DOI: http://dx.doi.org/10.22059/jitm.2015.53555

مدیریت فناوری اطلاعات
دانشکدهٔ مدیریت دانشگاه تهران

دورهٔ ۷، شمارهٔ ۱
بهـار ۱۳۹۴
ص. ۱۸۴- ۱۶۳

شناسایی ریسک‌های امنیت اطلاعات سازمانی با استفاده از روش دلفی فازی در صنعت بانکداری

پریسا موسوی[۱]، رضا یوسفی زنوز[۲]، اکبر حسن‌پور[۳]

چکیده: بیشتر سازمان‌ها برای بقا و پیشرفت به سیستم‌های اطلاعاتی نیاز دارند، در نتیجه باید به‌طور جدی به حفاظت از دارایی‌های اطلاعـاتی خـود بپردازنـد. ایجـاد تبـادلات سـاختارمند و توجیه‌پذیر بین هزینه، امنیت و مأموریت برای کنترل ریسک‌های سیستم‌های امنیتی، ضـروری است. این امر در برنامه‌ریزی و توسعهٔ چنین سیستم‌هـایی از اهمیـت ویـژه‌ای برخـوردار اسـت. مدیریت ریسک و تصمیم‌گیری مناسب اولیه، می‌تواند ضمن کاهش هزینه‌هـا، سـهولت کنتـرل ریسک را افزایش دهد. اولین گام در فرایند مدیریت ریسک، شناسایی ریسک است. هـدف ایـن پژوهش، شناسایی مهم‌ترین ریسک‌های امنیت اطلاعات سازمانی است. این پـژوهش حاضـر از دید هدف کاربردی است و از دیدگاه روش انجام پژوهش، توصـیفی شـمرده مـی‌شـود. در ایـن پژوهش برای شناسایی ریسک‌هـای امنیـت اطلاعـات سـازمانی، از طریـق مطالعـهٔ اسـنادی و به‌کمک روش دلفی فازی و نظر خبرگان شامل ۱۰ متخصص فناوری اطلاعات بانـک، الگـویی بر اساس استاندارد ایزو ۲۷۰۰۲ و چارچوب کوبیت ۴ ارائه شده است. در این الگو شش شـاخص و ۲۰ زیرشاخص ریسک امنیت اطلاعات سازمانی برای بانک شناسایی شد.

واژه‌های کلیدی: امنیت اطلاعات، دلفی فازی، ریسک، شناسایی ریسک.

۱. کارشناس‌ارشد مدیریت فناوری اطلاعات، دانشکدهٔ مدیریت و حسابداری، دانشگاه خوارزمی، تهران، ایران
۲. استادیار گروه مدیریت، دانشکدهٔ مدیریت و حسابداری، دانشگاه خوارزمی، تهران، ایران
۳. استادیار گروه مدیریت، دانشکدهٔ مدیریت و حسابداری، دانشگاه خوارزمی، تهران، ایران

تاریخ دریافت مقاله: ۱۳۹۳/۰۶/۲۲
تاریخ پذیرش نهایی مقاله: ۱۳۹۳/۱۲/۰۹
نویسندهٔ مسئول مقاله: پریسا موسوی
E-mail: parisamusavi_7@yahoo.com

مقدمه

در دنیای کنونی اطلاعات با ارزش‌ترین دارایی هر سازمان محسوب می‌شود و باید آن را کالای اساسی هر سازمان دانست. همانند الکتریسیته که بدون آن بسیاری از کسب‌وکارها نمی‌توانند به‌سادگی جریان داشته باشند (نیکرک و سولمز، ۲۰۱۰)؛ اطلاعات نیز ارزشمندترین دارایی هر سازمان شمرده می‌شود و عامل بسیار حیاتی برای موفقیت سازمان است. از این رو عالی‌ترین سطح مدیریت که برای رسیدن سازمان به موفقیت پاسخگو است، مسئولیت حفاظت از اطلاعات سازمانی را برعهده دارد (ازکان و کارابکاک، ۲۰۱۰). توسعهٔ سیستم‌های اطلاعاتی مانند شمشیر دولبه‌ای است که از یک سو منافع بسیاری را برای بشر به ارمغان آورده است و از سوی دیگر، به‌سبب امنیت اطلاعات، زیان‌های جبران‌ناپذیری را به‌دنبال دارد (یان و چن، ۲۰۱۲). براساس بررسی ادارهٔ تحقیقات فدرال آمریکا[1]، زیان‌های اقتصادی ناشی از امنیت شبکه در ایالات متحدهٔ آمریکا، بیش از ۱۷۰میلیارد دلار در سال است (یان و چن، ۲۰۱۲). طبق بررسی مؤسسهٔ امنیت کامپیوتری برای جرایم رایانه‌ای و امنیتی ۷۳۸ سازمان در سال ۲۰۱۰، زیان سالانهٔ ناشی از حوادث امنیتی سیستم‌های اطلاعاتی، صدونود میلیون دلار گزارش شده است (نان، هری و مینکیانگ، ۲۰۱۴). همچنین به گزارش مؤسسهٔ امنیت کامپیوتری، در آمریکا درصد شرکت‌هایی که بخشی (۳ درصد یا بیشتر) از بودجهٔ IT خود را به امنیت اختصاص داده‌اند، از ۴۰ درصد در سال ۲۰۰۶ به ۵۵ درصد در سال ۲۰۰۸ افزایش داشته است. چنین نتایجی موجب شده است که در سازمان‌های امروزی، امنیت اطلاعات از اهمیت ویژه‌ای برخوردار شود.

موضوع امنیت اطلاعات[2] در سازمان‌ها، استفاده از سیستم‌های امنیت اطلاعات را با چالش ریسک مواجه کرده است. چنانچه فرایند مدیریت ریسک در این سیستم‌ها به‌درستی انجام شود، می‌توان به اجرای موفق آن دست یافت (نان، هری و مینکیانگ، ۲۰۱۴).

هر فعالیتی با ریسک و مخاطره همراه است و انسان‌ها از زمان‌های بسیار دور به این مفهوم پی برده‌اند و به‌دنبال شناسایی عوامل و منابع آن هستند. از این رو، مطالعات زیادی به‌منظور شناسایی و بررسی عوامل کلیدی مؤثر بر امنیت اطلاعات برای اجرای موفق آن، انجام گرفته است (نان و همکاران، ۲۰۱۴). مسئلهٔ دیگری که در محیط‌های سازمانی و تصمیم‌گیری امروز مطرح است، پیچیدگی وضعیت و ترکیب اطلاعات است که دستیابی به تصمیم‌های بهینه را مشکل می‌کند و دیگر قوانین سرانگشتی و بهترین حدس و گمان، کارساز نیست (لو و چن، ۲۰۱۲). از این رو به‌کارگیری روش‌های مدیریت و ارزیابی ریسک می‌تواند تأثیر شگرفی بر

1. Federal Bureau of Investigation (FBI)
2. INFOSEC

نحوهٔ سازماندهی فعالیت‌های سازمان‌ها در زمینهٔ امنیت اطلاعات داشته باشد. شناسایی مهم‌ترین ریسک‌های امنیت اطلاعات، گام اول فرایند مدیریت ریسک است و در تصمیم‌گیری‌های مدیریتی نقش اساسی برعهده دارد (هامب، فرانکویرا و ارلند،۲۰۱۰). نکتهٔ مهم اینکه قبل از شناسایی ریسک، تعیین میزان پیامدهای مثبت یا منفی آن امکان‌پذیر نیست و این به تنهایی یکی از عوامل مهم اجرای پروژه‌ها در وضعیت غیر قطعی و نامطمئن است. ریسک‌های معلوم، پس از شناسایی و تجزیه‌وتحلیل، هدایت‌پذیرند و می‌توان برای آنها برنامه‌ریزی کرد؛ در حالی‌که ریسک‌های پیش‌بینی‌نشده حتی با تکیه بر تجربهٔ مجریان و بهره‌مندی از رویکرد اقتضایی، مدیریت‌پذیر نیستند (جعفرنژاد و یوسفی زنوز، ۱۳۸۷).

به‌طور کلی مدیریت ریسک شامل سه گام اساسی شناسایی ریسک، ارزیابی ریسک و برنامه‌ریزی کاهش ریسک است. در شناسایی و تعیین میزان ریسک سیستم اطلاعاتی، مشکلاتی مانند نبود داده‌های آماری، موجب می‌شود مقادیر نادرستی برای ریسک سیستم اطلاعاتی، محاسبه شود. از این رو اغلب روش‌های ارزیابی ریسک برای سیستم‌های اطلاعاتی بر پایهٔ معیارهای کیفی بنا شده‌اند نه معیارهای کمی. با این حال، ارزیابی کیفی ریسک برای شناسایی ریسک‌ها تا حدودی ذهنی است. به همین دلیل برای کاهش ماهیت ذهنی معیارها به‌منظور ارزیابی کیفی ریسک، از روش فازی در تحقیقات استفاده می‌شود (لو و چن، ۲۰۱۲). روش فازی ابزاری مفید برای برخورد با ابهام در فرایند ارزیابی داده‌ها فراهم می‌کند.

هدف مدیریت امنیت اطلاعات هر سازمان، حفظ سرمایه‌های سازمان (نرم‌افزاری، سخت‌افزاری، اطلاعاتی و ارتباطی و نیروی انسانی) در برابر هرگونه تهدید (دسترسی غیر مجاز به اطلاعات، خطرهای ناشی از محیط و سیستم و خطرهای ایجادشده از سوی کاربران) است و برای دستیابی به این اهداف به برنامهٔ منسجمی نیاز دارد. مدیریت سیستم امنیت اطلاعات راهکاری برای رسیدن به این اهداف است (چین، تانگ، یانگ، وانگ و وانگ، ۲۰۰۹ و بارگس و ماتوس، ۲۰۰۵). مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که ضمن تعیین اهداف امنیت و بررسی موانع رسیدن به این اهداف، راهکارهایی را برای آن ارائه می‌دهد. همچنین مدیریت امنیت، وظیفهٔ پیاده‌سازی و کنترل عملکرد سیستم امنیت سازمان را بر عهده دارد و تلاش می‌کند سیستم را همیشه روزآمد نگه دارد. پژوهش‌های حوزهٔ امنیت اطلاعات بسیار گسترده است و روش‌های فنی، رفتاری، مدیریتی، فلسفی و سازمانی را شامل می‌شود که به حفاظت دارایی‌های اطلاعاتی موجود در سیستم‌های مبتنی بر رایانه و کاهش ریسک‌های آن می‌پردازد (کراسلر، جانستون، لوری، وارکنتین و باسکرویل، ۲۰۱۳). ریسک، جزء ذاتی و جدایی‌ناپذیر از زندگی و تجارت است. همواره وضعیت نامطمئنی که از اطلاعات و داده‌های

ناقص یا متغیرهای کنترل‌ناپذیر ناشی می‌شود با فرصت‌ها و تهدیدهایی همراه است. مدیریت ریسک فرایندی است برای درک ریسک‌های بالقوه و برنامه‌ریزی به‌منظور از بین بردن، کاهش اثر یا بهره‌برداری از این ریسک‌ها (چین و همکاران، ۲۰۰۹ و بارگس و ماتوس، ۲۰۰۵).

در این پژوهش تلاش شده است مدلی مبتنی بر استاندارد ایزو و چارچوب کوبیت ارائه شود که به شناسایی ریسک‌های امنیت اطلاعات سازمانی با روش دلفی فازی بپردازد.

پیشینهٔ نظری پژوهش

مفهوم ریسک

ریسک پروژه، رویدادها یا وضعیت‌هایی است که امکان وقوع نامعلومی دارند و در صورت وقوع، به‌صورت پیامدهای منفی یا مثبت بر اهداف پروژه تأثیر می‌گذارند. هر یک از این رویدادها یا وضعیت‌ها دلایل مشخصی دارد، اما پیش‌بینی نتایج و پیامدهای آن امکان‌پذیر است (جعفرنژاد و یوسفی‌زنوز، ۱۳۸۷).

مدیریت ریسک

مدیریت ریسک پروژه یکی از موضوعات عمدهٔ مدیریت پروژه است که برنامه‌ریزی، سازماندهی، پایش و کنترل تمام جنبه‌های پروژه را دربردارد و شامل شناسایی ریسک، اندازه‌گیری آن، توسعهٔ پاسخ ریسک و کنترل پاسخ ریسک است (جعفرنژاد و یوسفی‌زنوز، ۱۳۸۷). مدیریت ریسک فرایند شناسایی ریسک‌ها، ارزیابی ریسک و تلاش برای کاهش ریسک‌ها در سطح قابل قبول است (لو و چن، ۲۰۱۲).

امنیت اطلاعات سازمانی

موضوع امنیت اطلاعات از زمانی در کانون توجه قرار گرفت که مبحث امنیت فیزیکی مطرح شد و این دو موضوع با پشتیبانی از یکدیگر، به استخوان‌بندی کنترل امنیت شرکت‌ها می‌پردازند (مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، ۱۳۸۷). امنیت اطلاعات به حفاظت از اطلاعات و کمینه‌سازی خطر افشای اطلاعات در بخش‌های غیر مجاز اشاره دارد. امنیت اطلاعات به مجموعه‌ای از ابزارها اطلاق می‌شود که برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری به‌کار می‌روند و علم مطالعهٔ روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیر مجاز است. با توجه به تعاریفی که بیان شد، به‌طور کلی امنیت به مجموعه‌ای از تدابیر، روش‌ها و ابزارهایی گفته می‌شود که برای جلوگیری از دسترسی و تغییرات غیر مجاز در نظام‌های رایانه‌ای و ارتباطی به‌کار می‌رود (ملک‌الکلامی، ۱۳۹۲). با توجه

به گسترش استفاده از اینترنت، تبادلات اطلاعاتی و هزینه‌های صرف‌شده به‌منظور یکپارچگی اطلاعاتی، امروزه مبحث کنترل و مدیریت جابه‌جایی‌های اطلاعاتی و برخورداری از سامانهٔ جامعی برای مدیریت امنیت اطلاعات، بیش از پیش احساس می‌شود (سانگو، لی و کیم، ۲۰۰۷). امنیت اطلاعات مبحث بسیار مهمی است؛ زیرا هدف آن حفاظت کاربر در برابر تهدیدها و ریسک‌ها و دسترسی به اطلاعات امن، مطمئن و محرمانه است و برای اطمینان از امنیت آن، سازمان باید سیاست‌ها و خط‌مشی‌های امنیت اطلاعات را شناسایی و تبیین کند. با این حال، گاهی سازمان‌ها برای پیاده‌سازی سیاست‌های امنیت اطلاعات با شکست مواجه می‌شوند (یان، کینگ و لی، ۲۰۱۱).

مفهوم ریسک امنیت اطلاعات

به‌طور کلی اگر نقص در امنیت اطلاعات، پیامدهای منفی شایان توجهی برای سازمان، فرایندهای کسب‌وکار یا دارایی‌های در پی داشته باشد، سازمان با ریسک امنیت اطلاعات مواجه شده است و باید به شناسایی و ارزیابی ریسک‌ها بپردازد (مؤسسهٔ امنیت اطلاعات، ۲۰۰۸).

مدیریت امنیت اطلاعات

مدیریت امنیت اطلاعات، بخشی از مدیریت اطلاعات است که وظیفهٔ تعیین اهداف امنیت و بررسی موانع رسیدن به این اهداف و ارائهٔ راهکارهای لازم را بر عهده دارد.

با پیدایش اولین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵، نگرش نظام‌مند به مقولهٔ ایمن‌سازی فضای تبادل اطلاعات شکل گرفت (سانگو، لی و کیم ،۲۰۰۷). بر اساس این نگرش، امنیت فضای تبادل اطلاعات سازمان‌ها، با تکرار تأمین نمی‌شود، بلکه باید این کار به‌صورت مداوم طی چرخهٔ ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح انجام گیرد. برای این منظور باید هر سازمان براساس روش‌شناسی مشخص و برنامه‌ریزی‌شده‌ای به کنترل و نظارت بر اطلاعات و تبادلات اطلاعات در سازمان خود بپردازد (برادریک، ۲۰۰۶). مدیریت امنیت اطلاعات از طریق استانداردها و سامانه‌های مدیریتی امنیت اطلاعات در سازمان‌ها اجرا می‌شود (مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، ۱۳۸۷). هدف مدیریت امنیت اطلاعات در سازمان، حفظ سرمایه‌های سازمان (نرم‌افزاری، سخت‌افزاری، اطلاعاتی، ارتباطی و نیروی انسانی) در برابر هرگونه تهدید (شامل دسترسی غیر مجاز به اطلاعات، خطرهای ناشی از محیط و سامانه و خطرهای ایجادشده از سوی کاربران) است و برای رسیدن به این هدف، به برنامهٔ منسجمی نیاز دارد. فرایند سامانهٔ مدیریت امنیت اطلاعات به یک دورهٔ اقدام در نظام مدیریتی

خلاصه نمی‌شود، بلکه طی فرایندی دائمی در چرخهٔ ایمن‌سازی چهارمرحله‌ای به ثمر می‌رسد. این چهار مرحله عبارت‌اند از (مؤسسهٔ امنیت اطلاعات، ۲۰۰۵):

۱. برنامه‌ریزی: برپایی شرایط اولیهٔ سامانهٔ مدیریت امنیت اطلاعات؛

۲. اجرا: پیاده‌سازی و اجرای سامانهٔ مدیریت امنیت اطلاعات؛

۳. ارزیابی و کنترل: فعالیت‌های نظارتی یا بررسی فعالیت‌های انجام گرفته؛

۴. بهبود و اصلاح: فعالیت‌های نگهداری و بهبود مستمر در این سامانهٔ مدیریتی.

قوانین و استانداردهای امنیت اطلاعات

سیستم‌های متعددی در کشورهای گوناگون برای ایجاد امنیت اطلاعات سازمانی تدوین و پیشنهاد شده است. در کشور آمریکا، سیستم‌های امنیت اطلاعات سازمانی از استاندارد خاصی پیروی نمی‌کنند و دولت استاندارد خاصی را برای آن اجبار نکرده است. مؤسسه‌ها نیز با در نظر گرفتن نوع تجارت، از یک‌سری کنترل‌ها و فرایندهای امنیتی تبعیت می‌کنند. فقط مؤسسهٔ استاندارد و فناوری آمریکا (NIST)[1] استانداردهایی را برای امنیت در حوزه‌های گوناگون پیشنهاد کرده است (میراسکندری، ۱۳۸۹). دو سندی که در بحث امنیت اطلاعاتِ این پژوهش در کانون توجه قرار دارد، دستورالعمل معمول مدیریت امنیت اطلاعات یا ایزو، ۲۷۰۰۲ و کنترل اهداف فناوری اطلاعات است که کوبیت[2] نامیده می‌شود و بخش DS۵ آن به‌طور خاص به مبحث امنیت اطلاعات می‌پردازد (در بخش‌های بعدی این دو استاندارد پس از معرفی، مقایسه خواهد شد). در واقع این دو سند یکدیگر را تکمیل می‌کنند و به‌منزلهٔ چارچوب‌های مرجع امنیت اطلاعات، دو انتخاب بسیار خوب هستند. کاربرد این دو با هم سبب هم‌افزایی می‌شود و برای شرکت‌ها بسیار مفید خواهد بود (یان،کینگ و لی، ۲۰۱۱).

ایزو/آی. ایی. سی. ۲۷۰۰۲[3]

در ماه مه سال ۱۹۸۷، همزمان با پایه‌گذاری مرکز امنیت تجارت کامپیوتری (CCSC)[4] وابسته به دفتر تجارت و صنعت انگلستان، استاندارد بی. اس. ۷۷۹۹ تنظیم شد. این استاندارد طی سال‌ها تغییر یافت و سرانجام در سال ۲۰۰۷ با نام ایزو آی. ایی. سی. ۲۷۰۰۲ معرفی شد (ملک‌الکلامی، ۱۳۹۲).

---

1. National Institute of Standards and Technology
2. Cobit
3. ISO/IEC 27002
4. Computer Commerce Security center (CCSC)

اهداف کنترلی و کنترل‌های این استاندارد برای برآورده‌کردن الزامات شناسایی ورودی، از طریق ارزیابی خطر پیاده‌سازی می‌شود. این استاندارد که ممکن است به‌مثابهٔ رهنمود پیاده‌سازی توسعهٔ استانداردهای امنیت سازمانی، تجارب مدیریت امنیت اثربخش و کمک به ایجاد اطمینان در فعالیت‌های درون سازمانی به‌کار رود، از کنترل‌های امنیتی بسیار جامعی در ۱۱ دامنه (بند) برخوردار است که این ۱۱ دامنه، مبنای ارزیابی مخاطرات امنیتی و گسترش امنیت در نظر گرفته می‌شوند. دامنه‌های اشاره شده عبارت‌اند از: ۱. سیاست‌های امنیتی؛ ۲. ساختار مدیریت امنیت اطلاعات؛ ۳. مدیریت امنیت اموال سازمان؛ ۴. مدیریت امنیت منابع انسانی؛ ۵. مدیریت امنیت فیزیکی و محیطی؛ ۶. مدیریت عملیات و ارتباطات؛ ۷. کنترل دسترسی‌ها و اکتساب؛ ۸. توسعه، حفظ و نگهداری نظام‌های اطلاعاتی؛ ۹. مدیریت بحران امنیت اطلاعات؛ ۱۰. مدیریت استمرار کسب‌وکار؛ ۱۱. تطابق با قانون. هر بند از تعدادی طبقهٔ امنیتی عمده شکل گرفته است. در کل این ۱۱ بند در ۳۹ طبقهٔ اصلی امنیتی و ۱ بند مقدماتی برآورد و برطرف‌سازی ریسک تدوین شده است (مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، ۱۳۸۷).

کوبیت، کنترل اهداف فناوری اطلاعات

کوبیت چارچوبی است که به‌منظور کنترل عملکرد فناوری اطلاعات طراحی شده است. بنیاد کنترل و حسابرسی سیستم‌های اطلاعاتی یا مؤسسه تحقیقاتیِ انجمن کنترل و حسابرسی سیستم‌های اطلاعاتی، این چارچوب را توسعه داده است. کوبیت ۴/۱ در سال ۲۰۰۷ انتشار یافت. چارچوب کوبیت الگوی فرایندی در سطح بالاست که دامنهٔ وسیعی از فعالیت‌های فناوری اطلاعات را در ۳۴ فرایند و ساختاری واحد برای اجرا و فهم سازماندهی می‌کند و ارزیابی عملکرد، خطرها و قابلیت‌های فناوری اطلاعات با هدف ابتداییِ برآورده‌ساختن نیازهای کاری را فراهم می‌کند (میربها، ۲۰۰۷ و غضنفری، فتحیان و رئیس صفری، ۱۳۸۷). دامنه‌های کنترل اهداف در DS۵ (DS۵: اطمینان از امنیت سیستم) کوبیت عبارت‌اند از: DS۵/۱: مدیریت امنیت فناوری اطلاعات؛ DS۵/۲: طراحی امنیت فناوری اطلاعات؛ DS۵/۳: مدیریت شناسایی؛ DS۵/۴: مدیریت حساب کاربری؛ DS۵/۵: آزمون امنیت، نظارت و مانیتورینگ؛ DS۵/۶: شناسایی حوادث امنیتی؛ DS۵/۷: حفاظت از امنیت فناوری؛ DS۵/۸: مدیریت کلیدی رمزنگاری؛ DS۵/۹: تشخیص، تصحیحو پیشگیری از نرم‌افزارهای مخرب (ویروس‌ها، کرم‌ها، اسپم و...)؛ DS۵/۱۰: امنیت شبکه؛ DS۵/۱۱: تبادل اطلاعات حساس (مؤسسهٔ حاکمیت اطلاعات، ۲۰۰۷).

کوبیت چارچوبی برای حاکمیت فناوری اطلاعات است، به بحث امنیت اطلاعات محدود نمی‌شود و در میان بسیاری از مسائل دیگر، به امنیت اطلاعات نیز اشاره می‌کند. مزیت استفاده از کوبیت به مثابهٔ چارچوب امنیت اطلاعات، «تلفیق و یکپارچگی» امنیت با حوزهٔ گسترده‌تر در

فناوری اطلاعات است. بهره‌مندی از کوبیت در امنیت اطلاعات خالی از ایراد نیست، کوبیت جزئیات و «چگونگی» انجام امور را در نظر نمی‌گیرد و بیشتر به این می‌پردازد که چه کاری باید انجام شود. کوبیت چارچوبی است که اغلب حسابرسان آن را به‌کار می‌برند و در مواقع بسیاری مدیران ریسک IT آن را چارچوب انتخاب‌شده و ترجیحی سازمان در نظر گرفته‌اند. استاندارد ایزو فقط به امنیت اطلاعات محدود می‌شود و فقط به این حوزه می‌پردازد. ایزو بیشتر از کوبیت به جزئیات و چگونگی انجام امور پرداخته است و بیشتر رویکرد «فنی و تکنیکی» دارد، در حالی‌که کوبیت رویکرد کلان و مدیریتی را در پیش می‌گیرد (یان و همکاران، ۲۰۱۱). کوبیت با گسترش نقش خود به‌عنوان ابزار حاکمیت IT و نه فقط ابزاری برای حسابرسی، می‌تواند در سطحی استراتژیک به بیان «چیستی» امنیت اطلاعات بپردازد، اما ایزو می‌تواند در سطح پایین‌تر و برای مشخص‌کردن «چگونگی» امنیت اطلاعات به‌کار رود. اغلب برای استفادهٔ بهتر از این دو سند (کوبیت DS۵ و ایزو) و به‌منظور انطباق اهداف کنترل DS۵ و مقیاس‌های اندازه‌گیری مبتنی بر ایزو، به هماهنگ‌سازی میان این دو نیاز است.

روش دلفی و دلفی فازی

نخستین‌بار دالکی و هولمر (۱۹۶۳) روش سنتی دلفی را در شرکتی توسعه دادند و پس از آن به‌شکل گسترده‌ای در بسیاری از حوزه‌های مدیریت به‌کار گرفته شد. دلفی روش بررسی نظرهای کارشناسان با سه مشخصهٔ پاسخ بی‌نام، تکرار و بازخورد کنترل‌شده و در نهایت پاسخ گروهی آماری است. روش دلفی، روش نظام‌مند جمع‌آوری و هماهنگی قضاوت‌های آگاهانهٔ گروهی از متخصصان دربارهٔ سؤال یا موضوعی خاص است. دلفی هم روش پژوهش و هم نوعی روش جمع‌آوری اطلاعات به‌شمار می‌رود. همهٔ دلفی‌ها از ویژگی‌های مشترک زیر برخوردارند:

۱. از پانل متخصصان برای جمع‌آوری داده‌ها استفاده می‌کنند؛
۲. به‌صورت نوشتاری انجام می‌شوند؛
۳. می‌کوشند تا دربارهٔ هر ایده به اجماع و توافق نظر برسند؛
۴. گمنام‌ماندن متخصصان را تضمین می‌کنند؛
۵. از بازگویی و بازخورد کنترل‌شده برای رسیدن به همگرایی یا مشخص‌سازی واگرایی در نظرها استفاده می‌کنند؛
۶. به مشارکت‌کنندگان اجازه می‌دهند که پس از خواندن نظرهای همکاران، نظرهای خود را بازنگری کنند.

به هر حال، روش دلفی همچنان در مرحلهٔ تکامل است. یکی از مزیت‌های روش دلفی، سادگی آن است؛ زیرا به مهارت‌های پیشرفتهٔ ریاضی، اجرا و تحلیل نیاز ندارد، بلکه نیازمند فردی

آگاه از مسائل و تکنولوژی دلفی و خلاقیت در طراحی پروژه است (صنایعی، قاضی‌فرد و سبحان‌منش،۱۳۹۰). این روش، همیشه از نظرهای کارشناسی با همگرایی پایین و هزینهٔ اجرایی بالا زیاد دیده است. همچنین احتمال دارد سازمان‌دهندگان ایده، نظرهای کارشناسانهٔ ویژه‌ای را حذف کنند. از این رو مری، پیپینو و گیگچ (۱۹۸۵) مفهوم تلفیق روش سنتی دلفی و نظریهٔ فازی را به‌منظور رفع ابهام و ناهمخوانی روش دلفی ارائه کردند. روش دلفی فازی به‌منظور غربال عوامل نامناسب و اجتناب از تأثیر مقادیر انتهایی، میانگین هندسی را مبنای گروه تصمیم‌گیرنده قرار می‌دهد. همچنین علاوه‌بر کاهش هزینه و زمان، این روش به تصمیم‌گیرندگان امکان ارزیابی فازی‌بودن فرایند تصمیم‌گیری و دستیابی به نتیجهٔ بهتر در انتخاب عامل را می‌دهد (صنایعی و همکاران، ۱۳۹۰). در روش دلفی فازی، اطلاعات در قالب زبان نوشتاری از خبرگان دریافت‌شده و به‌صورت فازی تحلیل می‌شود (یان و چن، ۲۰۱۲). در پژوهش حاضر برای انتخاب خبرگان و متخصصان معیارهای زیر در نظر گرفته شده است:

۱. دانش و تجربه در موضوع (مدرک تحصیلی حداقل کارشناسی و دو سال تجربهٔ کار در زمینهٔ مد نظر)؛
۲. تمایل و زمان کافی برای همکاری در پژوهش؛
۳. مهارت‌های ارتباطی مؤثر.

الگوریتم اجرای روش دلفی فازی در شکل ۱ نمایش داده شده است.

شکل ۱. الگوریتم اجرای روش دلفی فازی

پیشینهٔ تجربی

از اواسط دههٔ نود، پژوهش‌های بسیاری به ارائهٔ راهکارهای مؤثر برای محافظت و ایمن‌سازی اطلاعات، چه در ابعاد فنی و چه مدیریتی در داخل و خارج ایران پرداخته‌اند که اغلب بر شناسایی ریسک توجه ویژه‌ای داشته‌اند و آن را اولین و شاید مهم‌ترین گام در مدیریت ریسک دانسته‌اند. در ادامه به برخی از آنها اشاره می‌شود.

یزدی (۱۳۸۸) دربارهٔ اهمیت و لزوم سیستم مدیریت امنیت اطلاعات در تجربه‌های الکترونیک سازمان گمرک بوشهر بر این نکته تأکید کرد که برای پیاده‌سازی امنیت، تنها توجه به مسائل تکنیکی کافی نیست، بلکه ایجاد سیاست‌های کنترلی و استانداردسازی آن نیز حائز اهمیت است. بیگلریگیان (۱۳۹۱) در پژوهشی به تدوین شاخص‌های ارزیابی امنیت اطلاعات سازمان بورس و اوراق بهادار تهران پرداخت. شهریوری (۱۳۹۰) مدلی برای بررسی بلوغ حاکمیت بر امنیت اطلاعات در حوزهٔ مدیریت زنجیرهٔ تأمین ارائه کرد. کریمی (۱۳۸۵) در پژوهشی با هدف ارائهٔ مدل مفهومی برای ارزیابی ریسک امنیت اطلاعات در سازمان‌ها (بانک سپه)، به مرور ادبیات امنیت اطلاعات پرداخت. وی پس از مرور ادبیات امنیت اطلاعات در زمینهٔ قوانین و استانداردها و برنامه‌های امنیت اطلاعات و استفاده از راهنمای خودارزیابی ریسک امنیت اطلاعات به‌منزلهٔ مبنا، اجزای سازندهٔ برنامهٔ امنیت اطلاعات و مدل ارزیابی ریسک امنیت اطلاعات را در قالب چارچوب مفهومی ارائه کرد. عیسوی (۱۳۹۰) در پژوهشی، ریسک عملیاتی امنیت اطلاعات را در سامانهٔ بانکداری مدرن بررسی کرد و راهکارهایی برای کاهش آن ارائه داد. امنیت اطلاعات برای سازمان‌های مالی که اطلاعات مشتری را در اختیار دارند، از اهمیت ویژه‌ای برخوردار است و برای جلب رضایت مشتری، این اطلاعات باید دور از دسترس دیگران باشد. سازمان‌ها هر روز در معامله‌ها و دادوستدها، چندین‌بار از اطلاعات مشتریان استفاده می‌کنند. این مبادله‌ها انواع گوناگونی از ریسک را به‌دنبال دارند که در این پژوهش به ریسک‌های عملیاتی توجه شده است. در پژوهشی دیگر، جمالی و هاشمی (۱۳۹۰) با استفاده از روش دیماتل فازی به شناسایی و سنجش روابط عوامل مؤثر بر ریسک پروژه‌های فناوری اطلاعات در بانک ملت استان بوشهر پرداختند.

اولین چارسوقی و همکارانش در مقاله‌ای با عنوان «ارزیابی ریسک امنیت اطلاعات با استفاده از شبکه‌های عصبی مصنوعی» به ارزیابی ریسکِ سیستم مدیریت امنیت اطلاعات پرداختند (اولین چهارسوقی، دوستاری، یزدیان ورجانی و مهدوی اردستانی، ۱۳۹۲).

تقوا و ایزدی (۱۳۹۲) در مقاله‌ای با عنوان «بررسی امنیت در سیستم‌های امنیتی توسعه‌یافته با روش معماری سرویس‌گرا» به بررسی ابعاد مختلف امنیتی و ارائهٔ راهکارهایی برای امنیت در

سیستم‌های اطلاعاتی با معماری سرویس‌گرا پرداختند. در این مطالعه، مهم‌ترین شاخص‌ها و مهم‌ترین ابعاد امنیتی و زیرابعاد هریک، پس از شناسایی به‌ترتیب اهمیت اولویت‌بندی شدند (تقوا و ایزدی، ۱۳۹۲).

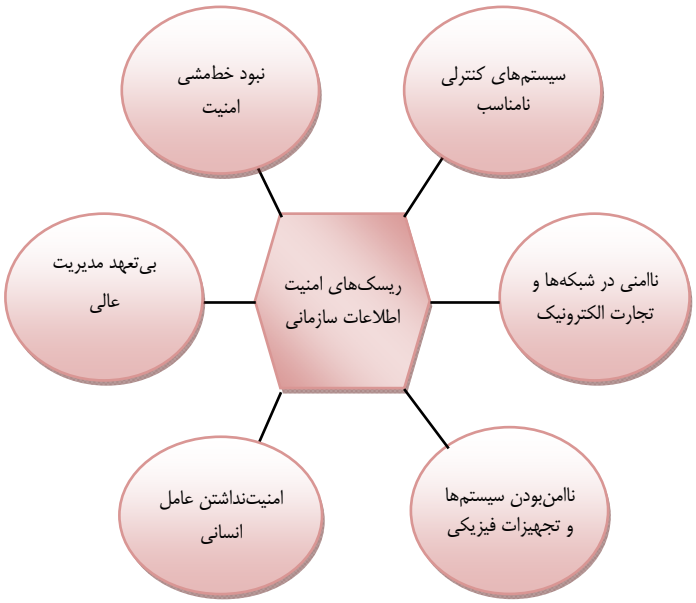
گوردون و لوئب (۲۰۰۲) با رویکردی کمی، مدلی ریاضی برای تعیین میزان سرمایه‌گذاری بهینه در امنیت برای سیستم‌های اطلاعاتی ارائه کردند (نان، هری و مینکیانگ، ۲۰۱۴). یو و همکارانش این مطالعات را با حل و فرموله‌کردن مسئله و با توجه به پارادایم مدیریت ریسک گسترش دادند. این پژوهش بینش‌های تازه‌ای برای کمک به مدیران در تصمیم‌گیری مطلوب ایجاد کرد (یو، کاکانیلدریم، ریو و لیو، ۲۰۰۷). وو و همکارانش، چالش‌ها و ریسک‌های مختلف توسعهٔ محصول را با مهندسی همزمان محیط یافتند و رویکردی کمی برای شناسایی سیستماتیک مهم‌ترین ریسک‌های انجام مهندسی همزمان پروژه‌ها پیشنهاد کردند (ژِی، چن و گویی، ۲۰۱۰).

محمد صالح و عبدالقادر الفندوخ (۲۰۱۱) چارچوبی برای مدیریت ریسک امنیت اطلاعات ارائه کردند. این چارچوب شامل دو بعد ساختاری و دو بعد رویه‌ای است. حوزه و معیارهای ارزیابی، ابعاد ساختاری در نظر گرفته شدند و روند و ابزار ارزیابی، ابعاد رویه‌ای چارچوب‌اند. این چارچوب با دیدی جامع، دربرگیرندهٔ استراتژی، فناوری، سازمان، مردم و محیط برای دامنهٔ ISRM است و معیارهای ارزیابی آن از استانداردهای گوناگون استخراج شده است. در ابعاد رویه‌ای این چارچوب برای فرایند ISRM، ضمن بهره‌گیری از چرخهٔ شش‌سیگما (تعریف، اندازه‌گیری، تجزیه‌وتحلیل، بهبود و کنترل) از ابزارهای گوناگونی استفاده شده است.

وو و اولسون (۲۰۱۰)، خلاصه‌ای از مجموعهٔ مدل‌های ریسک در صنعت خدمات مالی را بیان کردند و ابزاری مؤثری برای کاهش این‌گونه ریسک‌ها از طریق پیش‌بینی کارت‌های امتیاز پیشنهاد دادند (نان، هری و مینکیانگ، ۲۰۱۴).

مدل مفهومی پژوهش

با توجه به بررسی استاندارد ایزو و چارچوب کوبیت، پژوهش‌های گذشته و مصاحبه با کارشناسان، از میان عوامل متعدد مرتبط با امنیت اطلاعات، بر ۲۳ ریسک تأکید شده است که در شش گروه نبود خط‌مشی امنیت، بی‌تعهدی مدیریت عالی، امنیت‌نداشتن عامل انسانی، ناامنی سیستم‌ها و تجهیزات فیزیکی، ناامنی شبکه‌ها و تجارت الکترونیک و سیستم‌های کنترلی نامناسب، تقسیم‌بندی شدند. شکل ۲ اجزای مدل مفهومی این پژوهش را نشان می‌دهد.



شکل ۲. اجزای مدل مفهومی پژوهش

منبع: مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، ۱۳۸۷

روش‌شناسی پژوهش

بر اساس طرح پژوهش و از دید نحوهٔ گردآوری داده‌ها، پژوهش حاضر از نـوع توصـیفی اسـت و برای گردآوری اطلاعات سه روش مطالعهٔ اسنادی، دلفی فازی و پیمایشی را به‌کار برده است.

اطلاعات خبرگان به‌کمک پرسشنامه جمع‌آوری شده است. در پرسشنامهٔ این پژوهش کـه بـا هدف کسب نظر خبرگان دربارهٔ ریسک‌های امنیت اطلاعات سازمانی طراحی شده است، از میان عوامل امنیت اطلاعات استاندارد ایزو ۲۷۰۰۲ و بخش DS۵ چارچوب کوبیـت ۴ و نیـز، بررسـی مطالعات گذشته، ۵۵ ریسک امنیتی استخراج شد که سرانجام در قالـب ۲۳ ریسـک امنیتـی و در شش گروه اصلی جای گرفت. در این پرسشنامه، هر یک از خبرگان نظـر خـود را دربـارهٔ میـزان ریسک تک‌تک عوامل برای امنیت اطلاعات در طیف پنج‌گانهٔ لیکرت از طریق متغیرهای کلامی (خیلی کم، کم، متوسط، زیاد و خیلی زیاد) و با رویکردی فازی ابراز کردند. متغیرهای مـذکور بـا توجه به جدول ۱ به شکل اعداد فازی مثلثی تعریف شده‌اند.

گفتنی است روایی محتوایی، صوری و پایایی پرسشنامه پس از بررسی به تأیید رسیده است.

جدول ۱. اعداد فازی مثلثی متغیرهای کلامی

متغیرهای کلامی	عدد فازی مثلثی	عدد فازی قطعی‌شده
خیلی‌زیاد	(۰/۷۵ , ۱, ۱)	۰/۷۵
زیاد	(۰/۵ , ۰/۷۵ ,۱)	۰/۵۶۲۵
متوسط	(۰/۲۵ , ۰/۵ , ۰/۷۵)	۰/۳۱۲۵
کم	(۰, ۰/۲۵ , ۰/۵)	۰/۰۶۲۵
خیلی‌کم	(۰, ۰, ۰/۲۵)	۰/۰۶۲۵

در جدول ۱، اعداد فازی قطعی‌شده با استفاده از رابطهٔ مینکووسکی بـه شـکل زیـر محاسـبه شده‌اند:

رابطهٔ ۱) $$\chi = \mathrm{m} + \frac{\beta - \alpha}{4}$$

یافته‌های پژوهش

برای استخراج عوامل، علاوه‌بر بهره‌مندی از ادبیات پژوهش، معیارهای امنیت اطلاعات استاندارد ایزو ۲۷۰۰۲ و بخش DS5 چارچوب کوبیت ۴، از روش دلفی فازی طی مراحل زیر استفاده شـده است.

نظرسنجی مرحلهٔ نخست

در این مرحله، پرسشنامه‌ای شامل ۲۳ معیار امنیت اطلاعات در اختیار اعضای گـروه خبـره قـرار گرفت و از آنها درخواست شد نظرشان را دربارهٔ هر معیار در قالب متغیرهـای کلامـی منـدرج در پرسشنامه بیان کنند.

با توجه به نتایج به‌دست آمده از پرسشـنامهٔ مرحلـهٔ اول و بـا اسـتفاده از رابطـه‌هـای ۲ و ۳، میانگین فازی هر یک از مؤلفه‌ها به‌دست آمد (جدول ۲).

رابطهٔ ۲) $$\left(a_1^i, a_2^i, a_3^i\right) \quad i = 1,2,3, \dots n = A_i$$

در این رابطه A_i بیانگر دیدگاه خبرهٔ iام و n تعداد خبرگان است.

رابطهٔ ۳) $$A_{ave} = (m_1, m_2, m_3) = (\frac{1}{n}\sum_{i=1}^{n} a_1^i \,, \frac{1}{n}\sum_{i=1}^{n} a_2^i \,, \frac{1}{n}\sum_{i=1}^{n} a_3^i)$$

در این رابطه A_{ave} میانگین نظر خبرگان است.

جدول ۲. میانگین دیدگاه‌های خبرگان پس از نظرسنجی نخست

	مؤلفه‌ها	میانگین فازی مثلثی (m, α, β)			میانگین فازی‌زدایی شده (χ)
۱-۱	نبود خط‌مشی امنیت اطلاعات جامع و کامل و قابل بازنگری	(۰/۹۸	۰/۸۸	۰/۶۳)	۰/۶۵
۱-۲	ناهماهنگی بخش‌های گوناگون بانک، در زمینهٔ فعالیت‌های امنیت اطلاعات	(۰/۵۵	۰/۳۰	۰/۰۵)	۰/۱۱
۱-۳	روشن‌نبودن تعریف مسئولیت امنیت اطلاعات در بانک	(۰/۹۸	۰/۷۸	۰/۵۳)	۰/۵۸
۱-۴	به‌کارنبردن رویه‌ای مناسب در طبقه‌بندی وکدگذاری اطلاعات	(۰/۸۳	۰/۶۵	۰/۴۰)	۰/۴۴
۱-۵	ناهماهنگی سیستم‌ها با خط مشی‌ها و استانداردهای امنیتی بانک	(۰/۹۰	۰/۷۰	۰/۴۵)	۰/۵۰
۱-۶	همراستا نبودن فعالیت‌های امنیتی با نیازمندی‌های کسب‌وکار در بانک	(۰/۵۸	۰/۳۳	۰/۰۸)	۰/۱۴
۱-۷	مدیریت نادرست حوادث و ضعف‌های امنیت اطلاعات	(۰/۸۸	۰/۷۳	۰/۴۸)	۰/۵۱
۲-۱	بی‌تعهدی و حمایت‌نکردن مدیریت بانک دربارهٔ امنیت اطلاعات بانک	(۰/۹۵	۰/۸۳	۰/۵۸)	۰/۶۱
۲-۲	تخصیص بودجهٔ نامناسب به طرح امنیت	(۰/۹۸	۰/۸۰	۰/۵۵)	۰/۵۹
۲-۳	بی‌توجهی در زمان‌بندیِ پیاده‌سازی و اجرایی‌کردن طرح‌ها	(۰/۹۵	۰/۸۰	۰/۵۵)	۰/۵۹
۲-۴	بی‌بهرگی از طرح کلی برای امنیت اطلاعات و سرمایه‌گذاری‌های مناسب و متناسب با اولویت‌های امنیتی بانک	(۰/۹۵	۰/۸۵	۰/۶۰)	۰/۶۳
۳-۱	بهره‌نبردن از نیروی انسانی متخصص در زمینهٔ امنیت اطلاعات	(۰/۹۸	۰/۹۳	۰/۶۳)	۰/۶۹
۳-۲	ناآگاهی از امنیت اطلاعات و بی‌توجهی به آموزش آن	(۰/۹۰	۰/۷۵	۰/۵۰)	۰/۵۴
۴-۱	مشخص‌نبودن راهی برای دسترسی‌های مناسب	(۰/۹۵	۰/۷۸	۰/۵۳)	۰/۵۷
۴-۲	ناامن‌بودن تجهیزات در برابر حوادث طبیعی و مصنوعی (نداشتن برق اضطراری، UPS و...)	(۰/۵۰	۰/۲۵	۰/۰۸)	۰/۱۴
۵-۱	ناامن‌بودن خدمات شبکه	(۰/۹۸	۰/۸۸	۰/۶۳)	۰/۶۵
۵-۲	ناامن‌بودن فرایند تبادل اطلاعات و نرم‌افزارها در بانک یا خارج از بانک	(۰/۷۸	۰/۵۵	۰/۳۰)	۰/۳۶

ادامهٔ جدول ۲

	مؤلفه‌ها	میانگین فازی مثلثی (m, α, β)			میانگین فازی‌زدایی شده (χ)
۳-۵	نـاامن‌بـودن خـدمات تجـارت الکترونیکـی، شـامل دادوستدهای آنلاین و اطلاعات در دسترس عموم	(۰/۹۵	۰/۸۳	۰/۵۸)	۰/۶۱
۴-۵	نبود نسخهٔ پشتیبان و ناهماهنگی و دسـترس‌پـذیری اطلاعات و امکانات پردازش اطلاعات	(۰/۹۵	۰/۸۳	۰/۵۸)	۰/۶۱
۱-۶	کنترل‌نکردن صحت داده‌های ورودی، پـردازش‌هـای درونی، یکپارچگی پیغام و صحت داده‌های خروجی	(۰/۸۵	۰/۷۰	۰/۲۵)	۰/۲۹
۲-۶	توسعهٔ نرم‌افزارهای برون‌سپاری‌شـده بـدون پـایش و نظارت	(۰/۶۵	۰/۴۰	۰/۴۵)	۰/۵۱
۳-۶	گزارش‌نکردن رویدادها و ضعف‌های امنیتی	(۰/۸۸	۰/۶۳	۰/۳۸)	۰/۴۴
۴-۶	به‌کارنبردن اقدامات پیشگیرانه، اکتشـافی و اصـلاحی (به‌روزرسانی نرم‌افزارهای امنیتـی) بـرای حفاظـت از سیستم اطلاعات بانک از نرم‌افزارهای مخرب	(۰/۹۸	۰/۸۵	۰/۶۸)	۰/۷۱

در جدول ۲ میانگین فازی مثلثی و عملیات فازی‌زدایی، به‌ترتیب از طریق رابطهٔ ۳ و رابطهٔ ۱ محاسبه شده است.

نظرسنجی مرحلهٔ دوم

همان‌گونه که جدول ۳ نشان مـی‌دهـد، بیشـترین توافـق نظـر خبرگـان دربـارهٔ میـزان ریسـک محسوب‌شدن معیارها، به ریسک «بهـره‌نبـردن از نیـروی انسـانی متخصـص در زمینـهٔ امنیـت اطلاعات» اختصاص دارد و کمترین توافق نظر به معیار «همراستانبودن فعالیت‌هـای امنیتـی بـا نیازمندی‌های کسب‌وکار در بانک» تعلق دارد.

براساس نظر چنگ لین و همکارانش، چنانچه اختلاف بین دو مرحلهٔ نظرسنجی کمتر از حـد آستانهٔ خیلی کم (۰/۱) باشد، فرایند نظرسنجی متوقف می‌شود (چنگ چین، هسو و لـین، ۲۰۰۲). بنابراین در مرحلهٔ دوم نظرسنجی، نظرهای قبلی هر خبره و میزان اختلاف آنها بـا دیـدگاه سـایر خبرگان، همراه با پرسشنامه‌ای بار دیگر برای اعضای گروه خبره ارسال شد.

نتایج شمارش پاسخ‌های ارائه‌شده در مرحلهٔ دوم، همانند مرحلهٔ اول به‌کمک رابطه‌هـای ۱ و ۳ تحلیل شد که نتایج آن در جدول ۳ مشاهده می‌شود. همچنـین در جـدول ۳، میـزان اخـتلاف مرحله‌های اول و دوم نیز مشخص شده است.

جدول ۳. میانگین دیدگاه‌های خبرگان پس از نظرسنجی دوم

	مؤلفه‌ها	میانگین فازی مثلثی (m,α,β)			میانگین فازی‌زدایی شدهٔ (χ) مرحلهٔ دوم	اختلاف مرحلهٔ اول و دوم
۱-۱	نبود خط‌مشی امنیت اطلاعات جامع و کامل و قابل بازنگری	(۰/۹۳)	۰/۷۸	(۰/۷۰	۰/۷۴	۰/۰۹
۱-۲	ناهماهنگی بخش‌های گوناگون بانک، در زمینهٔ فعالیت‌های امنیت اطلاعات	(۰/۴۳)	۰/۱۸	(۰/۱۰	۰/۱۶	۰/۰۵
۱-۳	روشن‌نبودن تعریف مسئولیت امنیت اطلاعات در بانک	(۰/۹۵)	۰/۷۳	(۰/۵۸	۰/۶۳	۰/۰۵
۱-۴	به‌کارنبردن رویه‌ای مناسب در طبقه‌بندی وکدگذاری اطلاعات	(۰/۸۵)	۰/۶۳	(۰/۴۸	۰/۵۳	۰/۰۹
۱-۵	ناهماهنگی سیستم‌ها با خط مشی‌ها و استانداردهای امنیتی بانک	(۰/۹۵)	۰/۷۰	(۰/۵۳	۰/۵۹	۰/۰۹
۱-۶	همراستا نبودن فعالیت‌های امنیتی با نیازمندی‌های کسب‌وکار در بانک	(۰/۴۰)	۰/۱۵	(۰/۱۵	۰/۲۱	۰/۰۸
۱-۱۷	مدیریت نادرست حوادث و ضعف‌های امنیت اطلاعات	(۰/۷۸)	۰/۶۰	(۰/۵۰	۰/۵۴	۰/۰۳
۲-۱	بی‌تعهدی و حمایت‌نکردن مدیریت بانک دربارهٔ امنیت اطلاعات بانک	(۰/۹۳)	۰/۷۵	(۰/۶۵	۰/۶۹	۰/۰۹
۲-۲	تخصیص بودجهٔ نامناسب به طرح امنیت	(۰/۹۰)	۰/۷۳	(۰/۶۳	۰/۶۷	۰/۰۸
۲-۳	بی‌توجهی در زمان‌بندیِ پیاده‌سازی و اجرایی‌کردن طرح‌ها	(۰/۹۰)	۰/۷۰	(۰/۶۳	۰/۶۸	۰/۰۹
۲-۴	بی‌بهرگی از طرح کلی برای امنیت اطلاعات و سرمایه‌گذاری‌های مناسب و متناسب با اولویت‌های امنیتی بانک	(۰/۹۵)	۰/۸۳	(۰/۷۸	۰/۸۱	۰/۱۸
۳-۱	بهره‌نبردن از نیروی انسانی متخصص در زمینهٔ امنیت اطلاعات	(۰/۸۸)	۰/۷۸	(۰/۷۵	۰/۷۸	۰/۰۹
۳-۲	ناآگاهی از امنیت اطلاعات و بی‌توجهی به آموزش آن	(۰/۹۳)	۰/۷۸	(۰/۷۰	۰/۷۴	۰/۲۰
۴-۱	مشخص‌نبودن راهی برای دسترسی‌های مناسب	(۰/۹۵)	۰/۷۳	(۰/۶۵	۰/۷۱	۰/۱۴
۴-۲	ناامن‌بودن تجهیزات در برابر حوادث طبیعی و مصنوعی (نداشتن برق اضطراری، UPS و...)	(۰/۴۳)	۰/۱۸	(۰/۱۳	۰/۱۹	۰/۰۵
۵-۱	ناامن‌بودن خدمات شبکه	(۰/۹۰)	۰/۷۵	(۰/۶۸	۰/۷۱	۰/۰۶

ادامهٔ جدول ۳

	مؤلفه‌ها	میانگین فازی مثلثی (m, α, β)			میانگین فازی‌زدایی شدهٔ (χ) مرحلهٔ دوم	اختلاف مرحلهٔ اول و دوم
۵-۲	ناامن‌بودن فرایند تبادل اطلاعات و نرم‌افزارها در بانک یا خارج از بانک	(۰/۷۵	۰/۵۳	۰/۳۸)	۰/۴۳	۰/۰۸
۵-۳	ناامن‌بودن خدمات تجارت الکترونیکی، شامل دادوستدهای آنلاین و اطلاعات در دسترس عموم	(۰/۸۸	۰/۷۳	۰/۶۵)	۰/۶۹	۰/۰۸
۵-۴	نبود نسخهٔ پشتیبان و ناهماهنگی و دسترس‌پذیری اطلاعات و امکانات پردازش اطلاعات	(۰/۸۸	۰/۷۳	۰/۶۵)	۰/۶۹	۰/۰۸
۶-۱	کنترل‌نکردن صحت داده‌های ورودی، پردازش‌های درونی، یکپارچگی پیغام و صحت داده‌های خروجی	(۱/۰	۰/۸۸	۰/۸۳)	۰/۸۶	۰/۵۷
۶-۲	توسعهٔ نرم‌افزارهای برون‌سپاری‌شده بدون پایش و نظارت	(۰/۸۵	۰/۶۵	۰/۵۳)	۰/۵۸	۰/۰۶
۶-۳	گزارش‌نکردن رویدادها و ضعف‌های امنیتی	(۰/۸۵	۰/۶۰	۰/۴۳)	۰/۴۹	۰/۰۵
۶-۴	به‌کارنبردن اقدامات پیشگیرانه، اکتشافی و اصلاحی (به‌روزرسانی نرم‌افزارهای امنیتی) برای حفاظت از سیستم اطلاعات بانک از نرم‌افزارهای مخرب	(۰/۹۳	۰/۸۰	۰/۷۵)	۰/۷۸	۰/۰۷

همان‌گونه که جدول ۳ نشان می‌دهد، اعضای گروه خبره در معیارهای ۲-۵، ۱-۵، ۳-۵، ۱-۳، ۳-۲، ۲-۲، ۱-۲، ۷-۱، ۵-۱، ۴-۱، ۳-۱، ۱-۱، ۴-۶، ۳-۶، ۲-۶، ۴-۵ به وحدت نظر رسیده‌اند و اختلاف نظر مرحلهٔ اول و دوم در این معیارها کمتر از آستانهٔ خیلی کم (۰/۱) است. لذا نظرسنجی دربارهٔ معیارهای مذکور متوقف می‌شود و فقط برای چهار معیار ۲-۳، ۱-۴، ۱-۶ و ۴-۲ ادامه می‌یابد. امتیاز به‌دست‌آمده برای معیارهای ۲-۱، ۶-۱ و ۲-۴ در دامنهٔ خیلی کم قرار گرفته است، لذا این سه معیار از نظرسنجی حذف شدند.

نظرسنجی مرحلهٔ سوم

در این مرحله نیز پرسشنامهٔ سومی حاوی چهار معیار ۴-۲، ۱-۴، ۲-۳ و ۱-۶ طراحی شد و به همراه نظر قبلی هر فرد و میزان اختلاف آنها با میانگین دیدگاه سایر خبرگان، بار دیگر در اختیار خبرگان قرار گرفت. تحلیل فازی نتایج به‌دست‌آمده از این مرحله در جدول ۴ درج شده است.

جدول ٤. میانگین دیدگاه‌های خبرگان از نظرسنجی سوم

	مولفه‌ها	میانگین فازی مثلثی (m, α, β)			میانگین فازی‌زدایی شده(χ) مرحلهٔ سوم	اختلاف مرحلهٔ دوم و سوم
۲-۴	بی‌بهرگی از طرح کلی برای امنیت اطلاعات و سرمایه‌گذاری‌های مناسب و متناسب با اولویت‌های امنیتی بانک	(۱/۱۰	۰/۹۵	۰/۷۰)	۰/۷۴	۰/۰۷
۳-۲	ناآگاهی از امنیت اطلاعات و بی‌توجهی به آموزش آن	(۱/۰۸	۰/۸۸	۰/۶۳)	۰/۶۸	۰/۰۶
۱-۴	مشخص‌نبودن راهی برای دسترسی‌های مناسب	(۱/۰۸	۰/۸۰	۰/۵۵)	۰/۶۲	۰/۰۹
۱-۶	کنترل‌نکردن صحت داده‌های ورودی، پردازش‌های درونی، یکپارچگی پیغام و صحت داده‌های خروجی	(۱/۱۰	۰/۹۸	۰/۷۳)	۰/۷۶	۰/۰۹

همان‌طور که جدول ۴ نشان می‌دهد، میزان اختلاف نظر خبرگان در مرحله‌های دوم و سوم کمتر از حد آستانه خیلی کم (۰/۱) است، لذا نظرسنجی در این مرحله متوقف می‌شود. از ۲۳ ریسک امنیت اطلاعات سازمانی، طی سه مرحله نظرسنجی، سه ریسک ۲-۱، ۶-۱ و ۲-۴ حذف شدند و درنهایت ۲۰ ریسک برای امنیت اطلاعات سازمانی بانک شناسایی شد.

نتیجه‌گیری و پیشنهادها

در حال حاضر، اطلاعات مهم‌ترین گنجینهٔ سازمان‌ها و اشخاص محسوب می‌شود و از بین رفتن و حتی کوچک‌ترین آسیب به آن، نیازمند صرف زمان، هزینه و نیروی کار تصورناپذیریی برای جبران است و در برخی مواقع اصول کاری و موجودیت یک سازمان را تهدید می‌کند. در این راستا، مدیریت امنیت اطلاعات برای ایجاد امنیت در پیدایش و تبادل اطلاعات، به‌کمک نظام مدیریتی بر پایهٔ استانداردها و راهنماهای فنی و تصمیم‌های صحیح مدیریتی، می‌تواند موجب بهبود عملکرد نظام اطلاعاتی و ارتباطی شود. بنابراین ریسک‌های مرتبط با این فرایند باید کنترل شود. مدیریت ریسک ابزار خوبی برای کنترل ریسک است. به‌کارگیری روش‌های مدیریت و ارزیابی ریسک، تأثیر شگرفی بر چگونگی سروسامان‌دادن به فعالیت‌های سازمان‌ها در زمینهٔ امنیت اطلاعات دارد. در مدیریت ریسک اولین و اساسی‌ترین گام، شناسایی ریسک است.

الگویی که در این پژوهش برای شناسایی ریسک‌های امنیت اطلاعات سازمانی، مبتنی بر استاندارد ایزو ۲۷۰۰۲ و چارچوب کوبیت ۴ ارائه شده است، ضمن بهره‌گیری از مطالعات پیشین

برای شناسایی ریسک‌ها، از روش دلفی فازی نیز استفاده کرده است؛ به این ترتیب که از معیارهای امنیت اطلاعات استاندارد ایزو ۲۷۰۰۲ و بخش DS۵ چارچوب کوبیت ۴ و نیز بررسی مطالعات پیشین، ۵۵ ریسک امنیتی استخراج شد و پس از بررسی و تلفیق، ریسک‌ها در قالب ۲۳ ریسک امنیتی و شش گروه اصلی جانمایی شدند. در نهایت با استفاده از روش دلفی فازی، از ۲۳ ریسک امنیت اطلاعات سازمانی، سه معیار حذف شد و ۲۰ معیار در قالب شش گروه اصلی، برای امنیت اطلاعات سازمانی بانک شناسایی شد.

تصمیم‌گیری مناسب اولیه در زمینهٔ مدیریت ریسک امنیت اطلاعات، می‌تواند هزینه‌ها را کاهش دهد و کنترل ریسک را سهولت بخشد. در تصمیم‌گیری‌های امنیتی، سطح بالایی از بی‌اطمینانی در مجموعهٔ داده‌ها وجود دارد. به‌دلیل محدودیت‌های متعددی چون وقوع بعضی حوادث، ذهنیت بشر و ملاحظات اقتصادی، دستیابی به داده‌های کمی دشوار است و اگر هم داده‌هایی در دسترس باشند، اغلب نادرست‌اند یا به آنها نمی‌توان اطمینان کرد. منطق فازی برای حل بسیاری از مسائل دنیای واقعی که با ابهام مواجه‌اند، به‌کار می‌رود. از این رو می‌تواند چارچوبی برای ادارهٔ وضعیت عدم قطعیت نیز، ارائه کند.

در این راستا ارائهٔ راهکارهای منطقی و هدف‌دار برای کاهش و مدیریت ریسک، در گرو شناخت صحیح از وضعیت سازمان‌ها و ریسک‌ها است. لذا شناسایی و ارزیابی ریسک، در اولویت‌بندی و ارائهٔ راه‌حل صحیح برای اقدامات اصلاحی و پیشگیرانه نقش اساسی دارد. در این پژوهش، به‌کارگیری استاندارد ایزو و چارچوب پذیرفته‌شدهٔ نظام راهبری و کنترل IT (کوبیت) همراه با استفاده از منطق فازی در روش دلفی، سبب قوی‌تر شدن مرحلهٔ شناسایی ریسک شده است. این موضوع به مدلی توسعه‌پذیر انجامید که می‌توان آن را برای شناسایی ریسک‌های تأثیرگذار در سازمان‌های مختلف، گسترش داد.

نتایج پژوهش، ریسک‌های امنیت اطلاعات سازمانی در بانک را شناسایی و ارزیابی کرد. لذا به‌منظور کاهش و کنترل آنها، ارائهٔ راهکارهای مدیریتی مبتنی بر مدیریت ریسک، لازم به نظر می‌رسد. از سوی دیگر، ریسک‌هایی که نسبت به سایر ریسک‌ها برای سازمان مد نظر کمتر مطرح‌اند، به توجه و صرف زمان و هزینهٔ کمتری نیاز دارند.

سازمان‌ها می‌توانند از الگوی ارائه‌شده در این پژوهش برای طراحی سیستم‌های پشتیبان تصمیم‌گیری مدیران در مدیریت ریسک امنیت اطلاعات، بهره ببرند. به این ترتیب بخش‌هایی از سازمان که به توجه، زمان و هزینهٔ بیشتری نیاز دارند، مشخص می‌شود.

References

Avalincharsooghi, S. Doostari, M. Yazdianvarjani, A. & Mahdaviardestani, A. (2013). Use of artificial neural networks in the information security risk assessment. *Journal of Electronic & Cyber Defense*, 1(1): 1-14. (*in Persian*)

Biglarian, P. (2012). *Compilation of information security evaluation criteria's (Case Study: Exchange Organization of Tehran)*. Master Thesis, Azahra, Iran. (*in Persian*)

Broderick, J. S. ISMS. (2006). *security standards and security regulations*. Information Security Technical Report.

BS 7799-2, BS ISO/IEC27001. (2005). *Information technology-Security techniques-Information security management systems*. Available in: http://www.iso.org /iso/catalogue_ detail?csnumber=42103.

BS ISO/IEC27005. (2008). *Information technology-Security techniques-Information security risk management*. Available in: http://www.iso.org/iso/catalogue_ detail? csnumber=42107.

Cheng, CH. & Hsue, Y. (2002). Evaluating the best mail battle tank using fuzzy decision theory. *European Journal of Operational Research*, 142 (1): 174-186.

Chin, K.S., Tang, D.W., Wong, Sh. Y., Wang, H. (2009). Assessing new product development project risk by Bayesian network with a systematic probability generation methodology. *Expert Systems with Applications,* 36 (6): 9879-9890.

Crossler, R., Johnston, A., Lowry, P., Warkentin, M., Baskerville, R. & Qing, H. (2013). Future directions for behavioural information security research. *Computers & security*, 32: 90-101.

Feng, N., Jiannan Wang, H. & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information Sciences*, 256: 57-73.

GE Xiao, Y., Yuan,Y., & Lu Li, L. (2011). An Information Security Maturity Evaluation Model. *Procedia Engineering*, 24: 335 – 339.

Ghazanfari, M., Fathian, M. & Raeissafari, M. (2008). COBIT framework useful tool for measuring the maturity of IT governance in organizations (public banks in case study). *The Association Information and Communication Technology of Iran*, 1 (1&2): 55-64. (*in Persian*)

Houmb, S., Franqueira, V. & Erlend A. (2010). Quantifying security risk level from CVSS estimates of frequency and impact. *The Journal of Systems and Software*, 83(9): 1622-1634.

Iesavi, H. (2011). *Evaluation of operational risks related to information security in the modern banking system*. Master Thesis, Gilan, Iran. (*in Persian*)

IT Governance Institute, (2007). *CobiT 4.1: Control Objectives, Management Guidelines,* Maturity Models.

Jafarnejad, A. & yousefizenouz, R. (2008). The risk Ranking fuzzy Model in the drilling project of Petropars. *Journal of Industrial Management of Tehran University*, 1(1): 21-38. (*in Persian*)

Jamali, GH., Hashemi, M. (2012). Assessment of risk factors on the bank's IT projects Bushehr techniques using fuzzy Dematel. *Journal of Information Technology Management,* 3(9): 21-40. (*in Persian*)

Karimi, Z. (2006). *Conceptual Model of information security risk assessment. (Case Study: Bank Sepah).* Master Thesis, Azahra, Iran. (*in Persian*)

Lo, Ch. & Chen, W. (2012). Hybrid information security risk assessment procedure considering interdependences between controls. *Expert Systems with Applications*, 39: 247-257.

Malekalkalami, M. (2013). Evaluating the performance of information security management at the central libraries of public universities in Tehran, according to the international standard-ISO / IEC. *Journal of Information Processing and Management*, 28 (4): 895-916. (*in Persian*)

Mirbaha, M. (2008). *IT Governance in Financial Services and Manufacturing, Industrial Information and Control Systems at the Royal Institute of Technology ITGI*. Master Thesis, Stockholm, Sweden.

Mireskandari, M. (2010). Information Security Management System and the necessity of its use in organizations. *Processor magazine*. 11(107): 30-39. (*in Persian*)

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

Ozkan, S. & Karabacak, B. (2010). Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management*, 30: 567-572.

Saleh, M. & Alfantookh, A. (2011).A new comprehensive framework for enterprise information security risk management. *Computing and Informatics*, 9: 107-118.

Sanayeei, A. Ghazifard, A. & Sobhanmanesh, F. (2011). Factors affecting the development of identification technology by radio frequency in Electronic supply chain management. *Journal of New Marketing Research*, 1(1): 41-70. (*in Persian*)

Shafieinikabadi, M., Jafarian, A. & Jalilibolhasani, A. (2010). Impact of information security management on the integrity of organizational processes in the supply chain. *Journal of Information Processing and Management*, 27(2): 27-44. (*in Persian*)

Shahrivari, SH. (2011). *Providing the model of information security governance maturity for supply chain management*. Master Thesis, Tarbiyat modares, Iran. (*in Persian*)

Shaw, N. E., Burgess, T. F. & Mattos, C. D. (2005). Risk assessment of option performance for new product and process development projects in the chemical industry: A case study. *Journal of Risk Research,* 8(7-8): 693-711.

Standard Institute and Industrial Research of Iran. (2008). *IT- security technologies- and information security management procedures*. (*in Persian*)

Sungho, K, S., Jang, J.L. & Kim, S. (2007). Common defects in information security management system of Korean companies. *The Journal of Systems and Software,* 80(10):1631-1638.

Taghva,M., izadi,M. (2013). Security investigate in security system developed using service-oriented architecture. *Journal of Information Technology Management of Tehran University*, 5(3): 25-42. (*in Persian*)

Wu, DD., Kefan, X., Gang, C. & Ping, G. (2010). A risk analysis model in concurrent engineering product development. *Journal of Risk Analysis*, 30 (9): 1440-1453.

yuan, T. & Chen, P. (2012). Data Mining Applications in E-Government Information Security. *Procedia Engineering*, 29: 235–240.

Yue, W.T., Cakanyildirim, M., Ryu, Y.U., & Liu, D. (2007).Network externalities, layered protection and IT security risk management. *Decision Support Systems*, 44(1): 1-16.