فصلنامه علمی – پژوهشی مطالعات مدیریت صنعتی – سال سیزدهم، شماره ۳۷، تابستان ۹۴
صفحات ۱۸۵- ۱۶۱

ارائه مدلی جهت اولویت بندی ریسک‌های امنیت اطلاعات سازمانی با استفاده از AHP فازی و شبکه بیزین در صنعت بانکداری

رضا یوسفی زنوز، *اکبر حسن‌پور، **پریسا موسوی ***

(تاریخ دریافت:۹۳/۹/۸-تاریخ پذیرش:۹۴/۱/۲۴)

چکیده:

ریسک جزیی ذاتی و جدایی ناپذیراز زندگی و تجارت است. همواره شرایط عدم اطمینانی که ناشی از اطلاعات و داده‌های ناقص و یا متغیرهای غیرقابل‌کنترل است، با فرصت‌ها و تهدیداتی همراه است. در عصر حاضر بسیاری از سازمان‌ها به شدت به سیستم‌های اطلاعاتی خود متکی‌اند و مدیریت امنیت اطلاعات به یکی از موضوعات مهم سازمانی تبدیل شده‌است. با توجه به این واقعیت که در استفاده از سیستم‌های امنیت اطلاعات نیز ریسک‌هایی وجود دارد، یک فرایند مدیریت ریسک موثر، می‌تواند برنامه امنیتی موفقی را نتیجه دهد. مدیریت ریسک شامل فرایند شناسایی ریسک‌ها، ارزیابی ریسک، و تلاش برای کاهش ریسک‌ها به سطح قابل قبول می‌باشد. هدف این پژوهش، اولویت‌بندی ریسک‌های امنیت اطلاعات سازمانی، به‌منظور ارائه راهکاری برای ارتقا وضعیت امنیت اطلاعات سازمانی است. به این منظور، با استفاده از AHP فازی و شبکه بیزین، مدلی جهت ارزیابی و اولویت‌بندی ریسک‌های امنیت اطلاعات سازمانی ارائه گردید. در فرایند ارزیابی ریسک،شدت ریسک‌ها با استفاده از AHPفازی و احتمال آنها با استفاده از شبکه بیزین،محاسبه شد و سرانجام ریسک‌ها اولویت‌بندی شدند. یافته‌های این پژوهش نشان می‌دهد در سازمان مورد پژوهش، ریسک عدم آگاهی و عدم ارائه آموزش‌های مناسب در حوزه امنیت اطلاعات، بالاترین اولویت و بیشترین نیاز به توجه را دارد.

واژگان کلیدی:

امنیت اطلاعات، ریسک، مدیریت ریسک، AHP فازی، شبکه بیزین

* استادیار گروه مدیریت دانشکده مدیریت و حسابداری، دانشگاه خوارزمی تهران

** استادیار گروه مدیریت دانشکده مدیریت و حسابداری، دانشگاه خوارزمی تهران

*** کارشناسی ارشد مدیریت فناوری اطلاعات، دانشکده مدیریت و حسابداری، دانشگاه خوارزمی تهران
parisamusavi_7@yahoo.Com

مقدمه

در قرن بیست‌ویکم، اطلاعات شاهرگ حیاتی هر سازمان محسوب می‌شود. فناوری اطلاعات به سرعت رشد کرده و سیستم‌های اطلاعاتی، نقشی تعیین کننده و فراگیر در کسب وکارهای سازمانی دارند. توسعه سیستم‌های اطلاعاتی مانند یک شمشیر دولبه است که از یک سو منافع بسیاری را برای بشر به ارمغان آورده و از سوی دیگر،که موضوع امنیت اطلاعات مطرح است، زیان‌های جبران‌ناپذیری را موجب شده‌است. ویروس ها، هکرها، نشت اطلاعات محرمانه، نارسایی سیستم، قطع خدمات و .... صدمات زیادی را به سازمان‌ها وارد آورده‌اند(yuan & Chen, 2012). اگر چه امنیت اطلاعات اغلب منافع بسیاری را برای سازمان به ارمغان می-آورد، پیاده سازی آن، گاه با شکست مواجه می‌شود. در پژوهشی که توسط شرکت امنیتی مک آفی ۱(۲۰۰۹) در سال ۲۰۰۸ انجام شده‌است نشان داده شد که نقض امنیت اطلاعات در شرکت‌های جهانی به زیانی به ارزش بیش از ۱ هزار میلیارد دلار در عرض یک سال منجر می‌شود. از این رو، مطالعات زیادی به منظور شناسایی و بررسی عوامل کلیدی موثر بر امنیت اطلاعات به منظور اجرای موفقیت آمیز آن، انجام شده است(Feledi, Fenz & Lechner, 2013).

مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف امنیت و بررسی موانع سر راه رسیدن به این اهداف و ارائه راهکارهای لازم، را بر عهده دارد. همچنین مدیریت امنیت، وظیفه پیاده‌سازی و کنترل عملکرد سیستم امنیت سازمان را بر عهده داشته و در نهایت باید تلاش کند تا سیستم را همیشه روزآمد نگه دارد(Crossler &et al 2013).

مدیریت ریسک را می‌توان یکی از ملزومات مدیریت موفق در این عرصه دانست.فرایند مدیریت ریسک بر شناسایی ریسک‌های موجود و کاهش اثر نامطلوب آنها تمرکز دارد واز چهار فاز شناسایی، ارزیابی،کنترل یا مدیریت و ردیابی رخدادهای ریسکی تشکیل می‌شود.

یکی از مهمترین مراحل مدیریت ریسک، ارزیابی و رتبه‌بندی عوامل ریسک است زیرا با انجام رتبه‌بندی ریسک‌ها، ارجحیت هر ریسک بر اساس شاخص‌های تعیین شده در مقابل

1- McAfee

سایر ریسک‌ها مشخص و در نتیجه تصمیم‌گیرنده می‌تواند در مورد میزان تخصیص منابع موجود برای مقابله با هر ریسک برنامه‌ریزی نماید. به عبارتی دیگر با رتبه‌بندی این عوامل، مدیران سازمان‌ها از طریق تخصیص بودجه کافی و زمان لازم، آمادگی مورد نیاز برای مقابله با هر یک از این عوامل برحسب اولویت و توان سازمان برای پاسخ‌گویی به هر یک را کسب خواهند کرد. از این رو هدف از فاز ارزیابی ریسک، اندازه‌گیری ریسک‌ها بر اساس شاخص‌های مختلف از قبیل میزان تاثیر و احتمال وقوع می‌باشد(میرفخرالدینی، عندلیب اردکانی، رضایی اصل، ۱۳۹۰).

در سال‌های اخیر، تحلیل ریسک امنیت برای سیستم‌های اطلاعاتی توجه بسیاری از محققان را در این زمینه جلب کرده‌است. روش‌های موجود برای تجزیه و تحلیل ریسک را می‌توان به سه گروه اصلی تقسیم کرد: روش‌های کمی، روش‌های کیفی، و ترکیبی از رویکردهای کمی و کیفی. روش‌های کمی از مدل‌های ریاضی و آماری برای نشان دادن ریسک استفاده می‌کنند. قرار گرفتن در معرض ریسک امنیتی به عنوان تابعی از احتمال تهدید و شدت آسیب ناشی از این تهدیدات در نظر گرفته می‌شود(Yang, Shieh & Tzeng, 2013). در واقع روش‌های ارزیابی کمی ریسک، با استفاده از ابزارهای ریاضی وآماری ، تلاش می‌کنند تا مقادیر خاصی را به هزینه حفاظت از داده‌ها و میزان آسیب‌هایی که امکان دارد رخ دهد، اختصاص دهند. روش‌های کیفی ارزیابی ریسک، مبتنی بر قضاوت شخصی، نگرش‌ها و تجربیات شخصی است(Chen& Lo, 2012). از آنجا که تحلیل کیفی به طور گسترده به تجربه تحلیل‌گران وابسته است، هم فرآیند و هم نتیجه ارزیابی ریسک امنیت نسبتا ذهنی خواهد بود (Feng & Li, 2011). همگام با پیچیده‌تر شدن سیستم‌های اطلاعاتی در کسب و کار، هیچ یک از روشهای کمی و کیفی به تنهایی نمی تواند به درستی فرایند ارزیابی ریسک را مدلسازی کند (Solms & Niekerk, 2013) بنابراین به روشی جامع نیاز است که ترکیبی از هر دو رویکرد کمی وکیفی باشد (Feng & Li, 2011) .

با توجه به آنچه گفته شد،سیستم‌های اطلاعاتی باید با قابلیت بالایی از اطمینان عمل کنند و در این مسیر، ریسک ومخاطره‌آمیزی معقولی بر آنها مترتب باشد. به این منظور نیاز به یک فرایند

مدیریت ریسک موثر پیرامون امنیت اطلاعات سازمانی احساس می‌شود.هدف این پژوهش، اولویت‌بندی ریسک‌های امنیت اطلاعات، به‌منظور ارائه راهکاری برای ارتقا وضعیت امنیت اطلاعات سازمانی بانک[۲] است. به این منظور ترکیبی از رویکردهای کمی و کیفی به کار گرفته شده‌است. با روش AHP فازی شدت ریسک‌ها، تعیین شده است و احتمال ریسک‌ها با استفاده از شبکه بیزین مشخص شده‌است. حاصلضرب شدت ریسک در احتمال وقوع آن، اولویت هر ریسک را تعیین می کند.

پیشینه پژوهش

در زمینه مدیریت ریسک پژوهش‌های انجام گرفته‌است. عالم‌تبریز (۱۳۹۰)، در مقاله‌ای به تحلیل ریسک‌های پروژه بر اساس یک مدل تلفیقی از فرایند مدیریت ریسکPMBOK پرداخته‌است. بدین منظور در ابتدا ریسک‌های پروژه شناسایی و با استفاده از تکنیک RFMEA رتبه‌بندی می‌شوند(عالم‌تبریز و حمزه‌ای،۱۳۹۰). الفت(۱۳۸۹) در پژوهشی تحت عنوان"شناسایی و اولویت‌بندی ریسک پروژه بر مبنای استانداردPMBOK با رویکرد فازی" ، برای اولویت‌بندی ریسک‌های پروژه از AHP فازی و TOPSISفازی استفاده کرده‌است(الفت، خسروانی و جلالی، ۱۳۸۹). در پژوهشی دیگر میرفخرالدینی(۱۳۹۰) با استفاده از فنون الکتر، تاپسیس وتاکسونومی به رتبه‌بندی عوامل ریسک زنجیره تامین حوزه فناوری اطلاعات بنگاه‌های کوچک و متوسط پرداخته‌است(میرفخرالدینی، عندلیب اردکانی و رضایی اصل،۱۳۹۰).

در زمینه ارزیابی امنیت اطلاعات، اغلب پژوهشهایی که درایران انجام شده‌است، به ارائه مدل مفهومی پرداخته و تحقیقات اندکی موضوع تحلیل ریسک را مورد توجه قرار داده‌اند. از جمله این پژوهش‌ها عبارتند از: بررسی ریسک عملیاتی مربوط به امنیت اطلاعات در سامانه بانکداری مدرن (عیسوی،۱۳۹۰)، مطالعه کنترل‌های امنیت اطلاعات بر اساس استانداردهای

۲- به علت تعهد مولفان به سازمان مورد نظر، از ذکر نام خودداری شده‌است.

بین المللی(خواجویی،۱۳۹۰)، تدوین شاخص های ارزیابی امنیت اطلاعات سازمان (مورد مطالعه: سازمان بورس و اوراق بهادار تهران) (بیگلربگیان،۱۳۹۱)، ارائه یک مدل مفهومی جهت ارزیابی ریسک امنیت اطلاعات در سازمان‌ها(مورد بانک سپه)(کریمی،۱۳۸۵) و ارزیابی ریسک امنیت اطلاعات با استفاده از شبکه‌های عصبی مصنوعی(اولین چهارسوقی، دوستاری، یزدیان ورجانی و مهدوی اردستانی، ۱۳۹۲). در خارج از ایران نیز پژوهشهای بسیاری در زمینه ارزیابی ریسک امنیت اطلاعات، و با بکارگیری روش‌های متنوع انجام گرفته‌است. در ارزیابی ریسک از روشهای هوشمندی مثل فازی، سامانه‌های خبره، AHP و شبکه‌های عصبی استفاده شده‌است. وو و همکارانش[3] (۲۰۱۰)، چالش‌ها و ریسک‌های مختلف توسعه محصول با مهندسی همزمان محیط را یافته و رویکردی کمی برای شناسایی سیستماتیک مهمترین ریسک‌های انجام مهندسی همزمان پروژه ها، پیشنهاد کرده‌اند(Wu, Xie, Chen & Gui, 2010). « هازلم و همکارانش»[4](۲۰۰۸) مدل فازی را برای ارزیابی ریسک شبکه‌ها پیشنهاد کرده‌اند(Haslum, Abraham & Kanpskog, 2008). همچنین، « هانگ و همکارانش»[5] (۲۰۱۰)ریسک امنیت اطلاعات را بر اساس مدل شبکه عصبی مصنوعی و AHP فازی ارزیابی نموده‌اند(Wei, Zhang, & Huang,2010). ادغام نتایج تحقیقاتAHP، ریاضیات فازی و روش شبکه عصبی مصنوعی توسط «وانگ و زنگ»[6] (۲۰۱۰)نمونه دیگری از ارزیابی ریسک امنیت اطلاعات با استفاده از روش‌های هوشمند می‌باشد(Wang & Zeng, 2010). «چن و لو »[7] (۲۰۱۲) نیز برای ارزیابی و تحلیل ریسک امنیت اطلاعات روش‌های فرایند تحلیل شبکه‌ای(ANP)، و دیمتل[8] را به کار گرفته‌اند(Chen& Lo, 2012). محققین دیگری از جمله« نان فنگ، هری جیانا وانگ و

3 -Wu et al

4 -Haslum.K, etal

5 - Huang.Z etal

6 -Wang.Z, Zeng.H

7 -Chun Lo & Jia Chen

8 -Decision Making Trial And Evaluation(DEMATEL)

مین کیانگ لی»[9](۲۰۱۴)، با بکارگیری شبکه بیزین و کولونی مورچگان، مدلی جهت تحلیل ریسک امنیت سیستم‌های اطلاعاتی ارائه کرده‌اند(Feng, Wang, & Li, 2014).«یانگ، شی و تیزنگ»[10] (۲۰۱۳)، در مقاله‌ای مدلی جهت ارزیابی و کنترل ریسک امنیت اطلاعات پیشنهاد می‌دهند که می‌تواند امنیت اطلاعات را برای شرکت‌ها و سازمان‌ها ارتقا دهد. این مدل یک مدل تصمیم گیری چند معیاره[11] ترکیبی از VIKOR، DEMATEL، و ANP برای حل مساله معیارهای متناقض است که وابستگی و بازخوردآن‌ها را نشان می‌دهد. علاوه بر این، یک مطالعه موردی نیز برای ارزیابی مدل ارائه شده و نشان دادن اثربخشی آن، انجام گرفته-است(Yang ,Shieh & Tzeng, 2013). برای نمایش روابط بین فاکتورهای ریسک، «فن و یو»، یک شبکه بیزین (BN)مبتنی بر فرایند، ارائه نمودند که پشتیبانی برای تحلیل ریسک فراهم می‌کند(Feng, Wang, & Li,2014).

مفهوم ریسک

ریسک، رویدادها یا وضعیت‌های ممکن‌الوقوع نامعلومی است که در صورت وقوع به صورت پیامدهای منفی یا مثبت بر اهداف تاثیر می‌گذارد. هر یک از این رویدادها یا وضعیت‌ها دارای علل مشخص و نتایج و پیامدهای قابل تشخیص هستند(جعفرنژاد و یوسفی زنوز، ۱۳۸۷). بنا بر تعریف ایزو IEC ریسک عبارت است از ترکیب احتمال یک رویداد و میزان پیامدهای آن (Imamverdiev & .Derakshande, 2010)

مدیریت ریسک

مدیریت ریسک به عنوان یکی از موضوعات عمده مدیریت می‌باشد که شامل برنامه‌ریزی، سازماندهی، پایش و کنترل تمامی جنبه‌های یک پروژه بوده و شامل شناسایی ریسک، اندازه-گیری آن، توسعه پاسخ ریسک و کنترل پاسخ ریسک است(جعفرنژاد و یوسفی زنوز، ۱۳۸۷).

9 Nan Feng, Harry Jiannan Wang & Minqiang Li
10Yu-Ping Ou Yang How-Ming Shieh. Gwo-Hshiung Tzeng
11 MCDM

ارزیابی ریسک

یک ریسک، ترکیبی است از عواقب وقوع یک رویداد ناخواسته واحتمال وقوع این رویداد. ارزیابی ریسک، به صورت کمی یا کیفی، ریسک را توصیف کرده و مدیران را قادر می‌سازد ریسک‌ها را با توجه به شدت درک‌شده آنها، و یا دیگر معیارهای تعیین‌شده، اولویت بندی کنند. ارزیابی ریسک شامل فعالیت‌های زیر است:

تجزیه و تحلیل ریسک(شناسایی ریسک، برآورد ریسک) و ارزشیابی ریسک

ارزیابی ریسک ارزش دارایی‌های اطلاعاتی را تعیین کرده، تهدیدات و شدت آسیبی که هر ریسک دارد (و یا می‌تواند داشته باشد)، را شناسایی کرده و با تعیین کنترل‌های موجود و میزان اثر آنها بر ریسک‌های شناسایی شده، عواقب احتمالی هر ریسک را تعیین می‌کند و در نهایت ریسک‌ها را اولویت بندی کرده و رتبه آنها را بر اساس مجموعه معیارهای ارزیابی، تعیین می‌کند(BS ISO/IEC27005, 2008).

شبکه‌های بیزین

شبکه‌های بیزین (BN)یک مدل گرافیکی جهت استدلال در یک محیط غیر قطعی می-باشند (Kevin, Corb & Nicholson, 2004). شبکه‌های بیزین به عنوان شبکه‌های باور احتمالاتی یا شبکه‌های علی شناخته شده‌اند که قادر به نمایش وابستگی و استقلال متغیرهای تصادفی می‌باشد(Feng, Wang, & Li,2014). شبکه‌های بیزین، همچنین به عنوان یک روش مدل سازی برای بیان رابطه علت و معلولی مبتنی بر استنباط بیزی شناخته شده‌اند. این شبکه‌ها، در قالب یک گراف بدون دور نشان داده می‌شوند که در این گراف گره‌ها نمایانگر متغیرها و یال‌ها نشان‌دهنده روابط بین متغیرها هستند. این گراف، تمام روابط میان متغیرها را به‌طور انتزاعی مدلسازی می‌کند(Wagner,2010). احتمالات شرطی، توسط تعیین متغیرها و ارتباطات آنها با هم مشخص می‌شوند (korb & Nicholson,2004). برای هر گره یا متغیر، احتمال متناظر با آن گره وجود دارد، احتمال هر گره توسط گره‌های والدین، که گره فعلی را تحت تاثیر قرار می‌دهند، تعریف می‌شود(Wagner,2010).

مقایسات زوجی و فرایند تجزیه‌و تحلیل سلسله‌مراتبی گروهی فازی

فرایند تجزیه و تحلیل سلسله‌مراتبی (AHP) یکی از روش‌هایی است که می‌توان از توسعه فازی آن برای حل مسائل استفاده کرد. اگرچه روش AHP به دلیل عدم توانایی در توجه به عدم قطعیت و مبهم بودن اطلاعات برخی از تصمیم‌گیرندگان همواره مورد نقد بوده‌است، اما برای استفاده از نظرات مبهم و احتمالی، AHP فازی و اعداد مثلثی توصیه شده‌است (ناظمی، کاظمی و اخروی، ۱۳۹۰). در بسیاری از تحقیقات، برای اولویت‌بندی عوامل از AHP ساده یا فازی استفاده شده‌است. در این تحقیقات، در نهایت، عاملی که وزن بیشتری را به خود اختصاص دهد، مهمتر از سایر عوامل شناخته شده و در اولویت قرار می‌گیرد. صاحبنظران نظرات خود را درباره هر مقایسه زوجی، در طیف شش‌تایی از اهمیت یکسان تا کاملا مهم بیان می‌نمایند. هر کدام از اعداد این طیف نیز، بیانگر سه عدد هستند که در جدول ۱ آمده است. توابع عضویت مثلثی و ذوزنقه‌ای برای تقابل با ابهام ارزیابی کلامی مناسب هستند. در این پژوهش در AHP فازی از اعداد فازی مثلثی و روش « چانگ» استفاده شده است.

جدول ۱: تبدیل متغیرهای زبانی به اعداد فازی مثلثی(ناظمی، کاظمی و اخروی، ۱۳۹۰)

طیف	۱	۲	۳	۴	۵	۶
ترجیحات	شدت یکسان	شدت تقریبا یکسان	کمی شدیدتر	شدیدتر	بسیار شدیدتر	کاملا شدید
اعداد فازی مثلثی	(۱و۱و۱)	(۳/۲و۱و۱/۲)	(۲و ۳/۲ و۱)	(۵/۲و۲و۳/۲)	(۳، ۵/۲ ،۲)	(۵/۲ ،۷،۳/۲)

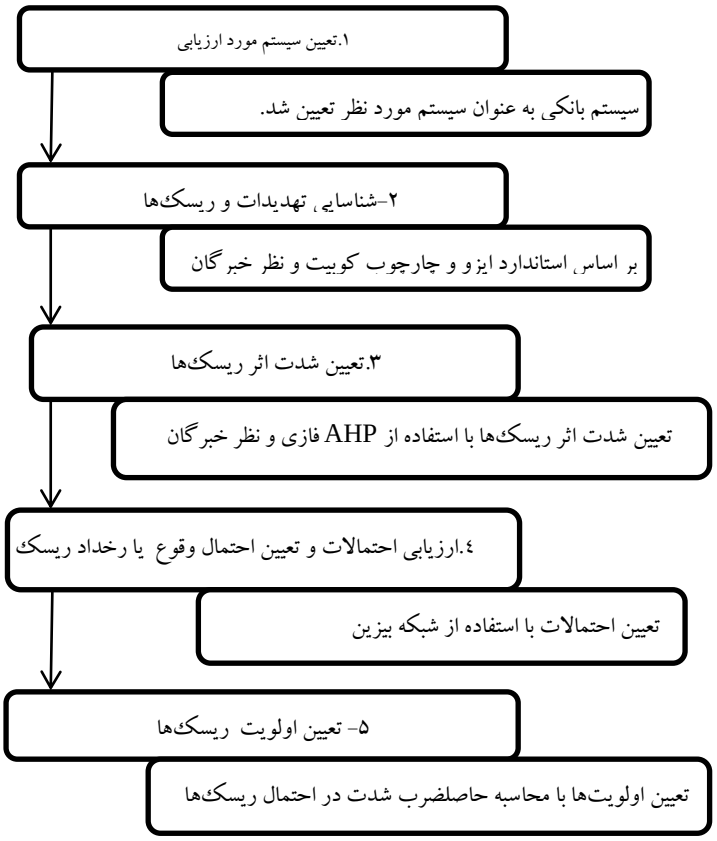
روش تحقیق

از آنجا که این پژوهش به طراحی یک مدل برای شناسایی و اولویت‌بندی ریسک‌های امنیت اطلاعات سازمانی می‌پردازد. جمع‌آوری اطلاعات از خبرگان از طریق پرسشنامه، و تجزیه و تحلیل داده‌ها از طریق روش AHP فازی، شبکه بیزین و نرم افزار نتیکا انجام گرفته است. شکل ۱ متدولوژی کلی این پژوهش را نشان می‌دهد.

در نرم‌افزار نتیکا ابتدا شبکه بیزین (گره‌ها و لبه‌ها) ترسیم شده و با توجه به حالت‌های موجود برای هر گره، احتمالات شرطی(CPT)های شبکه را کامل کرده و در انتها احتمال گره نهایی به عنوان خروجی از نرم‌افزار دریافت می‌شود.

در واقع بطورکلی پژوهش در چهار مرحله اصلی انجام شده‌است :

شکل۱: متدولوژی پژوهش



مرحله اول؛ شناسایی ریسک‌های امنیت اطلاعات سازمانی: بر اساس استاندارد ایزو ۲۷۰۰۲ و چارچوب کوبیت۴، مطالعه اسنادی ،بررسی ادبیات موضوع و نظر خبرگان مجموعا ۶ فاکتور و ۲۰ زیر فاکتور ریسک امنیت اطلاعات سازمانی شناسایی شدند. تیم خبرگان شامل ۱۰ نفر از متخصصان اداره فناوری اطلاعات بانک بوده است.

مرحله دوم؛ تعیین میزان شدت فاکتورها و زیرفاکتورها با استفاده از AHP گروهی فازی: این مرحله شامل تخصیص وزن نرمال شده به هر یک از عوامل است. تیم تصمیم نظریات خود را درباره مقایسات زوجی، در طیف شش‌تایی از شدت یکسان تا کاملا شدید(جدول۱) بیان نمودند. سپس با استفاده از روش چانگ، وزن‌های نرمال و نهایی، در مورد شدت اثر هر ریسک محاسبه گردیده‌است.

میانگین هندسی فازی

$$= (\alpha 1, \alpha 2, \alpha 3)$$
$$= \left(\left(\prod_{i=1}^{k} a1_{ijl} \right)^{\frac{1}{k}}, \left(\prod_{i=1}^{k} a2_{ijl} \right)^{\frac{1}{k}}, \left(\prod_{i=1}^{k} a3_{ijl} \right)^{\frac{1}{k}} \right)$$

فرمول (۱) (ناظمی، کاظمی و اخروی، ۱۳۹۰)

مرحله سوم؛ تعیین احتمال ریسک‌های امنیت اطلاعات: با استفاده از شبکه‌های بیزین، احتمال ریسک‌های امنیت اطلاعات تعیین شده‌است. در این پژوهش برای جمع‌آوری احتمالات و داده‌های مورد نیاز در شبکه بیزین، از قضاوت کارشناسان و افراد خبره حوزه امنیت اطلاعات استفاده شده است. ریسک‌هایی که در مرحله اول برای امنیت اطلاعات شناسایی شده اند، هر یک تحت تاثیر زیرفاکتورهایی قرار دارند. برای تعیین احتمال هر زیر فاکتور(گره) یک طیف لیکرت پنجگانه در نظر می‌گیریم که با نظر خبرگان مقادیر این احتمالات مشخص می‌گردد.

مرحله چهارم؛ اولویت‌بندی نهایی فاکتورهای ریسک امنیت اطلاعات: هرچه حاصلضرب شدت و احتمال فاکتورها یا زیر فاکتورها، بیشتر شود اولویت بالاتری خواهند

داشت. بنابراین در این مرحله احتمالات بدست آمده از مرحله سوم در شدت‌های حاصل از مرحله دوم ضرب شده و اولویت نهایی هر عامل به دست آمده است.

یافته‌های تحقیق

شناسایی ریسک‌ها

نتایج حاصل از مرحله اول پژوهش به شرح زیر ارائه می‌شود:

۲۰ مولفه در قالب ۶ فاکتوراصلی به عنوان ریسک‌های بانک شناسایی شدند. ۶ فاکتور اصلی ریسک عبارتند از: ۱-نبود خط مشی امنیت، ۲-عدم تعهد مدیریت عالی،۳-عدم امنیت عامل انسانی، ۴-عدم امنیت سیستم‌ها و تجهیزات فیزیکی،۵-عدم امنیت در شبکه‌ها و تجارت الکترونیک،۶-عدم وجود سیستم‌های کنترلی مناسب فاکتورها و زیر فاکتورهای ریسک امنیت اطلاعات سازمانی که در این مرحله شناسایی شدند در جدول ۲ ارائه گردیده است.

جدول ۲: فاکتورها و زیر فاکتورهای ریسک امنیت اطلاعات سازمانی

۱-نبود خط مشی امنیت	۲-عدم تعهد مدیریت عالی
۱,۱) عدم وجود یک خط مشی امنیت اطلاعات جامع و کامل و قابل بازنگری	۲,۱) نبود تعهد و حمایت مدیریت بانک نسبت به امنیت اطلاعات بانک
۱,۲) روشن نبودن تعریف مسئولیت امنیت اطلاعات در بانک	۲,۲) عدم تخصیص بودجه مناسب به طرح امنیت
۱,۳) عدم وجود رویه‌ای مناسب در طبقه‌بندی و کدگذاری اطلاعات	۲,۳) عدم توجه و زمانبندی جهت پیاده‌سازی و اجرایی نمودن طرحها
۱,۴) عدم انطباق سیستم‌ها با خط مشی‌ها و استانداردهای امنیتی بانک	۲,۴) نداشتن یک طرح کلی برای امنیت اطلاعات و سرمایه‌گذاری‌های مناسب و متناسب با اولویت‌های امنیتی بانک
۱,۵) عدم مدیریت حوادث و ضعف‌های امنیت‌اطلاعات	

۳-عدم امنیت عامل انسانی	۴-عدم امنیت سیستم‌ها و تجهیزات فیزیکی
۳,۱) نبود نیروی انسانی متخصص در زمینه امنیت اطلاعات	۴,۱) عدم تعریف دسترسی‌های مناسب
۳,۲) عدم آگاهی و عدم ارائه آموزشهای مناسب در حوزه امنیت اطلاعات	
۵-عدم امنیت در شبکه‌ها و تجارت الکترونیک	۶-عدم وجود سیستم‌های کنترلی مناسب
۵,۱) عدم ایجاد نسخه پشتیبان و عدم یکپارچگی و دسترس‌پذیری اطلاعات و امکانات پردازش اطلاعات	۶,۱) عدم کنترل در صحت داده‌های ورودی،پردازش‌های درونی، یکپارچگی پیغام و صحت داده‌های خروجی
۵,۲) عدم وجود امنیت در خدمات شبکه	۶,۲) عدم نظارت و پایش در توسعه نرم-افزارهای برون‌سپاری شده
۵,۳) عدم وجود امنیت درفرایند تبادل اطلاعات و نرم‌افزارها درون یک بانک و یا با هر موجودیت بیرونی	۶,۳) عدم گزارش‌دهی رویدادها و ضعف‌های امنیتی
۵,۴) عدم امنیت در خدمات تجارت الکترونیکی شامل دادو ستدهای آنلاین و اطلاعات در دسترس عموم	۶,۴) عدم وجود اقدامات پیشگیرانه، اکتشافی و اصلاحی(به روزرسانی نرم‌افزارهای امنیتی) برای حفاظت از سیستم اطلاعات بانک از نرم افزارهای مخرب)مانند ویروس ها، کرم ها، جاسوس افزارها، اسپم

تعیین شدت اثر فاکتورها و زیر فاکتورهای ریسک:

تیم تصمیم نظریات خود پیرامون شدت ریسک‌ها را با مقایسات زوجی و در طیف پنجگانه از شدت یکسان تا کاملا شدید بیان نمودند. هر کدام از اعداد این طیف نیز، بیانگر یک عدد فازی مثلثی است که با یک سه تایی نشان داده می‌شود. پس از اخذ نظرات خبرگان، میانگین

هندسی فازی نظریات (با توجه به فرمول (۱)) محاسبه شده است. در جدول ۳ میانگین هندسی فازی نظریات خبرگان در مقایسات زوجی فاکتور سوم آمده است.

جدول ۳: ماتریس فازی- گروهی مقایسات زوجی زیر مولفه‌های فاکتور سوم(عدم امنیت عامل انسانی):

	۳,۱	۳,۲
۳,۱	(۱،۱،۱)	(۱/۴۰، ۱/۰۸، ۰/۷۰)
۳,۲	(۰/۷۱، ۰/۹۲، ۱/۴۳)	(۱،۱،۱)

در توضیح اعداد این جدول، نمونه‌ای بیان شده‌است. در ردیف اول و ستون دوم جدول ۴ این اعداد آمده‌اند: (۱/۴۰، ۱/۰۸، ۰/۷۰)، با توجه به قوانین مقایسات زوجی فازی، سلول معکوس این سلول ، یعنی ردیف دوم و ستون اول جدول ۳: (۱/۴۳، ۰/۹۲، ۰/۷۱)به این شکل معکوس شده‌است(آذر و فرجی، ۱۳۸۱):

$$(\frac{1}{1.40} \ , \ \frac{1}{1.08} \ , \frac{1}{0.70})=(۱/۴۳، ۰/۹۲، ۰/۷۱)$$

میانگین هندسی نظرات خبرگان درباره فاکتورها و سایر زیر فاکتورهای ریسک امنیت اطلاعات، نیز به همین ترتیب محاسبه گردیده‌است. محاسبات AHP فازی درباره همه نتایج انجام شده است. در ادامه نحوه محاسبات وزن فاکتورها به تفصیل شرح داده شده است. با توجه به روش چانگ، ابتدا S_k محاسبه می‌شود(آذر و فرجی، ۱۳۸۱):

$$S_k = \sum_{j=1}^{n} M_{ij} * \left[\sum_{i=1}^{m}\sum_{j=1}^{n} M_{ij}\right]^{-1}$$

$$\left[\sum_{i=1}^{m}\sum_{j=1}^{n} M_{ij}\right]^{-1} = (3.41 \ , 4 \ , 4.83 \ )^{-1} = (0.21 \ , 0.25 \ , 0.29)$$

$$S_1 = (1.7, \ 2.08, \ 2.4)(0.21 \ , 0.25 \ , 0.29) = (0.082 \ \ , 0.119 \ \ , 0.175)$$

$$S_2 = (1.71 \ \ , 1.92 \ \ , 2.43)(0.21 \ , 0.25 \ , 0.29) = (0.082 \ , 0.109 \ , 0.177)$$

حال درجه بزرگ بودن هر یک از عناصر فوق برعناصر دیگر، با توجه به روابط زیر محاسبه شده‌است:

$$S_i = (l_i, m_i, u_i)$$

$V(S_1 \geq S_2)=1 \qquad if \;\; m_1 \geq m_2$

$V(S_1 \geq S_2)= \frac{(u_1-l_2)}{(u_1-l_2)+(m_2-m_1)} \quad , \quad 0.W$

$V(S_1 \geq S_2, \dots \dots, S_k) = Min\{V(S_1 \geq S_k)\}$

$V(S_1 \geq S_2) = 1$

$V(S_2 \geq S_1) = \frac{(u_2-l_1)}{(u_2-l_1)+(m_1-m_2)} = 0.91$

لذا وزن فاکتورها عبارت است از:

$W' = (1 \;\; , 0.91 \;)$

اینک بر اساس رابطه $W_i = \frac{\acute{W}_i}{\sum \acute{W}_i}$ اوزان نرمال فاکتورها عبارت است از:

$W=(0.52 \quad , \; 0.48 \;)$

در نهایت، وزن نرمال فاکتورها و زیرفاکتورها طبق روابط فوق مشخص شد. پس از ضرب نمودن وزن فاکتور در زیر فاکتور وزن نهایی زیر فاکتورها نیز بدست آمد و در جدول ۴ ارائه گردید.

جدول ۴: وزن نهایی فاکتورها و زیر فاکتورها و وزن نرمال زیر فاکتورها

فاکتور۱ ۰/۱۴	وزن نرمال	وزن نهایی	فاکتور۲ ۰/۱۲	وزن نرمال	وزن نهایی	فاکتور۳ ۰/۲۱	وزن نرمال	وزن نهایی	فاکتور۴ ۰/۱۳	وزن نرمال	وزن نهایی	فاکتور۵ ۰/۱۸	وزن نرمال	وزن نهایی	فاکتور۶ ۰/۲۲	وزن نرمال	وزن نهایی
۱,۱	۰/۴۱	۰/۰۵۷	۲,۱	۰/۰۳۵	۰/۰۴۲	۳,۱	۰/۵۲	۰/۱۰۹	۴,۱	۱	۰/۱۳	۵,۱	۰/۱۲	۰/۰۲۲	۶,۱	۰/۳۲	۰/۱۳۸
۱,۲	۰/۰۷	۰/۰۱۰	۲,۲	۰/۰۲۴	۰/۰۲۹	۳,۲	۰/۴۸	۰/۱۰۱				۵,۲	۰/۳۸	۰/۰۶۸	۶,۲	۰/۰۶	۰/۰۲۶
۱,۳	۰/۲۶	۰/۰۳۶	۲,۳	۰/۰۶	۰/۰۰۷							۵,۳	۰/۲۹	۰/۰۵۲	۶,۳	۰/۱۸	۰/۰۷۷
۱,۴	۰/۱۹	۰/۰۲۷	۲,۴	۰/۳۴	۰/۰۴۱							۵,۴	۰/۰۳	۰/۰۰۵	۶,۴	۰/۴۳	۰/۱۸۵
۱,۵	۰/۰۷	۰/۰۱۰															

وزن نهایی هر زیر فاکتور، از حاصلضرب وزن نرمال زیر فاکتور در وزن نرمال فاکتور حاصل می‌شود.

تعیین احتمال وقوع فاکتورها و زیر فاکتورهای ریسک:

با توجه به نتایج ارائه شده در جدول ۴ مشخص شد که کدام فاکتورها و به تبع آن کدام زیر فاکتورهای ریسک شدت اثر بیشتری دارند. اکنون با توجه به متدولوژی ارزیابی ریسک، مبنی

بر ضرب شدت اثر ریسک در احتمال آن، برای تعیین اولویت هر ریسک باید احتمال وقوع آن نیز محاسبه گردد. احتمال وقوع زیر فاکتورهای ریسک(احتمالات اولیه)، با استفاده از طیف پنجگانه (خیلی زیاد، زیاد، متوسط، کم، خیلی کم) و براساس نظر خبرگان، مشخص گردیده‌است.

احتمالات شرطی شبکه بیزین با استفاده از فرمول(۲) تعیین می‌گردد:

$$P(x|y) = \frac{P(x \cap y)}{p(y)}$$ فرمول(2) (Kevin, Corb &*Nicholson*, 2004)

در این پژوهش احتمالات شرطی نیز با استفاده از طیف پنجگانه (خیلی زیاد، زیاد، متوسط، کم، خیلی کم) و براساس نظر خبرگان، مشخص گردیده‌است.

فرض کنید مجموعه‌ای شامل n متغیر به صورت $\{x_1, \dots, x_n\}$ داشته باشیم،که هر x_I یک متغیر تصادفی است و گره‌های والد این متغیر را با $parent(x_i)$ نشان می‌دهیم. برای محاسبه توزیع احتمال توام این متغیرها از رابطه زیر استفاده می‌شود Kevin , Corb & (Nicholson, 2004).

فرمول(**3**) (Kevin , Corb & *Nicholson*, 2004)(Feng, Wang, & Li, 2014)

$$P(X_1, X_2, \dots., X_n) = \prod_{i=1}^{n} P\left(X_i \middle| Parents(X_i)\right)$$

احتمالات اولیه و شرطی برای فاکتور ۳ و زیر فاکتورهای آن به صورت ذیل تعیین شده است:

جدول ۵ : احتمالات اولیه گره ریشه‌ای ۳

زیر فاکتور۳,۲		زیر فاکتور۳,۱	
۰/۲	VH	۰	VH
۰/٤	H	۰/۱	H
۰/۲	M	۰/۲	M
۰/۲	L	۰/۵	L
۰	VL	۰/۲	VL

جدول۶ : احتمالات شرطی گره ریشه‌ای۳

۳,۲= VH	۳,۱=VH	۳
۰/۷	۰/۹	VH
۰/۲	۰/۱	H
۰/۱	۰/۰۰۰۱	M
۰/۰۰۰۱	۰/۰۰۰۱	L
۰/۰۰۰۱	۰/۰۰۰۱	VL
۳,۲= H	۳,۱=H	۳
۰/۵	۰/۹	VH
۰/٤	۰/۱	H
۰/۱	۰/۰۰۰۱	M
۰/۰۰۰۱	۰/۰۰۰۱	L
۰/۰۰۰۱	۰/۰۰۰۱	VL
۳,۲= M	۳,۱=M	۳
۰/۲	۰/۲	VH
۰/۵	۰/۵	H
۰/۳	۰/۳	M
۰/۰۰۰۱	۰/۰۰۰۱	L
۰/۰۰۰۱	۰/۰۰۰۱	VL
۳,۲= L	۳,۱=L	۳
۰/۰۰۰۱	۰/۰۰۰۱	VH
۰/۰۰۰۱	۰/۰۰۰۱	H
۰/٤	۰/۵	M

L	۰/۳	۰/٤
VL	۰/۲	۰/۲
۳	**۳,۱=VL**	**۳,۲=VL**
VH	۰/۰۰۰۱	۰/۰۰۰۱
H	۰/۰۰۰۱	۰/۰۰۰۱
M	۰/۵	۰/۳
L	۰/۳	۰/٤
VL	۰/۲	۰/۳

احتمالات شرطی ترکیبی

$$P(3 = VH \mid 3.1 = VH, 3.2 = VH) = \alpha\, P(3 = VH \mid 3.1 = VH) P(3 = VH \mid 3.2 = VH)$$

که در این رابطه α برابر است با:

$$\alpha = \frac{1}{k}$$

$$\begin{aligned} k = {} & P(3 = VH \mid 3.1 = VH) P(3 = VH \mid 3.2 = VH) \\ & + P(3 = H \mid 3.1 = VH) P(3 = H \mid 3.2 = VH) \\ & + P(3 = M \mid 3.1 = VH) P(3 = M \mid 3.2 = VH) \\ & + P(3 = L \mid 3.1 = VH) P(3 = L \mid 3.2 = VH) \\ & + P(3 = VL \mid 3.1 = VH) P(3 = VL \mid 3.2 = VH) \end{aligned}$$

بنابراین:

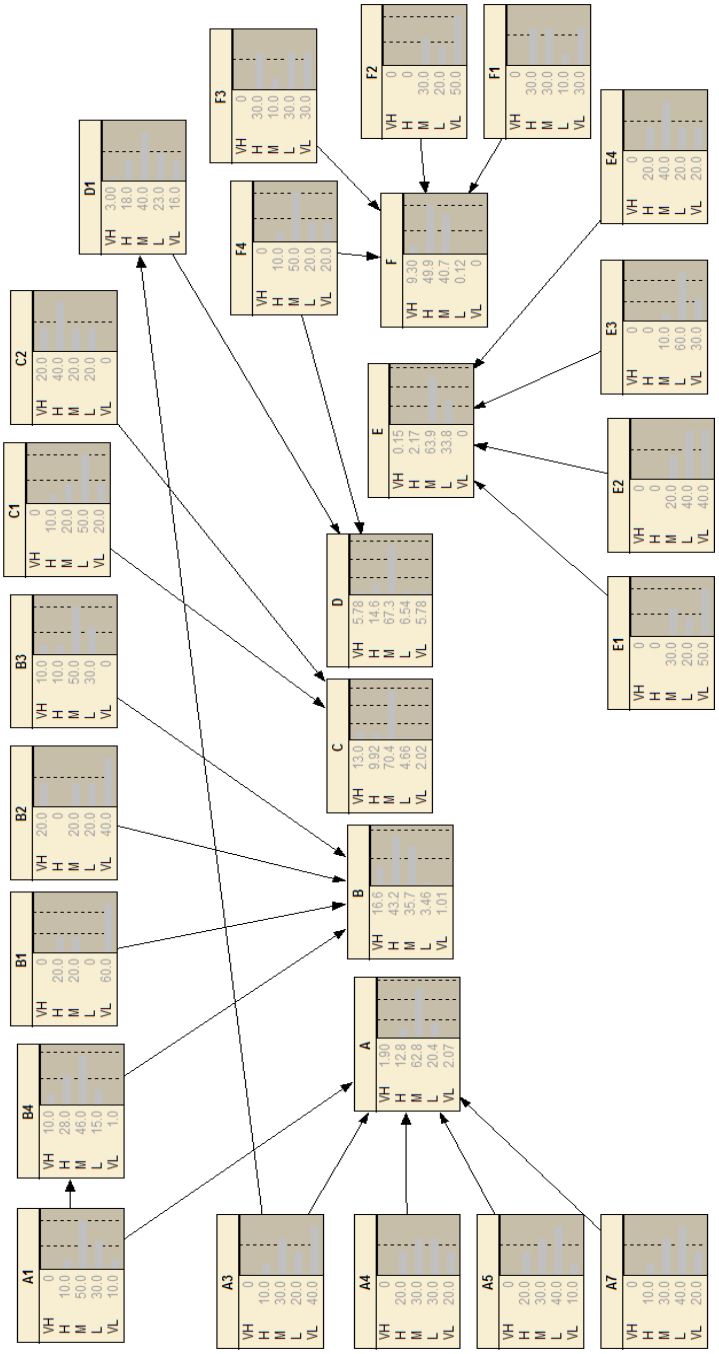
$$P(3 = VH \mid 3.1 = VH, 3.2 = VH) = 0.97$$
$$P(3 = H \mid 3.1 = VH, 3.2 = VH) = 0.03$$
$$P(3 = M \mid 3.1 = VH, 3.2 = VH) = 0$$
$$P(3 = VL \mid 3.1 = VH, 3.2 = VH) = P(3 = L \mid 3.1 = VH, 3.2 = VH) = 0$$
$$0$$

دیگر احتمالات شرطی نیز به همین ترتیب محاسبه گردیده است.

پس از ساخت شبکه و تعیین احتمالات اولیه و شرطی برای همه فاکتورها و زیر فاکتورها ، مدل در نرم‌افزار نتیکا اجرا شده‌است. نتیکا،نرم‌افزاری مربوط به شبکه‌های بیزین می‌باشد. در نرم‌افزار نتیکا ابتدا شبکه بیزین، (گره‌ها و لبه‌ها)، ترسیم شده و با توجه به حالت‌های موجود برای هر گره، احتمالات شرطی(CPT)های شبکه را کامل کرده، و در انتها احتمال گره نهایی به عنوان خروجی از نرم‌افزار دریافت می‌شود.

شکل ۲ خروجی نرم‌افزار نتیکا را نشان می‌دهد.

شکل ۲ : خروجی نرم‌افزار نتیکا



بر اساس خروجی نرم‌افزار نتیکا، احتمالات فاکتورهای ریسک مشخص شده است. برای تعیین اهمیت فاکتورها، به هر حالت یک ضریب اهمیت احتمال اختصاص داده‌شده است. اهمیت حالت(VH) برابر با ۱، اهمیت حالت(H) برابر با ۰/۷۵، اهمیت حالت(M) برابر با ۰/۵، . اهمیت حالت(L) برابر با ۰/۲۵ و اهمیت حالت(VL) برابر با صفر در نظر گرفته شده‌است. و با استفاده از روابط فوق، اهمیت احتمال ریسک‌ها تعیین گردیده و در جدول ۷ ارائه شده‌است.

جدول ۷: اهمیت احتمال فاکتورها و زیر فاکتورهای ریسک

فاکتور۱ ۰/٤۸	اهمیت	فاکتور۲ ۰/٦۸	اهمیت	فاکتور۳ ۰/۵۷	اهمیت	فاکتور٤ ۰/۵۲	اهمیت	فاکتور۵ ۰/٤۲	اهمیت	فاکتور٦ ۰/٦۷	اهمیت
۱,۱	۰/۴	۲,۱	۰/۲۵	۳,۱	۰/۳۰	۴,۱	۰/۴۲	۵,۱	۰/۴۲	۶,۱	۰/۴
۱,۲	۰/۲۸	۲,۲	۰/۳۵	۳,۲	۰/۶۵			۵,۲	۰/۲	۶,۲	۰/۲
۱,۳	۰/۳۸	۲,۳	۰/۵۰					۵,۳	۰/۲	۶,۳	۰/۳۵
۱,۴	۰/۴۰	۲,۴	۰/۵۸					۵,۴	۰/۴	۶,۴	۰/۳۸
۱,۵	۰/۳۳										

نتایج ارائه شده در جدول۷ مشخص می‌کند که کدام فاکتورها و کدام زیر فاکتورهای ریسک اهمیت(احتمال) بالاتری دارند.

محاسبه حاصلضرب اهمیت در شدت اثر ریسک و اولویت‌بندی ریسک‌ها

برای پاسخ به سوال اصلی پژوهش(مبنی بر اینکه کدامیک از ریسک‌های امنیت اطلاعات سازمانی اولویت بالاتری دارند؟) احتمالات بدست آمده از مرحله سوم (اهمیت فاکتورها) در شدت‌های حاصل از مرحله چهارم ضرب شده و اولویت نهایی هر عامل محاسبه شده‌است. با توجه به نتایج حاصل، ریسک‌های ۶(عدم وجود سیستم‌های کنترلی مناسب)، ۳(عدم امنیت عامل انسانی)، ۲(عدم تعهد مدیریت عالی)، ۵(عدم امنیت در شبکه‌ها و تجارت الکترونیک)،۴ (عدم امنیت سیستم‌ها و تجهیزات فیزیکی)، ۱(نبود خط مشی امنیت)، به ترتیب دارای بیشترین اولویت تا کمترین اولویت می‌باشند. اولویت بندی زیر فاکتورها در جدول ۸ ارائه شده‌است.

جدول۸- اولویت‌بندی ریسک‌های امنیت اطلاعات

۳,۲	عدم آگاهی و عدم ارائه آموزشهای مناسب در حوزه امنیت اطلاعات
٤,۱	عدم تعریف دسترسی‌های مناسب
٦,٤	عدم وجود اقدامات پیشگیرانه، اکتشافی و اصلاحی(به روزرسانی نرم‌افزارهای امنیتی) برای حفاظت از سیستم اطلاعات بانک از نرم افزارهای مخرب)مانند ویروس ها، کرم ها، جاسوس افزارها، اسپم
۳,۱	نبود نیروی انسانی متخصص در زمینه امنیت اطلاعات
٦,۱	عدم کنترل در صحت داده‌های ورودی،پردازش‌های درونی، یکپارچگی پیغام و صحت داده‌های خروجی
۲,٤	نداشتن یک طرح کلی برای امنیت اطلاعات و سرمایه‌گذاری‌های مناسب و متناسب با اولویت‌های امنیتی بانک
۱,۱	عدم وجود یک خط مشی امنیت اطلاعات جامع و کامل و قابل بازنگری
٦,۳	عدم گزارش‌دهی رویدادها و ضعف‌های امنیتی
۱,۳	عدم وجود رویه‌ای مناسب در طبقه‌بندی و کدگذاری اطلاعات
٥,۲	عدم وجود امنیت در خدمات شبکه
۱,٤	عدم انطباق سیستم‌ها با خط مشی‌ها و استانداردهای امنیتی بانک
۲,۱	نبود تعهد و حمایت مدیریت بانک نسبت به امنیت اطلاعات بانک
٥,۳	عدم وجود امنیت درفرایند تبادل اطلاعات و نرم‌افزارها درون یک بانک و یا با هر موجودیت بیرونی
۲,۲	عدم تخصیص بودجه مناسب به طرح امنیت
٥,۱	عدم ایجاد نسخه پشتیبان و عدم یکپارچگی و دسترس‌پذیری اطلاعات و امکانات پردازش اطلاعات
۲,۳	عدم توجه و زمانبندی جهت پیاده‌سازی و اجرایی نمودن طرحها
۱,٥	عدم مدیریت حوادث و ضعف‌های امنیت اطلاعات
۱,۲	روشن نبودن تعریف مسئولیت امنیت اطلاعات در بانک
٦,۲	عدم نظارت و پایش در توسعه نرم‌افزارهای برون‌سپاری شده
٥,٤	عدم امنیت در خدمات تجارت الکترونیکی شامل دادو ستدهای آنلاین و اطلاعات در دسترس عموم

نتیجه‌گیری

چارچوب ارائه شده در این پژوهش یک مدل ارزیابی ریسک مبتنی بر استاندارد ایزو و چارچوب کوبیت است که ریسک‌های امنیت اطلاعات سازمانی را به عنوان یک شبکه باور بیزی در نظر گرفته و سطح ریسک امنیت اطلاعات را به عنوان ترکیبی از احتمال وقوع و تخمین شدت اثر هر ریسک برآورد می‌نماید.پژوهش حاضر به طور خلاصه در چهار مرحله انجام گرفته است:

مرحله اول؛ شناسایی ریسک‌های امنیت اطلاعات سازمانی

مرحله دوم؛ تعیین میزان شدت ریسک‌های امنیت اطلاعات با استفاده از AHP فازی

مرحله سوم؛ تعیین احتمال ریسک‌های امنیت اطلاعات با بکارگیری شبکه بیزین

مرحله چهارم؛ اولویت‌بندی نهایی فاکتورهای ریسک امنیت اطلاعات

با توجه به نتایج ارزیابی ریسک و اولویت‌بندی ریسک‌های امنیت اطلاعات، که در این پژوهش انجام شده‌است، "عدم آگاهی و عدم ارائه آموزش‌های مناسب در حوزه امنیت اطلاعات"، "عدم تعریف دسترسی‌های مناسب" و "عدم وجود اقدامات پیشگیرانه، اکتشافی و اصلاحی" به عنوان ریسک‌هایی با اولویت بالا شناسایی گردیدند. لذا به منظور کاهش و کنترل آن‌ها، ارائه راهکارهای مدیریتی مبتنی بر مدیریت ریسک، لازم به نظر می‌رسد. از سوی دیگر ریسک‌های "روشن نبودن تعریف مسئولیت امنیت اطلاعات در بانک"، "عدم نظارت و پایش در توسعه نرم‌افزارهای برون‌سپاری شده" و "عدم امنیت در خدمات تجارت الکترونیکی شامل داد و ستدهای آنلاین و اطلاعات در دسترس عموم" اولویت پایینی دارند و نسبت به سایر ریسک‌ها به توجه و صرف زمان و هزینه کمتری نیاز دارند.

همانگونه که پیش از این نیز گفته شد برای تأمین امنیت اطلاعات در یک سازمان فقط تأمین تجهیزات سخت افزاری و نرم‌افزاری کافی نیست بلکه لازم است فرآیندهای مرتبط با امنیت اطلاعات در سازمان نیز اصلاح شوند. استاندارد جهانی ایزو ۲۷۰۰۲ و کوبیت۴، استانداردهای شناخته شده‌ای هستند که می‌توان برای پیاده‌سازی سیستم مدیریت امنیت اطلاعات از آنها بهره برد. طراحی یک سیستم امنیت اطلاعات سازمانی مبتنی بر استاندارد ایزو ۲۷۰۰۲ و

کوبیت۴، و نیز انجام پژوهش‌هایی مشابه پژوهش حاضر در دیگر سازمان‌هایی که اولویت نیازمندی‌های امنیت اطلاعات در آنها بالاست، انجام این پژوهش با بکارگیری تحلیل حساسیت در شبکه بیزین به منظور اولویت‌بندی ریسک‌ها و یا استفاده از سایر روش‌هایی مثل الگوریتم‌های فراابتکاری و روشهای (MCDM) با رویکرد ترکیبی پیرامون امنیت اطلاعات سازمانی، برای پژوهش‌های آتی می‌تواند مناسب باشد.

منابع

آذر، عادل؛ فرجی، حجت. (۱۳۸۱)، *علم مدیریت فازی*. چاپ اول، اجتماع، تهران

الفت، لعیا؛ خسروانی،فرزانه؛ جلالی، رضا.(۱۳۸۹). *شناسایی و اولویت‌بندی ریسک پروژه بر مبنای استاندارد PMBOK با رویکرد فازی*. فصلنامه علمی پژوهشی مطالعات مدیریت صنعتی۸ (۱۹)، ۱۶۳-۱۴۷

اولین چهارسوقی، صدیقه؛ دوستاری، محمدعلی؛ یزدیان ورجانی،علی؛ مهدوی اردستانی، سید علیرضا. (۱۳۹۲). *بکارگیری شبکه های عصبی مصنوعی در ارزیابی ریسک امنیت اطلاعات*. مجله علمی پژوهشی پدافند الکترونیکی و سایبری. (۴) ۲۳-۳۳

بیگلربگیان، پریسا. (۱۳۹۱). *تدوین شاخص‌های ارزیابی امنیت اطلاعات سازمان(مورد مطالعه: سازمان بورس و اوراق بهادار تهران)*.پایان نامه کارشناسی ارشد. دانشگاه الزهراء علیها السلام

جعفرنژاد، احمد؛ یوسفی زنوز، رضا.(۱۳۸۷). *ارائه مدل فازی رتبه‌بندی ریسک در پروژه‌های حفاری شرکت پتروپارس. نشریه مدیریت صنعتی دانشگاه تهران*، ۱ (۱) : ۳۸-۲۱

خواجویی، حمید. (۱۳۹۰). *مطالعه کنترل‌های امنیت اطلاعات بر اساس استانداردهای بین المللی*. پایان نامه کارشناسی ارشد . دانشگاه سیستان و بلوچستان

شفیعی نیک‌آبادی، محسن؛ جعفریان احمد؛ جلیلی بوالحسنی اعظم.(۱۳۸۹). *تاثیر مدیریت امنیت اطلاعات بر یکپارچگی فرایندهای سازمانی در زنجیره تامین. پژوهشنامه پردازش و مدیریت اطلاعات،۲(۶۸): ۴۴-۲۷*

عالم‌تبریز،اکبر؛ حمزه‌ای،احسان. (۱۳۹۰). *ارزیابی و تحلیل ریسک‌های پروژه با استفاده از رویکرد تلفیقی مدیریت ریسک استاندارد PMBOK و تکنیک RFMEA*، فصلنامه علمی پژوهشی مطالعات مدیریت صنعتی۹(۲۳)، ۱-۱۹

عیسوی، هیرو. (۱۳۹۰). *بررسی ریسک عملیاتی مربوط به امنیت اطلاعات در سامانه بانکداری مدرن*. پایان نامه کارشناسی ارشد. دانشگاه گیلان

کریمی، زهرا. (۱۳۸۵). *ارائه مدل مفهومی ارزیابی ریسک امنیت اطلاعات: مورد بانک سپه*. پایان نامه کارشناسی ارشد. دانشگاه الزهرا

میرفخرالدینی، سیدحیدر؛ عندلیب اردکانی، داود؛ رضایی اصل،مرتضی.(۱۳۹۰). *بکارگیری فنون تصمیم‌گیری چندشاخصه جهت ارزیابی عوامل ریسک زنجیره تامین. فصلنامه علمی پژوهشی مطالعات مدیریت صنعتی*۸(۲۱)، ۱۰۷-۱۳۰

ناظمی، شمس‌الدین؛ کاظمی، مصطفی؛ اخروی، امیرحسین.(۱۳۹۰). *ارائه مدل تلفیق شکاف عملکردی با AHP گروهی-فازی برای تعیین اولویت‌های بهبود. مجله مدل‌سازی در مهندسی*، ۹(۲۷)

BS ISO/IEC27005:2008. *Information technology-Security techniques -Information security risk management*.

Chi-Chun Lo & Wan-Jia Chen. (2012*). hybrid information security risk assessment procedure considering interdependences between controls. Expert Systems with Applications*.(39),247-257 .

D.D. Wu, K. Xie, G. Chen, P. Gui. (2010). *A risk analysis model in concurrent engineering product development.* Risk Analysis.

Daniel Feledi, Stefan Fenz & Lukas Lechner.(2013*) Toward web-based information security knowledge sharing.* information security technical report ,17(2013) ,199-209.

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(2014): 57-73

Haslum. K, Abraham. A & Kanpskog. S. (2008*). "Fuzzy Online Risk Assessment for Distributed Intrusion Prediction and Prevention Systems" Proc.* Tenth International Conference on computer Modeling and Simulation, Combridge, USA.

Imamverdiev Ya. N & Derakshande S. A. (2011). *Fuzzy OWA Model for Information Security Risk Management.* AUTOMATIC CONTROL AND COMPUTER SCIENCES . 1(2011)20-28.

ISO/IEC27001. (2005). *Information technology-Security techniques-Information security management systems Requirements*.

Kevin B. Corb & Ann E.Nicholson.(2004). *Bayesian artificial intelligence, Boca Raton London New York Washington,* D.C. chapman & hall.

korb KB & Nicholson AE. (2004*). Bayesian Artificial Intelligence*. CHAPMAN & HALL/CRC.

Nan Feng & Minqiang Li. (2011). *An information systems security risk assessment model under uncertain environment*.Applied Soft Computing.

Robert E. Crossler . Allen C. Johnston, Paul Benjamin Lowry, Merrill Warkentin, Richard Baskerville, Qing H. (2013). *Future directions for behavioral information security research, computers & security,* 32(2013)90-101.

Rossouw von Solms & Johan van Niekerk. (2013). *From information security to cyber security.* computers & security,38(2013), 97-102

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

Stefan Wagner. (2010*). A Bayesian network approach to assess and predict software quality using activity-based quality models.* Information and Software Technology.

Tongwei yuan & Peng Chen. (2012) . *Data Mining Applications in E- Government Information Security.* Procedia Engineering

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.

Wang. Z,Zeng. H. (2010). *Study on the Risk Assessment Quantitative Method of Information Security Proc*. 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)

Wei. G, Zhang,. X,Zhang. X & Huang. Z. (2010). *"Research on E-government information security risk assessment Based on Fuzzy AHP and Artificial Neural Network model," proc.* First International Conference on Networking and Distributed Computing.

Yu-Ping Ou Yang, How-Ming Shieh & Gwo-Hshiung Tzeng. (2013). *A VIKOR technique based on DEMATEL and ANP for information security risk control assessment ,* Information Sciences.