازمان خود را حفظ کرده و حتی آن را افزایش بدهند.

بحث و نتیجه‌گیری

هر سازمان باید ارزش اطلاعات خود را ارزیابی کند و سپس خط‌مشی امنیتی برای مواردی که باید مورد محافظت قرار گیرد، مشخص نماید. سیستم امنیت اطلاعات شاید پرهزینه و وقت‌گیر به نظر آید اما با توجه به اهمیت اطلاعات در بقای سازمان، وجود چنین سامانه‌ای بسیار ضروری است. از روی دیگر، افزایش روزافزون اهمیت موضوع امنیت در سامانه‌های اطلاعاتی، سازمان‌ها را ملزم به سرمایه‌گذاری و توجه ویژه به آن کرده است. در این پژوهش سعی شده است بامطالعه ادبیات نظری و شناسایی عوامل درون‌سازمانی مؤثر بر امنیت سامانه‌های اطلاعاتی و پس‌ازآن استفاده از روش تحلیل سلسله مراتبی فازی به‌عنوان روشی برای رتبه‌بندی این عوامل، چارچوبی روشن برای اولویت‌بندی عوامل درون‌سازمانی مؤثر بر امنیت سامانه‌های اطلاعاتی معرفی کرد. نتایج این پژوهش نشان می‌دهد که عامل نیروی انسانی مهم‌ترین عامل تأثیرگذار بر امنیت سامانه‌های اطلاعاتی و زیر شاخص عدم آگاهی از میزان ارزش اطلاعات مهم‌ترین زیر شاخص مربوط به نیروی انسانی است. اگر نتایج این پژوهش را با نتایج مطالعاتی که در پیشینه‌ی پژوهش نیز به آن اشاره شد مقایسه کنید، خواهید دید عامل انسانی و خطاهایی که از آن سر میزند مهم‌ترین چالش برای امنیت سامانه‌های اطلاعاتی است که این امر نیز بیشتر به خاطر عدم آگاهی نیروی انسانی از ارزش اطلاعات و یا چگونگی حفظ و محافظت از اطلاعات باارزش است. با توجه به این‌که دغدغه اصلی کارکنان برآورده ساختن درخواست‌ها و انجام وظایفی است که بر عهده آنان است اولین چیزی که معمولاً نادیده گرفته می‌شود مسائل امنیتی است. دلیل عمده آن را می‌توان نداشتن قانون مدون و ابلاغ‌شده به کارکنان دانست. نکته بسیار مهم این است که نداشتن مقررات مکتوب باعث می‌شود اولاً کارکنان ندانند چه وظایفی نسبت به حفظ اطلاعات در سازمان دارند و ثانیاً در صورت بروز تخلف آن‌ها، مرجعی برای رسیدگی به تخلفات وجود ندارد. پس می‌توان به مدیران و تصمیم‌گیرندگان سازمان‌ها پیشنهاد داد در بحث امنیت سامانه‌های اطلاعاتی، بیش‌ترین تمرکز خود را بر نیروی انسانی و آموزش آن‌ها

قرار دهد تا بتواند امنیت سیستم اطلاعاتی سازمان خود را حفظ و ارتقا دهد. بعلاوه نباید از شاخص‌های دیگر مانند سیاست امنیت اطلاعات که وزنی نزدیک به نیروی انسانی دارد غافل شد که عدم توجه به این شاخص‌ها به‌نوبه خود می‌تواند آسیب‌های جبران‌ناپذیری به سیستم اطلاعاتی سازمان بزند.

در انتهای این پژوهش برای مطالعات آتی می‌توان مطالعه‌ی عوامل بیرون سازمانی مؤثر بر امنیت سامانه‌های اطلاعاتی مانند خطرات هکرهای خارجی و یا حوادث طبیعی و غیره را با روش‌های دیگر تصمیم‌گیری و یا آماری را پیشنهاد داد.

منابع

آذر، ع. علی، ر. (۱۳۸۹). تصمیم‌گیری کاربردی رویکرد MADM. تهران: **نگاه دانش**.

الهی، ش. طاهری، م. حسن‌زاده، ع. ارائه چارچوبی برای عوامل انسانی مرتبط در امنیت سیستم‌های اطلاعاتی. **فصلنامه مدرس علوم انسانی** دوره ۱۳، شماره ۲، تابستان ۱۳۸۸.

اسعدی شالی، ع. (۱۳۸٤). **مدیریت سیستم‌های امنیت اطلاعات**. (جلد شماره ٤). مجله الکترونیکی مرکز اطلاعات و مدارک علمی ایران.

جدّی، م. مدیری، ن. جنگجو، م. (۱۳۹۰). مدلی برای افزایش ضریب امنیت در سیستم مدیریت امنیت اطلاعات بر پایه مدیریت ریسک با استفاده از چرخه مدیریتی دمینگ. **سومین کنفرانس مهندسی برق و الکترونیک ایران**. دانشگاه آزاد اسلامی گناباد.

مانیان، ا. موسی خانی، م. رحیمیان، س. (۱۳۹۳). ارائه‌ی مدل عوامل مؤثر بر رضایت کاربران سامانه جامع آموزش دانشگاه تهران. **فصلنامه مطالعات مدیریت فناوری اطلاعات** سال دوم، شماره ۸، تابستان ۹۳، صفحات ۱۲۳ تا ۱۳۸.

محمود زاده، ا. رادرجبی، م. (۱۳۸۵). مدیریت امنیت در سیستم‌های اطلاعاتی. **فصلنامه علوم مدیریت ایران**، ص ۱۱۲-۷۸.

مؤسسه‌ی استاندارد و تحقیقات صنعتی ایران، فناوری اطلاعات-فنون امنیتی-سیستم‌های مدیریت امنیت اطلاعات ـ الزامات (چاپ اول).

قاسمی شبانکاره، ک. مختاری و. امینی لاری، م. (۱۳۸٦). امنیت و تجارت الکترونیک. **چهارمین همایش ملی تجارت الکترونیکی**.

سعیدی، ع. آقایی، آ. (۱۳۸٦). امنیت سیستم‌های اطلاعاتی حسابداری. **ماهنامه حسابدار**، ۱۳-۲۰.

جعفری، ن. صادقی مجرد، م. (۱۳۸٦). سیستم مدیریت امنیت اطلاعات از طرح تا اصلاح. **ماهنامه تدبیر**.

Bojanc, R. & Jerman-Blazic, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*.

Clinch, J. (2009). ITIL V3 and Information Security. *Best Management practice*.

Chang, D.Y. (1992). Extent Analysis and Synthetic Decision, Optimization Techniques and Applications.*WorldScientific, Singapore*.

Doherty, N. & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *computers & security*.

Dzazali, S. Sulaiman, A. & Zolait, A. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. *Government Information Quarterly*, 26.

Farn, K.J. Lin, S.K. & Lo, C.C. (2008). A study on e-Taiwan information system security classification and implementation. *Computer Standards & Interfaces*.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information& Management*, 51 (1): 69–79.

Kim, H.b. Lee, D.S. & Ham, S. (2012). Impact of hotel information security on system reliability. *International Journal of Hospitality Management*.

Knapp, K. Rainer, R. Ford, F. & Marshall, T. (2006). Information security:management's effect on culture and policy. *Information Management & Computer Security*.

Kraemer, S. Carayon, C. & Clem, J. (2006). Characterizing violations in computer and information security systems In: Proceedings. *Maastricht, The Netherlands*.

Kraemer, S. Carayon, P. & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *computers & security*.

Kwong, c &. Bai, H. (2002). fuzzy AHP approach to the determination of importance weights of customer requirements in quality function deployment. *Journal of Intelligent Manufacturing*.367-377.

Laudon, J. Laudon, C. K. & Laudon, p. J. (2006). *Management Information Systems*: Managing the Digital Firm.

Pipkin, D. L. (2000) .Information security. *Prentice Hall.*

Post, V. G. & Kagan, A. (2007). Evaluating information security tradeoffs:Restricting access can interfere with user tasks. *computer & security*, 229-237.

Ren-Wei Fung, A. Farn, K.J. & C. Lin, A. (2003). Paper: a study on the certification of the information security management systems. *Computer Standards & Interfaces*.

Ruighaver, A. Maynard, S. & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *computers & security*.

Siponen, M. & Willison, R. (2009). Information security management standards:Problems and Solutions. *Information & Management*, 267-270.

Stanton, J. Stam, K. Mastrangelo, P. & Jeffery, J. (2005). Analysis of end

user security behaviors. *Computers & Security*.

Van Niekerk, J & Von Solms, R (2010). Information security culture: A management perspective. *Computers & Security*.486-476, (4)29.

Wei, L. Yong-feng, C. Ya, L. (2015). Information systems security assessment based system dynamics. *International Journal of Security and Its Applications*. Vol.9, No.2, pp.73-84