

سورة الاحقاف

وزارت علوم، تحقیقات و فناوری



دانشگاه علم و هنر
وابسته به جهاد دانشگاهی

پایان نامه کارشناسی ارشد دانشکده علوم انسانی

گروه مدیریت صنعتی

عنوان:

شناسایی و اولویت بندی عوامل انسانی موثر بر
امنیت اطلاعات با استفاده از رویکرد ترکیبی ANP
و DEMATEL فازی

استاد راهنما :

دکتر سید محمود زنجیرچی


استاد مشاور:

دکتر سید حبیب الله میرغفوری

تحقیق و نگارش :

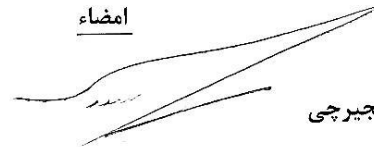


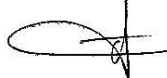
محبوبه باغبانزاده

آبان ۱۳۹۳

شماره فرم: ۹ شماره: ۹۳/۲۲۷/م تاریخ: ۹۳/۰۸/۲۸ پیوست:	صور تجلسه دفاعیه پایان نامه دانشجوی دوره کارشناسی ارشد (ویرایش مهر ۱۳۹۲)	 وزارت علوم، تحقیقات و فناوری دانشگاه علامه و هنر وابسته به جهاد دانشگاهی مدیریت تحصیلات تکمیلی
--	--	--

جلسه دفاعیه پایان نامه تحصیلی خانم محبوبه باغبانزاده دانشجوی کارشناسی ارشد رشته مدیریت صنعتی- تولید به شماره دانشجویی ۹۰۱۲۵۴۰۰۵ تحت عنوان "شناسایی و اولویت بندی عوامل انسانی موثر بر امنیت اطلاعات با استفاده از رویکرد تلفیقی ANP و Dematel فازی" و تعداد واحد ۴ در تاریخ ۹۳/۰۸/۲۹ با حضور اعضای هیات داوران (به شرح ذیل) تشکیل گردید.

پس از ارزیابی توسط هیات داوران، پایان نامه با نمره: به عدد ۱۷/۷۵... به حروف هجدهم، صد و هفتاد و پنج و درجه و درجه هجدهم... مورد تصویب قرار گرفت.

امضاء	نام و نام خانوادگی	عنوان
	آقای دکتر سید محمود زنجیرچی	استاد راهنما:
	آقای دکتر سید حبیب ا... میرغفوری	استاد مشاور:
	آقای دکتر مسعود احمدخانی	متخصص و صاحب نظر داخلی:
	آقای دکتر علی مروتی شریف آبادی	متخصص و صاحب نظر خارجی:

نام و نام خانوادگی نماینده تحصیلات تکمیلی دانشگاه (ناظر): آقای دکتر مسعود احمدخانی

امضاء: 

تعهدنامه

اینجانب محمد باغیان دانشجوی دوره دکتری کارشناسی ارشد رشته صنایع دستی دانشگاه صنعتی دانشگاه علم و هنر تحت راهنمایی دکتر محمد باغیان متعهد می‌شوم:

- نتایج ارائه شده در این پایان نامه حاصل مطالعات علمی و عملی اینجانب بوده و مسئولیت صحت و اصالت مطالب مندرج را به طور کامل بر عهده می‌گیرم.
- در خصوص استفاده از نتایج پژوهش‌های محققان دیگر به مرجع مورد نظر استناد شده است.
- مطالب مندرج در این پایان نامه را اینجانب یا فرد دیگری به منظور اخذ هیچ نوع مدرک یا امتیازی تاکنون به هیچ مرجعی تسلیم نکرده است.
- کلیه حقوق معنوی این اثر به دانشگاه علم و هنر تعلق دارد. مقالات مستخرج از پایان نامه، ذیل نام دانشگاه علم و هنر (Science and Art University) به چاپ خواهد رسید.
- حقوق معنوی تمام افرادی که در به دست آمدن نتایج اصلی پایان نامه تأثیرگذار بوده‌اند در مقالات مستخرج از رساله، رعایت خواهد شد.

نام و امضا دانشجو محمد باغیان

تاریخ

مالکیت نتایج و حق نشر

- کلیه حقوق معنوی این اثر و محصولات آن (مقالات مستخرج، برنامه‌های رایانه‌ای، نرم‌افزارها و تجهیزات ساخته شده) به دانشگاه علم و هنر تعلق دارد و بدون اخذ اجازه کتبی از دانشگاه قابل واگذاری به شخص ثالث نیست.
- استفاده از اطلاعات و نتایج این پایان نامه بدون ذکر مرجع مجاز نیست.

چکیده :

امروزه امنیت اطلاعات یک مساله حیاتی است و موفقیت سازمان‌ها در سراسر دنیا به آن وابسته است. امنیت سیستم‌های اطلاعاتی هم فناوری و هم افراد (عوامل انسانی) را در بر می‌گیرد. در بیشتر تحقیقاتی که در زمینه امنیت سیستم‌های اطلاعاتی صورت گرفته، یک نوع دید و رویکرد فنی وجود داشته است. پژوهش حاضر در راستای الگوی جدیدی است که آن را مساله انسانی و مساله سازمانی می‌نامند و در آن بر این نکته که کاربران و در کل عوامل انسانی، ضعیف‌ترین و سست‌ترین عنصر آسیب‌پذیر در مدل‌های امنیت سیستم‌های اطلاعاتی هستند، تاکید می‌شود. بنابراین با در نظر گرفتن فقدان یا کمبود عمومی تحقیقات تجربی و اهمیت امنیت اطلاعات برای سازمان‌های امروزی، این مطالعه در جست و جوی شناسایی و رتبه‌بندی عوامل انسانی مؤثر بر امنیت اطلاعات در شرکت توزیع برق استان یزد در سه ماهه دوم ۱۳۹۳ می‌باشد.

در این راستا، ابتدا با استفاده از ادبیات تحقیق و پژوهش‌های صورت گرفته در خصوص موضوع پژوهش، شاخص‌های اولیه شناسایی گردید. براساس مدل پیشنهادی تحقیق، ۲۷ شاخص شناسایی شده در نه بعد حمایت مدیریت عالی، فرهنگ امنیتی، آموزش امنیتی، خط‌مشی امنیتی، تجربیات مستقیم، خودباوری، مهارت، رعایت اخلاق و رفتار امنیتی گروه‌بندی شد. پس از طراحی پرسشنامه و نظرسنجی از خبرگان شرکت برق شاخص‌های نهایی در قالب هشت بعد و ۱۹ شاخص تعیین گردید. پس از تایید شاخص‌ها، به شیوه نظرسنجی از خبرگان تلاش شد تا میزان اهمیت هر یک از ابعاد و مولفه‌های انسانی مؤثر بر امنیت اطلاعات در شرکت توزیع برق استان یزد بدست آید.

براساس داده‌های گردآوری شده، با استفاده از تلفیق تکنیک دیمتل فازی و ANP فازی، روابط علت و معلولی و اهمیت هر یک از عوامل تعیین و در نهایت رتبه‌بندی گردید. نتایج نشان داد که پنج شاخص اول به شرح زیر می‌باشند.

- اشاعه و استفاده از اطلاعات محرمانه (امنیتی)
- سو استفاده از سیستم اطلاعات (سوء استفاده عمدی کارمندان داخلی از منابع IS)
- آگاهی از اهمیت و ضرورت پیروی از قوانین و اجرای فعالیت‌های امنیتی
- استفاده از ابزارهای آموزشی متنوع برای آموزش فعالیتهای مرتبط با امنیت سیستمهای اطلاعاتی
- تعهد و وفاداری کارمندان نسبت به سازمان و حفظ اطلاعات

در نهایت با نظرسنجی از خبرگان و پیشینه تحقیق، راهکارهای بهبود امنیت اطلاعات که با توجه به شاخص‌های برتر و تاثیرگذار در این شرکت ارائه گردید. این راهکارها عبارتند از:

- پیاده‌سازی سیستم‌های مدیریت امنیت اطلاعات نظیر سیستم مدیریت امنیت فناوری اطلاعات ISO۲۷۰۰۰
- استفاده از سیستم‌ها و نرم افزارهایی در جهت محدود کردن دسترسی کاربران به اطلاعات
- برگزاری دوره‌های آموزشی ضمن خدمت برای کارکنان جهت آشنایی با اصول امنیت اطلاعات در سازمان و آگاه کردن کارمندان از اهمیت و ضرورت آن
- وجود افراد آموزش دیده و متخصص در زمینه امنیت اطلاعات و سیستم‌ها

کلمات کلیدی : امنیت اطلاعات، فرایند تحلیل شبکه‌ای، تکنیک دیمتل. فازی

فهرست مطالب

عنوان	صفحه
فصل اول: کلیات تحقیق	۱
۱-۱- مقدمه	۲
۲-۱- تعریف مسئله	۲
۳-۱- اهداف تحقیق	۳
۴-۱- سوال‌های تحقیق	۳
۵-۱- محدودیت‌های تحقیق	۳
۶-۱- روش تحقیق	۳
۷-۱- قلمرو تحقیق	۴
۸-۱- فصل بندی تحقیق	۴
۹-۱- شرح واژه‌ها و اصطلاحات به کار رفته در تحقیق	۴
۱۰-۱- خلاصه	۵
فصل دوم: ادبیات و پیشینه پژوهش	۶
۱-۲- مقدمه	۷
۲-۲- مفاهیم مربوط به داده و اطلاعات	۷
۳-۲- اهمیت و نقش اطلاعات در سازمان	۸
۴-۲- سیستم‌های اطلاعاتی	۹
۱-۴-۲- طبقه‌بندی سیستم‌های اطلاعات	۹
۱-۱-۴-۲- طبقه بندی بر اساس سطوح سازمان	۹
۲-۱-۴-۲- سیستم‌های اطلاعات کارکردی (بخشی)	۱۰
۳-۱-۴-۲- سیستم‌های اطلاعات سازمانی	۱۰
۴-۱-۴-۲- سیستم‌های بین سازمانی	۱۰
۲-۴-۲- طبقه بندی بر مبنای نوع پشتیبانی	۱۱
۴-۱-۴-۲- طبقه بندی سیستم‌های اطلاعاتی بر اساس محتوای اطلاعات پردازش شده	۱۲
۵-۲- مفاهیم امنیت اطلاعات	۱۲
۱-۵-۲- امنیت چیست؟	۱۲
۲-۵-۲- امنیت اطلاعات چیست؟	۱۳
۳-۵-۲- اهمیت امنیت اطلاعات در سازمان	۱۳
۴-۵-۲- اصول پایه ای امنیت اطلاعات	۱۴
۵-۵-۲- سطوح امنیت اطلاعات	۱۴
۶-۵-۲- اهداف، مزایا و محدودیتهای سیستم مدیریت امنیت اطلاعات	۱۵
۷-۵-۲- طراحی، پیاده سازی، نگهداری و بهبود سیستم های مدیریت امنیت اطلاعات	۱۷
۱-۷-۵-۲- عوامل موثر در طراحی سیستم مدیریت امنیت اطلاعات	۱۷
۲-۷-۵-۲- مراحل پیاده سازی سیستم مدیریت امنیت اطلاعات(ایمن سازی)	۱۷
۳-۷-۵-۲- استانداردهای مدیریت امنیت اطلاعات	۲۲
۱-۳-۷-۵-۲- ISO/IEC ۲۷۰۰۱:۲۰۰۵	۲۳

۲۴	۲-۵-۷-۳-۱-۱-۱- فواید استاندارد ISO ۲۷۰۰۱ و لزوم پیاده سازی
۲۴	۲-۵-۷-۳-۲- استاندارد BSV۷۹۹
۲۵	۲-۵-۷-۳-۳- استاندارد ISO/IEC ۱۷۷۹۹
۲۵	۲-۵-۸-۱- ابعاد امنیت اطلاعات
۲۵	۲-۵-۸-۱- بعد فیزیکی امنیت اطلاعات
۲۶	۲-۵-۸-۱- برنامه امنیت فیزیکی و حفاظت از سختافزار رایانه
۲۷	۲-۵-۸-۲- بعد تکنیکی امنیت اطلاعات
۲۸	۲-۵-۸-۳- امنیت منابع انسانی
۲۸	۲-۵-۹- لایه‌های امنیت اطلاعات
۲۹	۶- نقش جنبه‌ها و عوامل مختلف در سازمان
۲۹	۲-۶-۱- جنبه‌های مختلف در امنیت اطلاعات
۳۰	۲-۶-۱-۱- تکنولوژی
۳۰	۲-۶-۱-۲- فرایندها و عملیات
۳۱	۲-۶-۱-۳- افراد
۳۱	۲-۶-۲- عوامل مختلف در امنیت اطلاعات
۳۱	۲-۶-۲-۱- نقش عوامل فنی و غیرفنی در امنیت اطلاعات
۳۲	۲-۶-۲-۲- نقش عوامل انسانی امنیت سیستم‌های اطلاعاتی
۳۵	۲-۶-۲-۱- ابعاد انسانی
۴۱	۷- بخش دوم: روش‌های و تکنیک‌های کاربردی تحقیق
۴۱	۲-۷-۱- تکنیک‌های تصمیم‌گیری چندمعیاره (MCDM)
۴۲	۲-۷-۱-۱- ارزیابی و بررسی مدل‌های MADM
۴۳	۲-۷-۲- علم مدیریت فازی
۴۳	۲-۷-۲-۱- اعداد فازی و عملیات جبری
۴۴	۲-۷-۲-۲- اعداد فازی نوع LR
۴۵	۲-۷-۲-۳- اعداد فازی دوزنقه‌ای و مثلثی
۴۵	۲-۷-۳- روش DEMATEL فازی
۴۸	۲-۷-۴- تکنیک فرایند تحلیل سلسله مراتبی شبکه ANP
۵۲	۲-۷-۵- تکنیک ANP فازی
۵۳	۸- پیشینه تحقیقات خارجی و داخلی
۵۶	۹- خلاصه
۵۷	فصل سوم: روش تحقیق
۵۸	۳-۱- مقدمه
۵۸	۳-۲- روش تحقیق
۵۹	۳-۳- فرآیند تحقیق
۵۹	۳-۳-۱- شناسایی عوامل انسانی موثر بر امنیت اطلاعات
۵۹	۳-۳-۲- طراحی مدل شبکه‌ای تحقیق
۶۰	۳-۳-۳- اولویت‌بندی عوامل انسانی موثر بر امنیت اطلاعات با رویکرد تلفیقی ANP و دیمتل فازی
۶۱	۳-۳-۴- ارائه راهکارهای بهبود
۶۱	۳-۴- روش‌شناسی تحقیق
۶۱	۳-۴-۱- سوالات پژوهشی
۶۱	۳-۴-۲- قلمرو مکانی و زمانی تحقیق

۶۲ ۳-۴-۳- جامعه و نمونه آماری
۶۲ ۳-۴-۴- روش گردآوری دادهها
۶۳ ۳-۴-۵- ابزار گردآوری دادههای پژوهش
۶۳ ۳-۴-۵-۱- روایی پرسشنامه
۶۳ ۳-۴-۵-۲- پایایی پرسشنامه
۶۴ ۳-۵- روشها و تکنیکهای تجزیه و تحلیل دادهها
۶۴ ۳-۶- جمعبندی
۶۵ فصل چهارم: تجزیه و تحلیل اطلاعات
۶۶ ۴-۱- مقدمه
 ۴-۲- شناسایی و اولویت بندی عوامل انسانی موثر بر امنیت اطلاعات در شرکت توزیع برق استان یزد با رویکرد
۶۶ تلفیقی ANP و DEMATEL فازی
۶۸ ۴-۲-۱- یافته‌های تکنیک دیمتل فازی
۶۸ ۴-۲-۱-۱- تعیین روابط علت و معلولی بین عوامل انسانی موثر بر امنیت اطلاعات استفاده از تکنیک DEMATEL فازی
۷۵ ۴-۲-۱-۲- تعیین روابط علت و معلولی بین شاخص‌های حمایت مدیریت عالی استفاده از تکنیک DEMATEL فازی
۷۶ ۴-۲-۱-۳- تعیین روابط علت و معلولی بین شاخص‌های فرهنگ امنیتی استفاده از تکنیک DEMATEL فازی
۷۷ ۴-۲-۱-۴- تعیین روابط علت و معلولی بین شاخص‌های آموزش امنیتی استفاده از تکنیک DEMATEL فازی
۷۸ ۴-۲-۱-۵- تعیین روابط علت و معلولی بین شاخص‌های خطمشی امنیتی استفاده از تکنیک DEMATEL فازی
۷۹ ۴-۲-۱-۶- تعیین روابط علت و معلولی بین شاخص‌های تجربه و مهارت استفاده از تکنیک DEMATEL فازی
۸۰ ۴-۲-۱-۷- تعیین روابط علت و معلولی بین شاخص‌های خودباوری استفاده از تکنیک DEMATEL فازی
۸۱ ۴-۲-۱-۸- تعیین روابط علت و معلولی بین شاخص‌های رفتار امنیتی استفاده از تکنیک DEMATEL فازی
۸۲ ۴-۲-۱-۹- تعیین روابط علت و معلولی بین شاخص‌های رعایت اخلاق استفاده از تکنیک DEMATEL فازی
 ۴-۲-۲- بهدست آوردن بردار ویژه ابعاد امنیت اطلاعات نسبت به هدف و شاخص‌ها نسبت به ابعاد هشت‌گانه با استفاده از
۸۳ ANP فازی
۸۵ ۴-۲-۱- مراحل بهدست آوردن وزن مؤلفهها با تحلیل شبکههای فازی
۹۲ ۴-۲-۳- تعیین وزن نهایی عوامل و شاخص‌ها نسبت به هدف
۹۷ ۴-۳- نتیجه گیری
۹۸ فصل پنجم: بحث و نتیجه گیری
۹۹ ۵-۱- مقدمه
۹۹ ۵-۲- پاسخ به سوالات تحقیق
۱۰۲ ۵-۳- پیشنهادات کاربردی
۱۰۳ ۵-۴- پیشنهادات پژوهشی

فهرست جدول ها

صفحه	عنوان جدول
۱۱	جدول ۱-۲: طبقه انواع اصلی سیستمهای پشتیبانی مبتنی بر فناوری اطلاعات
۲۰	جدول ۲-۲: اقدامات لازم جهت پیاده سازی سیستم مدیریت امنیت اطلاعات
۳۷	جدول ۳-۲: اشتباهات انسانی مطرح در سیستمهای اطلاعاتی
۴۴	جدول ۴-۲: مفاهیم مربوط به رفتار امنیتی
۴۵	جدول ۵-۲: چارچوب مفهومی رفتار امنیتی
۶۶	جدول ۱-۳: عبارت کلامی و اعداد فازی جهت مقایسه ترجیحات ابعاد و مولفهها
۶۶	جدول ۲-۳: اعداد فازی محاسبه ارتباطات داخلی
۷۵	جدول ۱-۴: میانگین نظر تمام خبرگان در خصوص تاثیر عوامل هشتگانه
۷۶	جدول ۲-۴: ماتریس نرمالیزه شده ابعاد امنیت اطلاعات
۷۸	جدول ۳-۴: ماتریس روابط کل ابعاد امنیت اطلاعات
۷۹	جدول ۴-۴: اهمیت و تأثیرگذاری ابعاد امنیت اطلاعات (اعداد فازی)
۸۰	جدول ۵-۴: اهمیت و تأثیرگذاری ابعاد امنیت اطلاعات (اعداد قطعی)
۸۱	جدول ۶-۴: ماتریس روابط کل شاخصهای حمایت مدیریت عالی
۸۱	جدول ۷-۴: اهمیت و تأثیرگذاری شاخصهای حمایت مدیریت عالی (اعداد قطعی)
۸۲	جدول ۸-۴: ماتریس روابط کل شاخصهای فرهنگ امنیتی
۸۳	جدول ۹-۴: اهمیت و تأثیرگذاری شاخصهای فرهنگ امنیتی (اعداد قطعی)
۸۴	جدول ۱۰-۴: ماتریس روابط کل شاخصهای آموزش امنیتی
۸۴	جدول ۱۱-۴: اهمیت و تأثیرگذاری شاخصهای آموزش امنیتی (اعداد قطعی)
۸۵	جدول ۱۲-۴: ماتریس روابط کل شاخصهای خطمشی امنیتی
۸۵	جدول ۱۳-۴: اهمیت و تأثیرگذاری شاخصهای خطمشی امنیتی (اعداد قطعی)
۸۶	جدول ۱۴-۴: ماتریس روابط کل شاخصهای تجربه و مهارت امنیتی
۸۶	جدول ۱۵-۴: اهمیت و تأثیرگذاری شاخصهای تجربه و مهارت (اعداد قطعی)
۸۷	جدول ۱۶-۴: ماتریس روابط کل شاخصهای خودباوری
۸۸	جدول ۱۷-۴: اهمیت و تأثیرگذاری شاخصهای خودباوری (اعداد قطعی)
۸۸	جدول ۱۸-۴: ماتریس روابط کل شاخصهای رفتار امنیتی
۸۹	جدول ۱۹-۴: اهمیت و تأثیرگذاری شاخصهای رفتار امنیتی (اعداد قطعی)
۸۹	جدول ۲۰-۴: ماتریس روابط کل شاخصهای رعایت اخلاق
۹۰	جدول ۲۱-۴: اهمیت و تأثیرگذاری شاخصهای رعایت اخلاق (اعداد قطعی)
۹۲	جدول ۲۲-۴: شاخصهای تصادفی (RI)
۹۴	جدول ۲۳-۴: میانگین مقایسات زوجی نسبت به هدف
۹۵	جدول ۲۴-۴: میانگین مقایسات زوجی شاخصهای حمایت مدیریت عالی
۹۵	جدول ۲۵-۴: میانگین مقایسات زوجی شاخصهای فرهنگ امنیتی
۹۵	جدول ۲۶-۴: میانگین مقایسات زوجی شاخصهای آموزش امنیتی
۹۵	جدول ۲۷-۴: میانگین مقایسات زوجی شاخصهای خطمشی امنیتی
۹۵	جدول ۲۸-۴: میانگین مقایسات زوجی شاخصهای تجربه و مهارت
۹۶	جدول ۲۹-۴: میانگین مقایسات زوجی شاخصهای خودباوری
۹۶	جدول ۳۰-۴: میانگین مقایسات زوجی شاخصهای رفتار امنیتی
۹۶	جدول ۳۱-۴: میانگین مقایسات زوجی شاخصهای رعایت اخلاق

- جدول ۴-۳۲: ماتریس بردار ویژه (وزن) عوامل انسانی امنیت اطلاعات نسبت به هدف ۹۶
- جدول ۴-۳۳: ماتریس بردار ویژه (وزن) شاخص‌ها نسبت به عوامل ۹۷
- جدول ۴-۳۴: ماتریس روابط کل نرمالایز شده عوامل انسانی امنیت اطلاعات ۹۹
- جدول ۴-۳۵: وزن نهایی عوامل موثر بر امنیت اطلاعات نسبت به هدف ۱۰۰
- جدول ۴-۳۶: ماتریس روابط کل نرمالایز شده شاخص‌ها ۱۰۱
- جدول ۴-۳۷: وزن نهایی معیارها نسبت به هدف ۱۰۳
- جدول ۵-۱: وزن نهایی عوامل انسانی موثر بر امنیت اطلاعات ۱۰۸
- جدول ۵-۲: مقادیر وزن و رتبه شاخص‌های امنیت اطلاعات در شرکت توزیع برق استان یزد ۱۰۸

فهرست شکل ها

عنوان شکل	صفحه
شکل ۱-۲: سیستم بخش (دپارتمانی).....	۱۰
شکل ۲-۲: مراحل ایمن سازی بر اساس ISO/IEC ۱۳۳۳۵.....	۱۹
شکل ۳-۲: مراحل پیاده سازی ISMS بر اساس استاندارد BS۷۷۹۹:۲۰۰۲.....	۲۰
شکل ۴-۲: مرحله برنامه ریزی سیستم مدیریت اطلاعات.....	۲۱
شکل ۵-۲: مرحله بکارگیری و اجرای سیستم مدیریت امنیت اطلاعات.....	۲۲
شکل ۶-۲: مرحله نظارت و بازنگری سیستم مدیریت امنیت اطلاعات.....	۲۳
شکل ۷-۲: مرحله برقرار نگهداشتن و بهبود سیستم مدیریت امنیت اطلاعات.....	۲۴
شکل ۸-۲: لایه های امنیتی اطلاعات.....	۳۱
شکل ۹-۲: مدل کوه یخ پولانی، دانش امنیت اطلاعات در سال ۱۹۹۴.....	۳۱
شکل ۱۰-۲: جنبه های مختلف در امنیت اطلاعات.....	۳۲
شکل ۱۱-۲: فاکتورهای غیرفنی اثرگذار بر به کارگیری خط مشی های امنیتی.....	۳۴
شکل ۱۲-۲: ارتباط بین میزان کنترل و هزینه ها.....	۳۵
شکل ۱۳-۲: تعدیل ارزش.....	۴۱
شکل ۱۴-۲: انواع مدل های تصمیم گیری در روش MADM.....	۴۶
شکل ۱۵-۲: تفاوت ساختاری بین یک زنجیره (a) و یک شبکه (b).....	۵۳
شکل ۱۶-۲: شکل استاندارد یک سوپرماتریس.....	۵۵
شکل ۱۷-۲: زنجیره و شبکه (a) یک زنجیره (b) یک شبکه.....	۵۶
شکل ۱۸-۲: مدل تأثیر ویژگی های سازمانی بر ادراک و ارتقای امنیت اطلاعات.....	۵۹
شکل ۱۹-۲: تأثیر توانمندی های سازمانی بر امنیت اطلاعات.....	۵۹
شکل ۱-۳: مدل شبکه ای تحقیق.....	۶۵
شکل ۱-۴: نمودار شبکه ای تحقیق.....	۷۳
شکل ۲-۴: نمودار علت و معلولی ابعاد امنیت اطلاعات.....	۸۰
شکل ۳-۴: نمودار علت و معلولی شاخص های حمایت مدیریت عالی.....	۸۲
شکل ۴-۴: نمودار علت و معلولی شاخص های فرهنگ امنیتی.....	۸۳
شکل ۵-۴: نمودار علت و معلولی شاخص های آموزش امنیتی.....	۸۴
شکل ۶-۴: نمودار علت و معلولی شاخص های خط مشی امنیتی.....	۸۶
شکل ۷-۴: نمودار علت و معلولی شاخص های تجربه و مهارت.....	۸۷
شکل ۸-۴: نمودار علت و معلولی شاخص های خودباوری.....	۸۸
شکل ۹-۴: نمودار علت و معلولی شاخص های رفتار امنیتی.....	۸۹
شکل ۱۰-۴: نمودار علت و معلولی شاخص های رعایت اخلاق.....	۹۰

فصل اول

کلیات تحقیق

۱-۱- مقدمه

امنیت اطلاعات یک مساله حیاتی است و امروزه سازمان‌ها در سراسر دنیا با آن روبه‌رو هستند. امنیت سیستم‌های اطلاعاتی هم فناوری و هم افراد (عوامل انسانی) را در بر می‌گیرد. در بیشتر تحقیقاتی که در زمینه امنیت سیستم‌های اطلاعاتی صورت گرفته، یک نوع دید و رویکرد فنی وجود داشته است. پژوهش حاضر در راستای الگوی جدیدی است که آن را مساله انسانی و مساله 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 هستند، تاکید می‌شود پژوهش حاضر در راستای این الگوی جدید، رویکردی متفاوت از امنیت اطلاعات را با تمرکز بر "عوامل انسانی مؤثر بر امنیت اطلاعات" ارائه می‌دهد. بنابراین با در نظر گرفتن فقدان یا کمبود عمومی تحقیقات تجربی و اهمیت امنیت اطلاعات برای سازمان‌های امروزی، این مطالعه در جست و جوی شناسایی و رتبه‌بندی عوامل انسانی مؤثر بر امنیت اطلاعات در شرکت توزیع برق استان یزد خواهد بود.

۱-۲- تعریف مسئله

اکثر قریب به اتفاق سازمان‌ها در معرض انواع تهدیدات داخلی و خارجی خرابکاران اطلاعاتی هستند؛ تهدیداتی چون دستکاری اطلاعات مرجع، سرقت اطلاعات حیاتی و سرمایه‌های اطلاعاتی. در چنین شرایطی، عواملی که می‌توانند از مزایای سیستم‌ها به شمار آیند (مثل سرعت و قابلیت دسترسی بالا)، اگر تحت کنترل نباشند ممکن است باعث بروز آسیب‌پذیری شوند و سوء استفاده افراد از آنها به نفوذ، خرابکاری و کلاهبرداری بیانجامد. علاوه بر این، مشکلات طبیعی و خطاهای غیرعمدی که توسط کاربران رایانه‌ای رخ می‌دهد، در صورت فقدان روال صحیح برای حفاظت از اطلاعات می‌تواند نتایج مخربی به بار آورد. بنابراین ضرورت توجه به "امنیت اطلاعات" و "مدیریت امنیت اطلاعات" بیش از پیش احساس می‌شود (Pathari & Sonar, ۲۰۱۲). در سال ۱۹۸۰، مجله ام ای اس، نتایج یکی از مطالعات کلیدی را که با همکاری تعدادی از اعضای جامعه مدیریت اطلاعات و یک گروه از مدیران اجرایی فناوری اطلاعات انجام شده بود، را منتشر کرد. طی دهه ۱۹۸۰ امنیت به عنوان یک مساله رده پایین رتبه‌بندی شد و هرگز رتبه‌ای بیشتر از ۱۲ کسب نکرد. در بررسی ۱۹۹۴ امنیت حتی از لیست ۲۰ مساله اولویت‌دار خارج شد. با وجود این در بررسی‌ای که در سال ۲۰۰۳ انجام شد، امنیت و حریم خصوصی نوسان زیادی پیدا کرد تا جایی که در میان شرکت‌کنندگان در این بررسی، به عنوان سومین مساله با درجه اهمیت زیاد شناسایی گردید (Shirtz & Elovici, ۲۰۱۱). طبق این شرایط نیاز به حمایت از اطلاعات و کاهش ریسک نسبت به قبل بسیار مهمتر و برجسته‌تر شده است. بررسی‌های ملی متعدد، تعداد زیادی از حملات به منابع اطلاعاتی سازمان را تطبیق داده‌اند. بین سال‌های ۱۹۹۸ و ۲۰۰۳، تعداد حوادث گزارش شده به "تیم پاسخ به شرایط اضطراری کامپیوتری آمریکا"، تقریباً هر سال دو برابر شده است، که باید به آن تعداد ۱۳۷، ۵۲۹ حادثه‌ای را که تنها در سال ۲۰۰۳ گزارش شده نیز اضافه کرد. حوادث امنیتی برای هر رخداد می‌تواند هزینه‌ای بین ۱۷ و ۲۸ میلیون دلار برای شرکت‌ها داشته باشد. از آن جا که حوادث، مکرر و هزینه بر هستند، مدیریت باید امنیت را به صورت جدی مورد توجه قرار دهد تا بتواند اطلاعات و سیستم‌های اطلاعاتی سازمانی را حفظ و حمایت کند (Debar & Viinikka, ۲۰۰۶).

تاکنون بیشتر تحقیقاتی که در زمینه امنیت سیستم‌های اطلاعاتی انجام شده، در زمینه مسائل فنی و تکتیکی بوده است و در نتیجه نگرش و دید موجود به امنیت اطلاعات به عنوان یک مساله فنی بر تحقیقات و تمرین‌های تحقیقاتی تسلط داشته است. به عنوان مثال (Bellone, ۲۰۰۸)، بیان می‌کند که در بیشتر تحقیقاتی که در زمینه امنیت اطلاعات صورت گرفته است یک نوع دید و رویکرد فنی وجود داشته است و متخصصین امنیت اطلاعات بیشتر به دنبال یک سری ابزارهای فنی مانند آنتی‌ویروس‌ها، فایروال‌ها و ... برای برطرف کردن مشکلات امنیتی‌شان بوده‌اند. با اینحال (Thomson & Niekerk, ۲۰۱۲)، بیان می‌کنند که امنیت اطلاعات هم تکنولوژی و هم فرد را در بر می‌گیرد، اما بیشتر سازمان‌ها راه حل‌های فنی را جواب فوری به مشکلات امنیتی خود می‌دانند، در حالی که موانع

زیادی برای یک رویکرد فنی وجود دارد. در یکی از تحقیقات (Bhattacharya, ۲۰۱۱)، عامل انسانی به عنوان پاشنه آشیل امنیت اطلاعات معرفی شده است. IBM بیان کرده بود که سال ۲۰۰۹ ضمن این که حملات کوچک‌تر، متمرکزتر و پنهان کارانه‌تری به سیستم‌های اطلاعاتی سازمان‌ها، صورت خواهد گرفت، کانون توجه نفوذگران "سهلانگاری و ساده‌اندیشی کاربران" خواهد بود. به گفته رئیس بخش آگاهی شرکت کامپیوتری آرمونگ، "کاربر" همچنان به عنوان سست‌ترین عنصر آسیب‌پذیر در مدل‌های امنیتی اطلاعات، مورد سوء استفاده قرار خواهد گرفت. امروزه به نظر می‌رسد، موفقیت امنیت اطلاعات تا حد زیادی به رفتار اثربخش کاربران وابسته است. رفتارهای درست و سازنده توسط کاربران، مدیران سیستم و افراد دیگر میتواند اثربخشی امنیت اطلاعات را تا حد زیادی بالا ببرد؛ در حالی که رفتارهای نادرست و مخرب، در حقیقت می‌تواند مانع اثربخشی آن شود (Hagen et al, ۲۰۱۱). پژوهش حاضر در راستای این الگوی جدید، رویکردی متفاوت از امنیت اطلاعات را با تمرکز بر "عوامل انسانی مؤثر بر امنیت اطلاعات" ارائه می‌دهد. بنابراین با در نظر گرفتن فقدان یا کمبود عمومی تحقیقات تجربی و اهمیت امنیت اطلاعات برای سازمان‌های امروزی، این مطالعه در جست‌وجوی شناسایی و رتبه‌بندی عوامل انسانی مؤثر بر امنیت اطلاعات در شرکت توزیع برق استان یزد خواهد بود. که برای این شناسایی عوامل و تعیین درجه اهمیت آنها از تکنیک ANP فازی و نیز دیماتل استفاده خواهد شد.

۱-۳- اهداف تحقیق

هدف اصلی تحقیق حاضر شناسایی و اولویت بندی عوامل انسانی مؤثر بر امنیت اطلاعات با استفاده از تکنیک‌های تصمیم‌گیری چند معیاره می‌باشد. همچنین تعیین اهمیت نسبی عوامل مؤثر بر امنیت اطلاعات در سازمان، از بعد انسانی هدف فرعی تحقیق حاضر می‌باشد.

۱-۴- سوال‌های تحقیق

براساس اهداف تحقیق، سوال‌های پژوهش حاضر عبارتند از:

- ۱- عوامل انسانی مؤثر بر امنیت اطلاعات در سازمان توزیع برق استان یزد کدامند؟
- ۲- اهمیت عوامل مؤثر بر امنیت اطلاعات با استفاده از تکنیک‌های تصمیم‌گیری چندمعیاره فازی چگونه است؟

۱-۵- محدودیت‌های تحقیق

مهمترین محدودیت‌هایی که در پژوهش حاضر، محقق با آنها مواجه شده است را می‌توان موارد زیر برشمرد:

- انجام کار میدانی و جمع‌آوری داده‌های تحقیق
- مشکل دسترسی به منابع خارجی

۱-۶- روش تحقیق

در تحقیق حاضر از روش‌های کتابخانه‌ای و میدانی جهت جمع‌آوری داده‌های تحقیق استفاده خواهد شد. با استفاده از روش کتابخانه‌ای مبانی نظری تحقیق در خصوص امنیت اطلاعات تدوین خواهد شد. در مرحله اول براساس مطالعات کتابخانه‌ای عوامل انسانی مؤثر بر امنیت اطلاعات شناسایی خواهد شد. در این مرحله با انجام مصاحبه نیمه ساختار یافته با استفاده از پروتکل طراحی شده عوامل انسانی نهایی مؤثر بر امنیت اطلاعات در شرکت توزیع برق استان یزد تعیین خواهد شد. سپس پرسشنامه‌های مقایسات زوجی تحقیق براساس تکنیک ANP و دیمتال فازی طراحی خواهد شد. براساس داده‌های گردآوری شده، با استفاده از تکنیک دیمتال فازی روابط علت و معلولی بین

عوامل تعیین خواهد شد. با استفاده از تلفیق ماتریس روابط کل دیمتل فازی و ANP فازی، اهمیت هر یک از عوامل تعیین و در نهایت رتبه‌بندی خواهد شد. در نهایت براساس رتبه عوامل، پروژه‌های بهبود تدوین خواهد شد. جامعه آماری پژوهش حاضر را مدیران و خبرگان شرکت توزیع برق استان یزد تشکیل می‌دهند. با توجه به اینکه حجم این جامعه محدود می‌باشد، در پژوهش از روش نمونه‌گیری استفاده نشد. در تحقیق حاضر از آمار توصیفی جهت توصیف متغیرهای جمعیت شناختی تحقیق در قالب جدول و نمودار استفاده خواهد شد. از آمار استنباطی جهت بررسی تاثیر گذاری عوامل شناسایی شده بر امنیت اطلاعات با استفاده از آزمون میانگین یک جامعه استفاده می‌شود. در مرحله بعد با استفاده از تکنیک‌های تصمیم‌گیری چندمعیاره فازی (ANP) و DEMATEL، اهمیت شاخص‌های مورد مطالعه در قالب اعداد فازی بررسی خواهد شد. بنابراین در پژوهش از نرم افزار آماری SPSS و نرم افزار اکسل جهت انجام محاسبات فازی استفاده خواهد شد.

۷-۱- قلمرو تحقیق

قلمرو موضوعی تحقیق را مباحث نظری مرتبط با امنیت اطلاعات و ابعاد مرتبط با آن تشکیل می‌دهد. شرکت توزیع برق استان یزد قلمرو مکانی پروژه حاضر را تشکیل می‌دهد. محدوده زمانی تحقیق به صورت مقطعی بوده و شامل سه ماهه دوم سال ۱۳۹۳ می‌باشد.

۸-۱- فصل بندی تحقیق

در فصل اول، به طرح مساله و اهمیت آن، اهداف تحقیق، دامنه تحقیق، روش تحقیق و محدودیت‌های تحقیق پرداخته شده است. در فصل دوم، ادبیات تحقیق شامل مفاهیم نظری در ارتباط با موضوع تحقیق مورد بررسی قرار گرفته است. همچنین به پژوهش‌های صورت گرفته در گذشته نیز اشاره گردیده است. در فصل سوم، روش انجام تحقیق، تشریح شده است. در فصل چهارم، نتایج حاصل از جمع‌آوری داده‌های تحقیق ارائه گردیده است. در فصل پنجم، به بحث و نتیجه‌گیری از پژوهش پرداخته شده و در نهایت پیشنهادها، کاربردی و پژوهشی حاصل از تحقیق بیان گردیده است.

۹-۱- شرح واژه‌ها و اصطلاحات به کار رفته در تحقیق

❖ امنیت اطلاعات^۱:

امنیت اطلاعات یعنی حفاظت اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز. این فعالیت‌ها عبارتند از دسترسی، استفاده، افشاء، خواندن، نسخه برداری یا ضبط، خراب کردن، تغییر و دستکاری.

❖ تصمیم‌گیری چندشاخصه^۲:

یک دسته از مدل‌های تصمیم‌گیری چندمعیاره است که به منظور انتخاب مناسب‌ترین گزینه از بین m گزینه موجود به کار می‌رود (اصغرپور، ۱۳۸۳).

❖ تصمیم‌گیری چندمعیاره^۳:

^۱-Information Security

^۲-Multiple Attribute Decision Making

^۳-Multiple Criteria Decision Making

یک تصمیم گیرنده از چندین معیار به منظور انتخاب راه کار استفاده می کند (Korhonen, Moskowitz and Wallenius, ۱۹۹۲).

❖ منطق فازی^۱:

منطق فازی شامل طیف وسیعی از تئوری ها و تکنیک ها می شود که اساساً بر پایه ۴ مفهوم بنا شده است: مجموعه های فازی، متغیرهای کلامی، توزیع احتمال (تابع عضویت)، و قوانین اگر- آنگاه فازی (Yenand Langari, ۱۹۹۹).

۱-۱- خلاصه

در فصل حاضر کلیات تحقیق نظیر بیان مساله، ضرورت، اهداف و سوال های پژوهشی مورد بررسی قرار گرفت. در پایان نیز به تعاریف واژه های کلیدی تحقیق پرداخته شد. در فصل آتی مبانی نظری پژوهش مورد بررسی قرار خواهد گرفت

^۱-Fuzzy Logic

فصل دوّم

ادبیات و پیشینه پژوهش

۲-۱- مقدمه

عصر کنونی عصر ارتباطات و دانش نامیده می‌شود. عمده‌ترین دلیل این نامگذاری به افزایش وسعت شبکه‌ها و دسترسی آسان به اطلاعات و همچنین اهمیت اطلاعات و دانش در مناسبات اجتماعی است. در این عصر، با رشد و توسعه فزاینده فناوری اطلاعات و گسترش شبکه‌های ارتباطی، آسیب‌پذیری فضای تبادل اطلاعات نیز افزایش یافته است. به همین دلیل، امروزه امنیت اطلاعات، به عنوان یکی از مهمترین ابعاد فناوری اطلاعات شناخته می‌شود. عدم پرداختن به امنیت اطلاعات ممکن است تبعاتی برای کسب و کار داشته باشد که جبران آن ماه‌ها و حتی سال‌ها به طول بیانجامد. از این رو ضرورت توجه به "امنیت اطلاعات"، "مدیریت امنیت اطلاعات" و حفظ ایمنی فضای تبادل اطلاعات بیش‌ازپیش احساس می‌شود (Wilson & Hash, ۲۰۰۳, Veiga & Eloff, ۲۰۱۰, Kruger & Pathari & Sonar, ۲۰۱۲, Kearney, ۲۰۰۶). امنیت سیستم‌های اطلاعات، بسته‌ای از خط‌مشی‌ها و فعالیت‌های نرم‌افزاری و سخت‌افزاری به منظور حفاظت از اطلاعات در برابر طیف وسیعی از تهدیداتی است که تداوم کارها، کمینه کردن ریسک و بیشینه نمودن میزان بازده سرمایه‌گذاری‌ها و فرصت‌ها را نشانه رفته است. و به عبارتی دیگر، امنیت اطلاعات، حفظ محرمانگی، تمامیت و در دسترس بودن اطلاعات و همچنین سایر مواردی مانند تصدیق هویت، مسئولیت‌پذیری، عدم انکار و قابلیت اطمینان را شامل می‌گردد. نیازهای امنیتی از طریق برآورد نظامند ریسک‌های امنیت، شناسایی می‌شود. در بحث امنیت اطلاعات، هزینه‌های صرف شده برای کنترل باید به روشی خاص، آسیب وارد شده به کسب‌وکار که ناشی از خطاهای امنیتی است را تعدیل نماید (Kraemer et al., ۲۰۰۷). با توجه به اهمیت مباحث امنیتی در سازمان‌ها، این فصل از پژوهش به بررسی مفاهیم و مطالعات مرتبط با موضوع تحقیق خواهد پرداخت.

۲-۲- مفاهیم مربوط به داده و اطلاعات

تعریف داده و اطلاعات کار مشکلی است و تنها از دیدگاه استفاده‌کنندگان می‌توان آنها را از هم تشخیص داد (کرمی و اسفیدانی، ۱۳۸۳). در زیر برخی از تعاریف داده و اطلاعات از دیدگاه صاحب‌نظران مختلف ارائه شده است. واژه "داده"، مناسب‌ترین واژه‌ای است که به واقعیات شکل نیافته و بدون ساختار فراوان تولید شده توسط کامپیوتر، می‌توان اطلاق نمود که بر اعداد، نمودارها و دیگر نوشته‌ها دلالت می‌کند و به تنهایی معنی ندارد (رضائیان، ۱۳۷۴). حسن زاده (۱۳۸۶)، معتقد است داده در پایین‌ترین سطح قرار دارد و عبارت است از یک نقطه فاقد معنا در بعد زمان و مکان، که اشاره به زمان یا مکان خاصی ندارد و بلازمینه است. به همین دلیل فاقد رابطه معنی‌دار یا چیزهای دیگر می‌باشد. افرادی که درباره یک رخداد، "داده" به دست آورند، نمی‌توانند درباره آن قضاوت یا تصمیمی اتخاذ کنند. به بیانی دیگر، داده‌ها حقایق و واقعیتهای خام هستند. برای نمونه به داده‌هایی که از یک عمل خرید ساده در یک فروشگاه می‌توان گردآوری کرد، توجه کنید. زمان خرید، کالا، تعداد آن و مقدار پول پرداخت شده می‌توانند داده‌های ثبت شده از خرید باشند. این داده‌ها فاقد هرگونه اطلاعی درباره علت خرید کالای فوق، و احتمال خریدهای بعدی از کالای فوق توسط همان مشتری یا دیگر مشتریان است (Ifinedo, ۲۰۱۲). این داده‌ها در مورد کیفیت سرویس فروشگاه و سوددهی یا زیان‌دهی آن نیز حرفی نمی‌زنند. ردمن (۱۳۸۱) معتقد است که داده‌ها عناصر اصلی اطلاعات هستند (ردمن، ترجمه فارسی، ۱۳۸۱). داده‌ها در صورتی به اطلاعات تبدیل می‌شوند که افراد بخواهند برای درک بیشتر از آنها استفاده کنند. اندیشمندان و پژوهشگران تعاریف متعددی از اطلاعات را ارائه داده‌اند که برخی از آنها مبتنی بر معنا (معنا شناسی) و برخی مبتنی بر کمیت است. مطابق تعریف واژه‌نامه ای ال ای^۱، اطلاعات عبارت است از تمام

^۱-ALA

ایده‌ها، واقعیت‌ها و کارهای خلاقانه ذهن که به صورت رسمی و غیررسمی و به هر حالتی ثبت، منتشر یا توزیع گردیده است و ممکن است مستند یا غیر مستند باشد (لاوان و لاوان، ۱۳۸۴).

بنا بر تعریف مبتنی بر نظریه اطلاعات، اطلاعات کمیتی است که با بیت‌ها اندازه‌گیری شده و بر حسب احتمالات پدیدار شدن نمادها تعریف می‌شود (لاوان و لاوان، ۱۳۸۴).

اطلاعات زمانی حاصل می‌شود که بین داده‌ها در بعد زمانی و مکانی ارتباط ایجاد شود. این ارتباط می‌تواند بین داده‌ها با داده‌ها و اطلاعات برقرار شود. بنابراین اطلاعات تا حدودی دارای زمینه است و اشخاص می‌توانند براساس تطابق داشته‌های قبلی خود را درک و تعبیر کنند (حسن‌زاده، ۱۳۸۶).

داده‌ها طی عملیات‌های منطقی پردازش می‌گردند و تبدیل به اطلاعاتی می‌شوند که دانشی را به کاربر منتقل می‌نماید. بنابراین اطلاعات از دانش پردازش شده تشکیل شده است (شیرازی و آل شیخ، ۱۳۸۹).

کلمه اطلاعات برای اشاره به پدیده‌های مختلفی به کار می‌رود. این پدیده‌ها در سه گروه رده‌بندی می‌شوند:

۱- هر چیزی که بتواند به عنوان دلالت بالقوه بر چیزی درک شود (مثلاً کتاب‌های چاپ شده)،

۲- فرآیند اطلاع دادن و

۳- چیزی که بتوان از مدارک یا ارتباطات یاد گرفت.

هر سه استفاده‌های معتبر از اصطلاح اطلاعات در زبان انگلیسی هستند. در واقع اطلاعات داده‌ای است که مقوله‌بندی و شمرده شده و بنابراین دارای معنی، ربط یا هدف است (Melitsk, ۲۰۰۳).

۲-۳- اهمیت و نقش اطلاعات در سازمان

اطلاعات یکی از مهمترین دارایی‌های هر سازمان محسوب می‌شود و به دلیل ارزش بالا و حیاتی آن برای هر سازمان باید از آن به خوبی محافظت شود. این اهمیت تا جایی است که عده‌ای آن را به خونی در رگ‌های سازمان تشبیه کرده‌اند که عامل حیات بخش به حساب می‌آید (Von Solms and Von Solms, ۲۰۰۴) و در صورت محدودیت و به خطر افتادن این جریان، سازمان خواهد مُرد. به هر حال اهمیت دادن به اطلاعات می‌تواند مزایای بسیاری برای سازمان داشته باشد و سهمی ضروری و اساسی در موفقیت سازمان در عرصه‌هایی چون جریان نقدینگی و ارزش بازار داشته باشد (لاودن و لاودن، ۱۳۸۴). همچنین اطلاعات عامل پیوند سایر منابع سازمان است (Eloff and Von Solms, ۲۰۰۰). اهمیت اطلاعات کسب و کار در چند دهه اخیر، در سازمان‌های امروزی به حدی است که بسیاری از محققان برجسته از اثرات آن بر ابعاد گوناگون سازمان به عنوان انقلاب اطلاعاتی یاد نموده‌اند (لاودن و لاودن، ۱۳۸۴).

برنامه‌ریزی استراتژیک و اقدام هدفمند به اطلاعات سازمان، نقش حیاتی از به هدر رفتن فرصت‌ها، دوباره‌کاری‌ها، اتلاف منابع و عدم سازگاری سیستم‌های اطلاعاتی دارد (علی احمدی، ۱۳۸۸) و می‌توان فرصتی برای بهره‌برداری صحیح از فرصت‌های ناشی از اطلاعات را به همراه داشته باشد. این امر چالشی برای بالا بردن کیفیت اطلاعات در سازمان از جنبه‌های صحت، وجود در زمان مناسب، اعتماد به منشا و اعتبار و مناسب بودن را ایجاد می‌کند. اطلاعات اغلب برای هدایت فرایندهای کسب و کار کارکنان از سطح عالی تا عملیاتی کاربرد دارد و بدون شک مدیریت اثر بخش اطلاعات موجب مزیت رقابتی و ارزش برای کسب و کار گشته و سهام‌داران و سرمایه‌گذاران را خشنود می‌کند (Veiga et al., ۲۰۱۰). از سویی دیگر تصمیم‌گیری، فرایندی مهم و پایه‌ای در فعالیت‌های مدیران است که اساس آن به دست آوردن و پردازش اطلاعاتی می‌باشد که باید سه صفت محرمانگی، صحت و در دسترس بودن را داشته باشد. در غیر این صورت خسارت بزرگی برای سازمان به بار می‌آورد (Grance et al., ۲۰۰۴).

۲-۴- سیستم‌های اطلاعاتی

تعاریف متعددی از سیستم اطلاعات در رشته‌هایی مانند مدیریت، علوم کامپیوتر، مهندسی نرم افزار و علوم کتابداری و اطلاع‌رسانی ارائه شده است. در واژه‌نامه انجمن کتابداری آمریکا (Young, ۱۹۸۳)، تعریفی جامع از سیستم‌های اطلاعاتی به صورت زیر آمده است:

«یک سیستم کامل طراحی شده برای تولید، جمع‌آوری، سازماندهی (پردازش)، ذخیره، بازیابی و اشاعه اطلاعات در یک مؤسسه، سازمان یا هر حوزه تعریف شده دیگر از جامعه».

براساس این تعریف، سیستم‌های اطلاعاتی محدود به سازمان‌ها نمی‌شوند و می‌توانند در محدوده‌ای وسیع‌تر از سازمان، به عنوان مثال در یک شهر نیز موضوعیت یابند. استفاده از سیستم‌های اطلاعاتی نیازمند شناخت سازمان، مدیریت و فن‌آوری اطلاعات است که شکل دهنده سیستم‌ها می‌باشند (Gorge, ۱۹۹۹). با پیشرفت فن‌آوری اطلاعات سیستم‌های اطلاعاتی به شکل گسترده‌ای مورد استفاده قرار می‌گیرند. شرکت‌های بزرگ به صورت روز افزون در فعالیت‌های خود برای پردازش، نگهداری و گزارش‌گیری اطلاعات ضروری به تعداد زیادی از سیستم‌های اطلاعاتی در سطوح مختلف وابسته‌اند (Cascarino, ۲۰۰۷). نقش سیستم‌های اطلاعاتی در عملکرد سازمانی به صورت مؤثری تغییر یافته است و امروزه سیستم‌های اطلاعاتی برای سازمان خالق ارزش هستند (Choon and oh, ۲۰۰۱).

عموماً سیستم‌های اطلاعاتی به عنوان ابزاری برای پشتیبانی‌های زیر توسعه می‌یابند:

- ۱- پشتیبانی اطلاعاتی؛ ارائه پشتیبانی برای دریافت، ذخیره، فیلتر و ردیابی کردن اطلاعات.
- ۲- پشتیبانی تصمیم‌گیری؛ استفاده از اطلاعات برای پشتیبانی هوشمند برای رسیدن به تصمیماتی در خصوص مسائل نیمه ساخت یافته یا ساخت نیافته.
- ۳- پشتیبانی ارتباطی؛ ارائه پشتیبانی برای به اشتراک گذاشتن یا تبادل اطلاعات بین کاربران (Mentzas, ۱۹۹۵).

۲-۴-۱- طبقه‌بندی سیستم‌های اطلاعات

در این قسمت طبقه‌بندی سیستم‌های اطلاعاتی بر اساس سطوح سازمانی، نوع پشتیبانی و محتوای اطلاعات پردازش شده تشریح می‌شوند.

۲-۴-۱-۱- طبقه بندی بر اساس سطوح سازمان

سازمان‌ها اجزائی مانند بخش‌ها، ادارات و واحدهای کاری تشکیل شده‌اند که در قالب سلسله مراتب، سازماندهی گشته‌اند. برای مثال اغلب سازمان‌ها دارای بخش‌های اجرایی مانند بخش تولید و حسابداری هستند که به مدیر کارخانه گزارش می‌دهند و او هم به دفتر مرکزی گزارش می‌دهد. اگرچه بعضی سازمان‌ها از ساختارهای نوین و مبتکرانه نظیر تیم‌های چندمنظوره بهره می‌برند، اما اکثریت سازمانها هنوز از ساختار سلسله مراتبی سنتی برخوردارند. بنابراین می‌توان سیستم‌های اطلاعاتی یافت که برای ادارات مرکزی، بخش‌ها، ادارات، واحدهای عملیاتی و حتی هریک از کارکنان طراحی شده باشند. اینگونه سیستم‌ها می‌توانند به تنهایی کار کنند، ولی معمولاً به یکدیگر متصل هستند. سیستم‌های اطلاعاتی که از ساختار سازمانی پیروی می‌کنند، عبارتند از: سیستم‌های کارکردی (بخشی)، سازمانی و بین سازمان. همانطور که در شکل (۲-۱) دیده می‌شود این سیستم‌ها به صورت سلسله مراتبی هستند که در آنها هر سیستم موجود در مرتبه بالاتر شامل چندین سیستم متنوع (این تعداد ممکن است بسیار زیاد باشد) در سطوح پایین‌تر است، همان‌گونه که در شکل نیز مشاهده می‌شود، یک سیستم بخشی (دپارتمانی) حوزه‌های کارکردی سازمان را مورد پشتیبانی قرار می‌دهد. در یک سطح بالاتر، یک سیستم سازمانی، تمام بخش‌های