

## ارزیابی سطح امنیت در تجارت الکترونیک با استفاده از آنتروپی شانون و تئوری دمپستر. شافر

مریم حاج‌ملک<sup>۱</sup>، احمد توکلی<sup>۲</sup>

**چکیده:** هدف پژوهش حاضر، توسعه روش و ساختاری است که بتوان از طریق آن به ارزیابی امنیت در تجارت الکترونیک شرکت‌های مختلف با بهره‌مندی از نظر کارشناسان مختلف پرداخت. در این پژوهش، روش آنتروپی شانون در کنار تئوری دمپستر- شافر قرار گرفته است تا از این طریق بتوان سطح نهایی امنیت را اندازه‌گیری کرد. با توجه به اینکه پژوهش حاضر مبتنی بر تیم تصمیم برای جمع‌آوری داده است، جمع‌آوری داده‌ها در دو مرحله به اجرا درآمد؛ در مرحله اول داده‌های مختص به تعیین وزن معیارها گردآوری شدند و در مرحله بعد داده‌های سطح امنیت معیارها با برگزاری مصاحبه و بهره‌مندی از تیم تصمیم چهار شرکت بازرگانی شهر مشهد که آماده همکاری بودند، جمع‌آوری شدند. سپس میزان اهمیت معیارهای امنیت، سطح امنیت هر معیار و سطح کلی امنیت در شرکت‌های بازرگانی مطالعه شده تعیین شد. نتایج نهایی پژوهش نشان داد سطح کلی امنیت برای سه شرکت بالاست، اما برای شرکت چهارم متوسط است.

واژه‌های کلیدی: آنتروپی شانون، امنیت، تجارت الکترونیک، دمپستر- شافر، عدم قطعیت.

۱. کارشناس ارشد مدیریت بازرگانی، دانشکده علوم اداری و اقتصاد، دانشگاه فردوسی مشهد، مشهد، ایران

۲. استادیار گروه مدیریت دانشکده علوم اداری و اقتصاد، دانشگاه فردوسی مشهد، مشهد، ایران

تاریخ دریافت مقاله: ۱۳۹۳/۱۰/۱۳

تاریخ پذیرش نهایی مقاله: ۱۳۹۴/۰۹/۱۱

نویسنده مسئول مقاله: مریم حاج‌ملک

E-mail: mhajmalek90@yahoo.com

## مقدمه

در دنیای امروز موفقیت راهبرد جهش صادراتی، مستلزم شناسایی تحولات جهشی، مانند تجارت الکترونیک در عرصه تجارت بین‌الملل است (خداداد حسینی و فتحی، ۱۳۸۱) و باید در نظر داشت که تجارت الکترونیک و جهانی‌شدن دو پدیده بسیار مهم و بحث‌انگیز جهان امروز است که فرصت‌های زیادی را برای بنگاه‌ها ایجاد می‌کنند و بنگاه‌ها با استفاده از این فرصت‌ها می‌توانند موفقیت خود را در بازار جهانی تضمین کنند (صباغ کرمانی و اسفیدانی، ۱۳۸۴)، البته با توجه به تحولات زیادی که در سال‌های گذشته در عرصه تجارت الکترونیک رخ داده است، شاهد هستیم که هزاران سازمان به کمک سرمایه‌داران بزرگ پا به عرصه تجارت الکترونیک گذاشته و می‌گذارند؛ ولی بسیاری از آنها با ناکامی مواجه شده‌اند. بنابراین با وجود رشد سریع تجارت الکترونیک، محدودیت‌هایی مانع گسترش آن می‌شوند. باید در نظر داشت که اطلاعات در سیستم‌های رایانه‌ای مجزا از یکدیگر، حالتی کاملاً ایستا دارند، بنابراین حفظ امنیت آن چندان مسئله دشواری نیست؛ اما با اتصال گسترده رایانه‌ها و پیدایش شبکه ارتباطی، اطلاعات به‌عنوان مهم‌ترین کالای این عرصه دیگر مقیم رایانه خاصی نیست و در پهنای شبکه گسترده ارتباطی، دائم نقل مکان می‌کنند (جعفری، ۱۳۸۵). این حرکت سبب می‌شود که حفظ امنیت اطلاعات به مقوله‌ای بسیار دشوارتر از پیش تبدیل شود. از سوی دیگر، افزایش استفاده از ایمیل برای تبادل اطلاعات و معاملات آنلاین در سازمان‌ها، سبب افزایش نیاز به ارتباطات امن شده است؛ به‌خصوص با پیشرفت و هوشمندی روزافزون حملات کلاه‌برداری، ره‌گیری انتقال و سایر روش‌های هک. بنابراین اگر شرکتی خود را به سیستم تجارت الکترونیک مجهز کند و خواهان دست‌یافتن به پتانسیل واقعی تجارت الکترونیک باشد، باید زیرساخت‌های لازم و مطرح در این حوزه را نیز در نظر بگیرد. درحالی‌که ریسک‌های زیادی در زمینه اینترنت و محیط شبکه برای تجارت الکترونیک وجود دارد، امنیت می‌تواند مانند ابزاری برای جلوگیری یا حداقل کردن ریسک استفاده شود (جاروپان فول و بواتن، ب. ت.).

از سوی دیگر، معرفی دائم فناوری‌های جدید سبب می‌شود مشکل تأمین امنیت سیستم‌های وب، بیشتر به چالش کشیده شود (گوسوا پاپس توجناوا، آنوستاسوسکی، دیمتری جوک، پانتو و میلر، ۲۰۱۴) و با توجه به نقش محوری فناوری اطلاعات<sup>۱</sup> در شرکت‌های امروزی و اهمیت اطلاعات به‌عنوان دارایی‌های ارزشمند هر سازمان، امنیت اطلاعات به یکی از مؤلفه‌های کلیدی مدیریت و برنامه‌ریزی در شرکت‌های مدرن تبدیل شده است. کرونین (۱۹۹۵) بر این باور است که مسائل خصوصی مانند امنیت، سانسور و استراق سمع، می‌تواند ارتباطات را سست کند،

1. Information Technology

در نتیجه می‌توان امنیت را پایه‌ای برای یکپارچگی و رشد کسب‌وکار الکترونیکی شمرد (کرونین ۱۹۹۵، به نقل از الجفیری، پونز و کالینز، ۲۰۰۳) و آن را یکی از مؤلفه‌های اساسی مدیریت و برنامه‌ریزی شرکت‌های مدرن در نظر گرفت.

شایان ذکر است که مدیریت امنیت اطلاعات، از شرکت‌ها در برابر طیف وسیعی از تهدیدها به‌منظور اطمینان از تداوم کسب‌وکار، به حداقل رساندن آسیب‌ها و حداکثر کردن بازده سرمایه‌گذاری محافظت می‌کند. البته امنیت کلی یک سیستم از طریق در نظر گرفتن عوامل فیزیکی مانند سخت‌افزار، منطقی از قبیل نرم‌افزار و اقدامات امنیت سازمانی برقرار می‌شود؛ بنابراین، روش بهتر برای ارزیابی امنیت، تجزیه و تحلیل حمله‌های داخلی و خارجی است (کیرسیبلیک و ونهوک، ۲۰۰۶).

با توجه به مفاهیم بیان شده و عنوان مقاله، هدف اصلی پژوهش حاضر، تعیین سطح امنیت تجارت الکترونیک شرکت‌های بازرگانی مطالعه شده است. با توجه به این هدف، اهداف فرعی مد نظر این پژوهش عبارت‌اند از: شناسایی معیارهای مطرح در زمینه امنیت تجارت الکترونیک؛ تعیین سطح اهمیت هر معیار و در نهایت تعیین سطح امنیت هر معیار در شرکت‌های بازرگانی مطالعه شده. براساس اهداف یادشده، سؤال‌های این پژوهش به شرح زیر است:

۱. مؤلفه‌های مهم امنیت در تجارت الکترونیک چیست؟
۲. ساختار مناسب برای اندازه‌گیری امنیت در تجارت الکترونیک چیست؟
۳. وزن هر یک از مؤلفه‌ها و شاخص‌ها با توجه به روش آنتروپی شانون چقدر است؟
۴. سطح کلی امنیت تجارت الکترونیک در شرکت‌های بازرگانی مد نظر چقدر است؟

### پیشینه نظری پژوهش

فناوری یکی از ابزارهای برقراری ارتباط با محیط به‌شمار می‌رود. تاریخ بشریت بیان‌کننده این مطلب است که انسان از همان ابتدا برای ادامه حیات خود به فناوری روی آورده است (مؤمنی، ۱۳۸۰، به نقل از محبوب عشرت‌آبادی، میرکمالی، اسماعیل مناپ و مهری، ۱۳۹۲).

در دنیای امروز با توجه به پیشرفت روزافزون فناوری در حوزه کسب‌وکار، عمده نگرانی و تلاش سازمان‌ها بقا و توسعه در این وضعیت است و در این راستا، مسئله امنیت اطلاعات سازمانی و حفاظت از آن اهمیت بسیاری یافته است. برای محافظت از اطلاعات سازمان، نمی‌توان به نوع خاصی از امنیت یا به محصولی خاص اکتفا کرد (میوالد، ۱۳۸۳، به نقل از تاج‌فر، محمودی میمند، رضا سلطانی و رضا سلطانی، ۱۳۹۳). در ادامه به‌منظور شفاف‌تر شدن موضوع، به بررسی پیشینه پژوهش می‌پردازیم.

### تجارت الکترونیک و تعریف آن

به دلیل گستردگی حوزه تجارت الکترونیک، برای آن تعاریف بسیاری بیان شده است و از مجموع آنها می‌توان دریافت که تجارت الکترونیک کاربردهای وسیعی دارد. گفتنی است بیش از ۳۰ نوع فناوری وجود دارد که از آنها در تعریف تجارت الکترونیک استفاده شده است و این موضوع گستردگی تجارت الکترونیک را نشان می‌دهد. توربان (۲۰۰۶) تجارت الکترونیک را فرایند خرید، فروش، انتقال یا مبادله محصولات، خدمات یا اطلاعات از طریق شبکه رایانه و اینترنت، تعریف کرد (توربان، ۲۰۰۶، به نقل از شاهیبی و وان فیکه، ۲۰۱۱). در تعریف دیگری آلفردو ریال (۲۰۱۳)، تجارت الکترونیک را خرید و فروش محصولات و خدمات به کمک شبکه ارتباطات از راه دور، به خصوص هنگامی که از سیستم پرداخت آنلاین استفاده شود، بیان کرده است که محصولات و خدمات می‌توانند هم فیزیکی و هم دیجیتالی باشند. شایان ذکر است که کسب و کار الکترونیک مفهومی عام‌تر از تجارت الکترونیک دارد و می‌توان گفت تجارت الکترونیک بیشتر به ارتباطات بیرونی بنگاه یا فرد تکیه می‌کند، اما کسب و کار الکترونیک علاوه بر ارتباطات بیرونی، به راهکارهای درون سازمان نیز اشاره دارد. بنابراین کسب و کار الکترونیک شامل موارد زیر است: کسب و کار الکترونیک = تجارت الکترونیک + هوشمندی شرکت‌ها + مدیریت روابط با مشتری + مدیریت زنجیره تأمین + مدیریت برنامه‌ریزی منابع شرکت<sup>۱</sup> (صنایعی، ۱۳۸۳).

### امنیت در تجارت الکترونیک

با پیشرفت سریع فناوری اطلاعات و جایگزینی تجارت آنلاین (تجارت از طریق اینترنت) با تجارت سنتی، مسائل امنیت، به‌ویژه برای کسب و کارها در محیط تجارت الکترونیک، اهمیت یافته است.

در تعریف امنیت می‌توان گفت که امنیت به مجموعه تدابیر، روش‌ها و ابزار برای جلوگیری از دسترسی و تغییرات غیرمجاز در نظام رایانه‌ای گفته می‌شود و امنیت اطلاعات به حفاظت از اطلاعات و به حداقل رساندن خطر افشای آنها در بخش‌های غیرمجاز اشاره دارد (قاسمی شبانکاره، مختاری و امینی لاری، ۱۳۸۶). با توجه به مباحث یادشده، در پژوهش حاضر معیارهای امنیتی تجارت الکترونیک، با در نظر گرفتن چهار معیار اصلی الزامات امنیتی، سیاست‌های امنیتی، مشخصات زیرساخت‌های امنیتی و پیاده‌سازی آنها و آزمایش‌های امنیتی، تعیین شدند که در ادامه به بررسی این معیارها می‌پردازیم.

1. EB= EC+ BI+ CRM+ SCM+ ERP

### الزامات امنیتی در تجارت الکترونیک

نیاز به نگرش جامع در زمینه امنیت و همچنین الزامات امنیتی، از دیدگاه وان سولمز (۲۰۰۱)، سرچشمه می‌گیرد؛ او امنیت را بحثی چندبعدی می‌داند. زوکاتو (۲۰۰۲) نیز در این زمینه نگرش جامعی را ارائه داد و جنبه‌های مختلف و روابط آنها را در مواجهه با ابعاد مختلف امنیت، بررسی کرد (وان سولمز، ۲۰۰۱؛ زوکاتو، ۲۰۰۲، به نقل از زوکاتو، ۲۰۰۴). از این رو باید در نظر داشت که نیازهای امنیتی راضی‌کننده سیستم باید همچون الزامات امنیتی در نظر گرفته شوند. در مقاله زوکاتو (۲۰۰۴)، تشخیص الزامات توسط منابع کسب‌وکار، محیط و مدیریت ریسک، پیشنهاد شد. از آنجا که فعالیت مهم در بخش مهندسی الزامات امنیتی، گردآوری آنها از منابع مختلف در یک مجموعه است؛ برای تشخیص چگونگی امنیت سیستم، باید الزامات براساس اهمیت و امکان‌پذیری طبقه‌بندی شوند (زوکاتو، ۲۰۰۴، به نقل از زوکاتو، ۲۰۰۷).

### سیاست‌های امنیتی در تجارت الکترونیک

با توجه به تهدیدهای زیادی که امروزه در محیط‌های سایبری وجود دارد، سازمان‌ها به کنترل‌های امنیتی برای محافظت از اطلاعات با ارزش خود نیاز دارند. براساس دیدگاه هون و الوف (۲۰۰۲)، بی‌شک یکی از کنترل‌های مهم، سیاست امنیت اطلاعات است. در همین راستا، وایتمن، تاوژند و آلبرتز (۲۰۰۱) بیان کردند توسعه سیاست امنیت اطلاعات، اولین گام در جهت آماده‌شدن سازمان در برابر حملات منابع داخلی و خارجی است (هون و الوف، ۲۰۰۲؛ وایتمن، تاوژند و آلبرتز، ۲۰۰۱، به نقل از کنپ، موریس، مارشال و برد، ۲۰۰۹). از جهتی دیگر، به‌منظور اثربخشی مدیریت امنیت، باید عوامل فنی و اجتماعی به‌طور هم‌زمان در نظر گرفته شوند. درواقع سیاست‌های امنیتی، این عناصر را در برنامه منسجمی که سازمان برای اجرای امنیت به‌کار می‌برد، ادغام می‌کند (پارکر، ۱۹۹۸؛ بارمن، ۲۰۰۲؛ بسکرویل و سپیون، ۲۰۰۲؛ گول، پون و منزیس، ۲۰۰۶، به نقل از گول و چنگالر اسمیت، ۲۰۱۰).

### مشخصات زیرساخت‌ها و پیاده‌سازی مباحث امنیتی

رشد تجارت الکترونیک، نیازمند زیرساخت‌های انعطاف‌پذیری است که می‌توان آنها را در دو حوزه خرد و کلان در نظر گرفت. حوزه کلان مختص به زیرساخت‌هایی است که باید آنها را دولت فراهم کند و حوزه خرد زیرساخت‌هایی را شامل می‌شود که هر سازمان به‌طور جداگانه باید برای خود فراهم می‌کنند؛ اما متأسفانه کشورهای در حال توسعه، معمولاً با کمبود زیرساخت‌های ارتباطی خوب مواجه‌اند. در نتیجه مردم و کسب‌وکارها در کشورهای در حال توسعه نمی‌توانند

بدون زیرساخت‌های کافی در تجارت الکترونیک سرمایه‌گذاری کنند (الجفیری، پونز و کالینز، ۲۰۰۳).

### آزمایش‌های امنیتی در تجارت الکترونیک

آزمایش‌های امنیتی به منظور بررسی اثربخشی زیرساخت‌های امنیتی، عملکرد سازوکار کنترل دسترسی، زمینه عملیاتی مشخص شده و آسیب‌پذیری‌های شناخته‌شده در زیرساخت‌ها اجرا می‌شوند و به سازمان‌ها در شناسایی ضعف‌های سیستم تجارت الکترونیک خود کمک می‌کنند. به‌طور کلی، می‌توان دو نوع آزمایش را در زمینه امنیتی نام برد: آزمایش پذیرش و آزمایش نفوذ. در آزمون پذیرش بررسی می‌شود که زیرساخت‌های امنیتی به اجرا درآمده منطبق بر سیاست‌های امنیتی سازمان است یا خیر و در آزمایش نفوذ به این موضوع پرداخته می‌شود که زیرساخت‌های امنیتی موجود برای دفع تمام تهدیدهای امنیتی ممکن تا چه اندازه کافی است (سنگوپتا، مزومدار و باریک، ۲۰۰۵).

### عدم قطعیت

تصمیم‌گیری در وضعیت عدم قطعیت یکی از مسائل مهم در حوزه سیستم‌های کنترل و خیره است؛ از این رو عامل پیچیده توسعه پشتیبانی تصمیم و سیستم‌های کارشناسی، بررسی قضاوت‌های غیرقطعی است. در سال‌های اخیر مجامع علمی و مهندسی تعاریف سودمندی از عدم قطعیت ارائه دادند. ماهیت دوگانه عدم قطعیت با تعاریف زیر از هلتنون (۱۹۹۷)، بیان شده است:

- عدم قطعیت نامعلوم؛ در نتیجه این واقعیت است که سیستم می‌تواند به‌طور تصادفی عمل کند.
- عدم قطعیت معرفت‌شناختی؛ در نتیجه کمبود دانش درباره سیستمی خاص روی می‌دهد و از ویژگی‌های عملکرد تحلیلگران، هنگام تجزیه و تحلیل است (هلتنون، ۱۹۹۷، به نقل از سنتز و فرسون، ۲۰۰۲).

### تئوری دمپستر – شافر

در زمان عدم قطعیت، ادغام داده‌ها اهمیت بسیاری دارد که برای این منظور تئوری بیزین، منطق فازی و تئوری شواهد روش‌های مؤثری شناخته شده‌اند. توافق عامی در زمینه کاربرد جهانی

---

1. Aleatory Uncertainty  
2. Epistemic Uncertainty

روش‌ها وجود ندارد، اما تئوری دمپستر- شافر یکی از تئوری‌های محبوب شمرده می‌شود که برای مدل‌سازی و استدلال هنگام عدم قطعیت و دقت، در سیستم‌های هوشمند به کار می‌رود. در نظریه دمپستر- شافر، قاعده ترکیب دمپستر، ابزار قدرتمندی است که برای ترکیب شواهد از منابع اطلاعاتی متمایز اهمیت بسزایی دارد (هیون، ۲۰۰۹) و ابزار بالقوه‌ای است که برای ارزیابی ریسک و قابلیت اعتماد در کاربردهای مهندسی، هنگام امکان‌ناپذیر بودن اندازه‌گیری دقیق از آزمایش‌ها و به دست آمدن دانش از استنباط متخصصان، استفاده می‌شود. یکی از جنبه‌های مهم این نظریه، ترکیب شواهد به دست آمده از منابع مختلف و مدل‌سازی تعارض بین آنهاست (سنتر و فرسون، ۲۰۰۲).

### پیشینه تجربی پژوهش

در اینجا به برخی از مطالعات تجربی درباره موضوع پژوهش اشاره می‌شود. موسوی، یوسفی زوز و حسن‌پور (۱۳۹۴)، پژوهشی را با عنوان «شناسایی ریسک‌های امنیت اطلاعات سازمانی با استفاده از روش دلفی فازی در صنعت بانکداری» اجرا کردند. هدف این پژوهش، شناسایی مهم‌ترین ریسک‌های امنیت اطلاعات سازمانی بود. آنان برای این منظور با مطالعه اسنادی و به کمک روش دلفی فازی و نظر خبرگان (۱۰ متخصص فناوری اطلاعات بانک)، الگویی براساس استاندارد ایزو و چارچوب کوبیت ۴ ارائه کردند و بر این اساس شش شاخص و ۲۰ زیرشاخص ریسک امنیت اطلاعات سازمانی برای بانک شناسایی شد. منوریان، مانیان، موحدی و اکبری (۱۳۹۳) پژوهشی را با عنوان «بررسی عوامل تأثیرگذار بر توسعه تجارت الکترونیکی (مطالعه موردی بنگاه‌های کوچک و متوسط تهران)» اجرا کردند. این پژوهش در پی پاسخ‌گویی به این مسئله اصلی است که مدل پذیرش تجارت الکترونیکی در بنگاه‌های کوچک و متوسط چگونه است و عوامل مؤثر بر توسعه تجارت الکترونیکی در این بنگاه‌ها چیست؟ در این زمینه، مراحل رشد تجارت الکترونیک در دو سطح پذیرش اولیه و نهادینه کردن در نظر گرفته شده است.

پژوهشی در زمینه ارزیابی امنیت در تجارت الکترونیک با بهره‌مندی از روش AHP<sup>۱</sup> و تئوری شواهد دمپستر- شافر اجرا شد (ژانگ، دنگ، ویی و دنگ، ۲۰۱۲). در این مطالعه روش جدیدی به منظور کمک به تشخیص امنیت در تجارت الکترونیک براساس AHP و تئوری شواهد دمپستر- شافر (DS) مطرح شد و کارایی مدل ارائه شده با مثالی گویا به اثبات رسید.

1. Analytic Hierarchy Process

لیو (۲۰۱۱) در زمینه تعیین امنیت سیستم تجارت الکترونیک براساس ارزیابی جامع روش تجزیه و تحلیل رابطه خاکستری<sup>۱</sup> مطالعه کرد. وی در این مطالعه به بررسی تصمیم‌گیری چندشاخصه (MADM) برای ارزیابی مشکلات امنیتی سیستم‌های تجارت الکترونیک با اطلاعات نامشخص پرداخت و براساس روش تجزیه و تحلیل رابطه خاکستری، مراحل محاسبه حل مشکلات ناشی از تصمیم‌گیری چندشاخصه با وزن‌های کاملاً مشخص از اطلاعات داده شده را نشان داد.

کرافت و کاکار (۲۰۰۹) در پژوهشی با عنوان «امنیت در تجارت الکترونیک» به ارزیابی امنیت تجارت الکترونیک پرداختند. در این مقاله برای اولین بار روندهای اخیر بازار در کسب و کارهای الکترونیکی و اهمیت تجارت الکترونیک در بازارهای خرده‌فروشی بررسی شده است و علاوه بر شیوه‌های فعلی، گرایش‌های تجارت الکترونیک، از جمله حفظ حریم خصوصی و جنبه‌های امنیتی بررسی و مستند شده است.

مرت هاگن، آبرتنس و هودن (۲۰۰۸) پژوهشی در زمینه پیاده‌سازی و اثربخشی اقدامات امنیت اطلاعات سازمانی اجرا کردند. هدف این مطالعه پیاده‌سازی اقدامات امنیت اطلاعات در سازمان‌های نیروی و ارزیابی این اقدامات بود. آنها برای اجرای این پژوهش از سیستم نظرسنجی آنلاین بهره بردند و پرسشنامه‌ها را از طریق ایمیل به ۶۵۸ نفر از مسئولان امنیت اطلاعات در سازمان‌های جامعه هدف (نیرو) ارسال کردند. نتایج این مطالعه نشان داد بین اقدامات امنیت اطلاعات سازمان و ارزیابی اثربخشی اقدامات امنیت سازمان، رابطه‌ای معکوس وجود دارد. در واقع این مطالعه در زمینه اقدامات غیرفنی امنیت بینشی ایجاد کرد.

تیوکالا، پوتاس و ون‌دی هار (۲۰۰۶) به بررسی پروفایل امنیت اطلاعات سازمانی پرداختند. آنان چارچوبی برای تسهیل اداره اطلاعات امنیتی در سازمان ارائه کردند و سپس به اندازه‌گیری سطح بهره‌وری امنیت اطلاعات پرداختند. هدف این مطالعه، معرفی سازوکاری به نام پروفایل امنیت اطلاعات سازمانی<sup>۲</sup> بود.

سنگوپتا و همکارانش (۲۰۰۵) در پژوهشی با عنوان «امنیت تجارت الکترونیک با رویکرد چرخه عمر» به بررسی مسائل امنیت دارایی‌ها و معاملات در مؤلفه‌ها و فعالیت‌های تجارت الکترونیک پرداختند. این مقاله پس از بررسی فناوری استفاده شده در تجارت الکترونیک، به سمت شناسایی نیازهای امنیتی سیستم‌های تجارت الکترونیک در مقابل آسیب‌ها و تهدیدهای درک شده می‌رود.

1. Grey Relational Analysis

2. The Organizational Information Security Profile(OISP)



با توجه به مطالعات پیشین، در این پژوهش محقق تلاش می‌کند ساختاری توسعه‌یافته برای معیارهای امنیتی مطرح در تجارت الکترونیک ارائه دهد. در کنار آن، هدف محقق اندازه‌گیری سطح امنیت تجارت الکترونیک به کمک روش محاسبه مناسبی است که مقاله‌های منتشرشده اندکی در این زمینه وجود دارد. شایان ذکر اینکه ترکیب ساختار و روش‌های ارائه‌شده این پژوهش، در هیچ‌یک از پژوهش‌های پیشین مشاهده نشده و تا کنون در این زمینه هیچ پژوهش داخلی صورت نگرفته است.

### روش‌شناسی پژوهش

پایه هر علم، شناخت آن است و ارزش قوانین هر علمی به روش‌شناسی‌ای مبتنی است که در آن علم به کار می‌رود. از این رو روش پژوهش مجموعه‌ای از قواعد، ابزار و راه‌های معتبر و نظام‌یافته برای بررسی واقعیت‌ها، کشف مجهولات و دستیابی به راه‌حل مشکلات است.

پژوهش حاضر از نظر هدف، کاربردی و از نظر روش پیمایشی-توصیفی است. با توجه به اینکه پژوهش حاضر مبتنی بر تیم تصمیم به‌منظور تهیه داده‌هاست، برای تعیین حجم نمونه مد نظر ابتدا فهرست تمام شرکت‌های بازرگانی ثبت‌شده در اتاق بازرگانی مشهد تهیه شد. از آنجا که مشخص نبود این شرکت‌ها فعالیت تجارت الکترونیک دارند یا خیر، با همه آنها تماس گرفته شد و در نهایت ۹ شرکت اعلام کردند در سطح قابل قبولی فعالیت تجارت الکترونیک دارند که به‌عنوان جامعه پژوهش در نظر گرفته شدند. از این تعداد به‌دلیل نگرانی‌های امنیتی تنها چهار شرکت حاضر به همکاری شدند، در نتیجه داده‌های پژوهش از تیم تصمیم ۱۲ نفره اعضای شرکت‌های بازرگانی شهر مشهد، شامل مدیرعامل، کارشناس بازرگانی و کارشناس فناوری اطلاعات جمع‌آوری شد. برای این منظور از پرسشنامه و مصاحبه استفاده شده است. در مجموع چهار پرسشنامه برای دنبال کردن اهداف زیر تهیه شد:

پرسشنامه ۱؛ به‌منظور تأیید ساختار ارائه‌شده و مصاحبه در زمینه معیارهای ارزیابی سطح امنیت در تجارت الکترونیک تهیه شد و در اختیار پنج تن از استادان فعال حوزه امنیت قرار گرفت.

پرسشنامه‌های ۲ و ۳؛ به‌منظور تعیین وزن معیارهای مطرح‌شده در حوزه امنیت تجارت الکترونیک تدوین شدند. یکی از پرسشنامه‌ها براساس مقیاس نه‌تایی ساعتی تهیه شد که در آن هدف مقایسه دوه‌دوی معیارها و تعیین ارجحیت آنها بود. در پرسشنامه دیگر که به‌صورت باز طراحی شد، تنها از پاسخ‌دهنده درخواست شد وزن هر یک از متغیرهای هم‌گروه را نسبت به یکدیگر تعیین کند.

پرسشنامه ۴: به منظور اجرای مصاحبه تهیه شد و طراحی آن براساس نیاز محاسباتی و ادبیات موضوع بود. هدف در این پرسشنامه تعیین سطح امنیت معیارهای مطرح در حوزه امنیت تجارت الکترونیک بود. بنابراین با توجه به هدف مد نظر، سطح امنیت هر معیار در مقیاس ده امتیازی درجه بندی و تعیین شد.

### روایی ابزار پژوهش

در پژوهش حاضر، پرسشنامه‌ها نوعی اعتبار منطقی و محتوایی دارند که به روش به کاررفته مربوط می‌شود. در روش مقایسه‌های زوجی باید تمام عوامل با هم سنجیده شوند و این عمل تمام احتمالات در نظر گرفته نشدن یک معیار یا سؤال را از بین می‌برد، علاوه بر این در سایر پرسشنامه‌ها نیز تمام معیارها بررسی و ارزیابی شدند. بنابراین، احتمال در نظر گرفته نشدن معیارها در آنها نیز مردود است. همچنین روایی صوری و محتوایی پرسشنامه‌ها براساس نظر استادان و اعضای گروه تصمیم تأیید شده است، از این رو می‌توان گفت که ابزار جمع‌آوری اطلاعات در این پژوهش اعتبار صوری و محتوایی دارد.

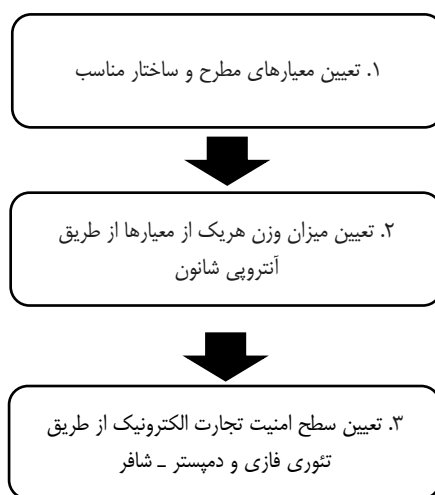
### پایایی ابزار پژوهش

با توجه به نوع پرسشنامه‌های تهیه شده، می‌توان گفت پرسشنامه‌ها تمام معیارها و گزینه‌ها را می‌سنجند. به بیانی دیگر، بیشترین سؤال‌های ممکن با ساختاری مطلوب از مخاطب پرسیده می‌شود. با در نظر گرفتن اینکه تمام معیارها بررسی شدند و طراح قادر به جهت‌گیری خاصی در طراحی پرسشنامه نیست و علاوه بر این به منظور تعیین سطح امنیت معیارها مصاحبه به عمل آمد و با استفاده از روش‌های فازی و دمپستر- شافر سطح کلی امنیت تعیین شد و خروجی‌های به دست آمده از نظر منطقی درست بود؛ پایایی ابزار اندازه‌گیری در این پژوهش از روش‌های کمی بهره نمی‌برد، بلکه اعتبار ارزیابی ارزیابان، ملاکی برای پایایی ابزار اندازه‌گیری محسوب خواهد شد. اما در پرسشنامه مقایسه‌های زوجی که براساس مقیاس ساعتی است، به منظور بررسی پایایی پرسشنامه از درصد سازگاری استفاده می‌شود. از این رو شاخص سازگاری CI برای اندازه‌گیری ناسازگاری در ماتریس مقایسه‌های زوجی (زمانی که از AHP گروهی برای ترکیب ماتریس‌ها استفاده می‌کنیم) به کار می‌رود که به صورت زیر تعیین می‌شود:

$$CI = \frac{(\lambda_{max} - n)}{n} \quad \text{رابطه ۱}$$

ارزیابی سطح امنیت در تجارت الکترونیک با استفاده از آنتروپی ... ۸۷

سپس درصد سازگاری یا CR، از طریق  $CR = \frac{CI}{RI}$  محاسبه می‌شود. اگر نتیجه CR کمتر از ۰/۱ باشد، سازگاری ماتریس M قابل قبول است. شکل ۱ فرایند پژوهش را به نمایش گذاشته است.



شکل ۱. فرایند انجام پژوهش

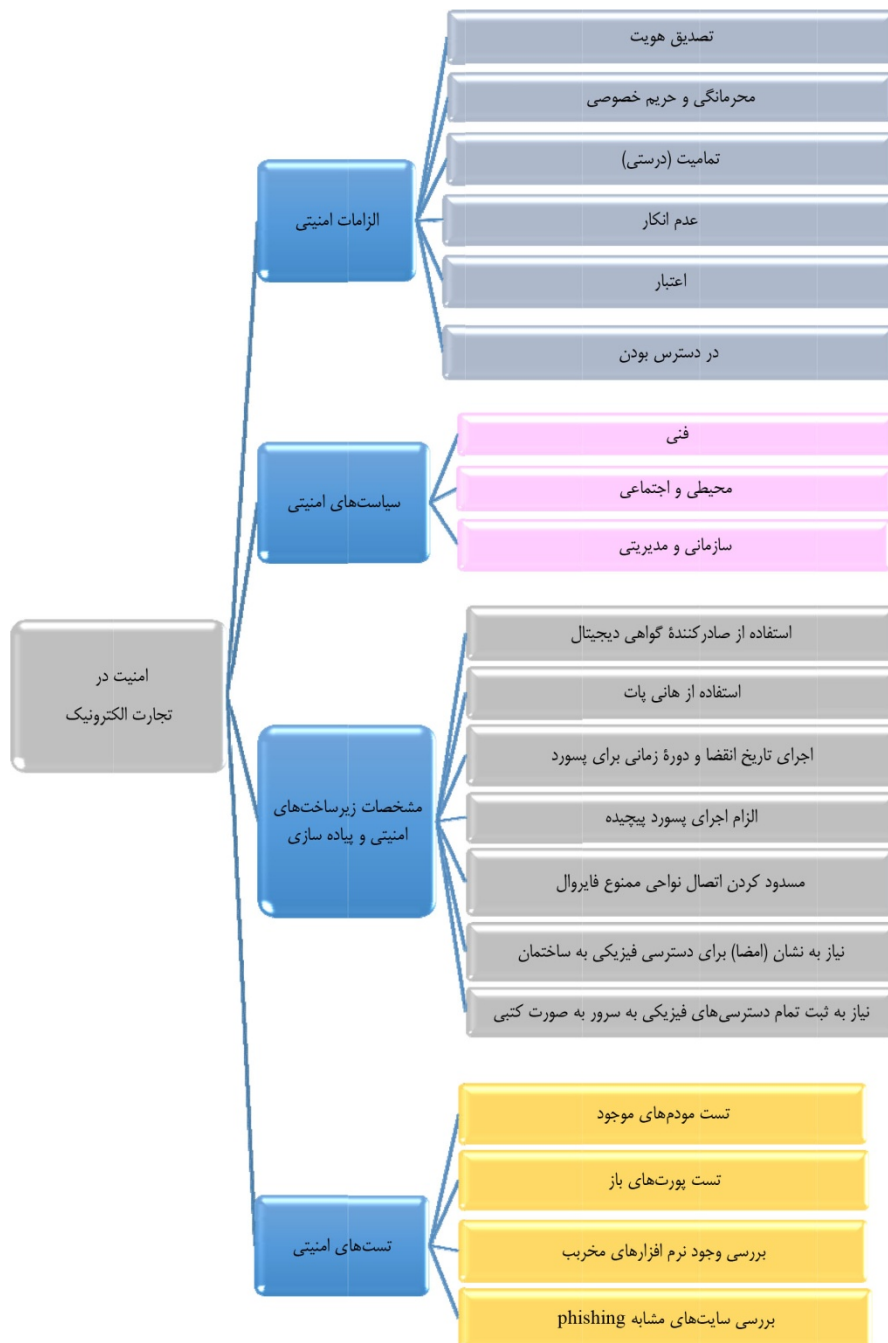
## فرایند پژوهش

### مرحله اول

در این مرحله از پژوهش معیارها و زیرمعیارهای مطرح در زمینه امنیت تجارت الکترونیک از طریق مطالعات کتابخانه‌ای، بررسی ادبیات موضوع و پژوهش‌های صورت‌گرفته در این حوزه شناسایی شدند و در ساختار مناسب به شکل چرخه عمر قرار گرفتند. در مجموع معیارهای الزامات امنیتی، سیاست‌های امنیتی، مشخصات زیرساخت‌های امنیتی و پیاده‌سازی و آزمون‌های امنیتی، عناصر اصلی چرخه عمر را شکل می‌دهند. به همین ترتیب زیرمعیارهای هر یک از معیارهای اصلی در زمینه امنیت تجارت الکترونیک تعیین شدند. سپس مؤلفه‌ها و زیرمؤلفه‌های به‌دست‌آمده، به تأیید خبرگان امنیتی رسید.

### ساختار مفهومی

شکل ۲ ساختار ارائه‌شده در زمینه امنیت تجارت الکترونیک را نشان می‌دهد.



شکل ۲. ساختار مؤلفه‌های امنیت در تجارت الکترونیک

## مرحله دوم

در این مرحله، هدف تعیین اهمیت معیارها از طریق روش آنتروپی شانون است. بنابراین به منظور دست‌یافتن به آن، ابتدا پرسشنامه‌ای در اختیار چند تن از خبرگان امنیت قرار گرفت و ماتریس‌های مختص به هر یک تشکیل شد. با توجه به شکل‌گیری چند ماتریس، برای به دست آوردن ماتریس نهایی باید از میانگین هندسی برای عناصر ماتریس  $\left\| a_{ij} = \frac{w_i}{w_j} \right\|$  استفاده کرد. به منظور محاسبه وزن متغیرها به صورت زیر عمل می‌کنیم.

$$a'_{ij} = \left( \prod_{l=1}^k a_{ijl} \right)^{\frac{1}{k}} \quad \text{رابطه ۲}$$

پس از به دست آوردن ماتریس‌های ادغام‌شده از طریق رابطه ۲، درصد سازگاری محاسبه می‌شود، نتایج این عملیات ورودی آنتروپی شانون است. در پایان وزن نهایی هر متغیر به کمک آنتروپی شانون تعیین می‌شود. شایان ذکر است که مراحل و خروجی‌های این پژوهش مجزا از یکدیگرند و هر یک بخشی از نیاز پژوهش را پوشش می‌دهد. بنابراین هر یک از روش‌های آنتروپی و فازی مطرح‌شده در این پژوهش خروجی‌های متفاوتی دارند. در این راستا، برای تعیین وزن متغیرها باید مراحل زیر طی شود.

ماتریس تصمیم‌گیری، حاوی اطلاعاتی است که در آنتروپی به عنوان معیار ارزیابی به کار می‌رود. فرض کنید که ماتریس تصمیم‌گیری به دست آمده از مقایسه‌های زوجی و ترکیب‌شده از طریق روش میانگین هندسی، به صورت جدول ۱ باشد.

جدول ۱. نظر تصمیم‌گیرندگان درباره شاخص‌ها

$C_n$	$C_r$	$C_1$	شاخص
$a_{1n}$	...	$a_{1r}$	$C_1$
$a_{rn}$	...	$a_{rr}$	$C_r$
$a_{mn}$	...	$a_{mr}$	$C_n$
$W_n$	...	$W_r$	$W_j$

با استفاده از این ماتریس،  $P_{ij}$  به صورت رابطه ۳ محاسبه می‌شود.

$$P_{ij} = \frac{a_{ij}}{\sum_{i=1}^m a_{ij}} ; \forall i, j \quad \text{رابطه ۳}$$

آنتروپی شاخص  $\lambda_m$  (Ej) از رابطه ۴ به دست می‌آید.

$$E_j = -k \sum_{i=1}^m [P_{ij} \ln P_{ij}] ; \forall j \quad \text{رابطه ۴}$$

عدم اطمینان یا درجه انحراف ( $d_j$ ) از اطلاعات به دست آمده برای شاخص  $j$ ، بیان می کند که شاخص مختص به ( $j$ )، چقدر اطلاعات مفید برای تصمیم گیری در اختیار تصمیم گیرنده قرار می دهد. مقدار ( $d_j$ ) از رابطه ۵ به دست می آید.

$$d_j = 1 - E_j ; \forall j \quad \text{رابطه ۵}$$

سپس مقدار وزن  $w_j$  از رابطه ۶ به دست می آید.

$$W_j = \frac{d_j}{\sum_{j=1}^n d_j} ; \forall j \quad \text{رابطه ۶}$$

اگر تصمیم گیرنده از قبل، وزن دهی مشخصی مثل  $\lambda_j$  را برای شاخص  $j$  در نظر گرفته باشد، در این صورت وزن تعدیل شده ( $w'_j$ )، به شرح رابطه ۷ محاسبه می شود.

$$W'_j = \frac{\lambda_j W_j}{\sum_{j=1}^n \lambda_j W_j} ; \forall j \quad \text{رابطه ۷}$$

### رابطه ۶) مرحله سوم

در این مرحله باید سطح امنیت معیارهای مطرح در تجارت الکترونیک ارزیابی شود که برای این منظور پرسشنامه چهارم در اختیار پاسخ دهندگان قرار گرفت. با جمع آوری داده های مد نظر، مرحله بعد که شامل تجزیه و تحلیل داده ها و نتیجه گیری نهایی است، آغاز می شود. شایان ذکر اینکه روش به کاررفته در این مرحله، برگرفته از روش پیشنهادی ژانگ و همکارانش (۲۰۱۲) است. در این مرحله به منظور تعیین سطح امنیت، داده های جمع آوری شده از پرسشنامه چهارم وارد توابع فازی می شوند تا برای تنزیل آماده شوند. باید در نظر داشت که یکی از انگیزه های اصلی در معرفی مجموعه های فازی، بیان مفاهیم غیر صریح و مبهم است و به دلیل اینکه عضویت یک فرد یا عنصر در یک مجموعه فازی ممکن است همراه با عدم اطمینان باشد، عضویت عناصر در آنها براساس درجه است. هر زیرمجموعه فازی  $A$ ، در مجموعه مرجع  $X$  را می توان به وسیله تابع مشخصه، تعریف کرد. این تابع که تابع عضویت نامیده می شود، برای هر عضو  $x$  از مجموعه مرجع  $X$ ، عددی در بازه  $[0, 1]$  قرار می دهد که مبین درجه عضویت  $x$  در مجموعه فازی  $A$ ، است؛ بنابراین به صورت  $A: X \rightarrow [0, 1]$  تعریف می شود. نمونه ای از یک مجموعه فازی  $A$  که در جامعه  $X$  تعریف شده به صورت زیر است:

$$A = \{(x, \mu_A(x)) | x \in X\}$$

که در آن  $\mu_A: X \rightarrow [0, 1]$  تابع عضویت  $A$  است. ارزش عضویت  $\mu_A(x)$  توصیف کننده درجه تعلق  $x \in X$  در  $A$  است. برای مجموعه متناهی  $A = \{x_1, \dots, x_i, \dots, x_n\}$  مجموعه فازی  $(A, m)$  معمولاً به صورت  $A = \left\{ \frac{\mu_A(x_1)}{x_1}, \dots, \frac{\mu_A(x_i)}{x_i}, \dots, \frac{\mu_A(x_n)}{x_n} \right\}$  نشان داده می شود. در پژوهش حاضر اگر  $X$  جامعه مد نظر باشد، پنج متغیر زبانی توصیف کننده درجه امنیت را دربرمی گیرد و به صورت زیر بیان می شود:

$$X = \{(VL) \text{ کم خیلی}, (L) \text{ کم}, (M) \text{ متوسط}, (H) \text{ زیاد}, (VH) \text{ زیاد خیلی}\}$$

در صورتی که فرض شود تنها دو متغیر مجاور با هم همپوشانی دارند، توابع فازی به صورت زیر تعریف می شوند:

$$f_{very\ low}(x) = -0.4x + 1, \quad 0 \leq x \leq 2.5 \quad (\text{رابطه ۸})$$

$$f_{low}(x) = -0.4x, \quad 0 \leq x \leq 2.5$$

$$f_{low}(x) = -0.4x + 2, \quad 2.5 \leq x \leq 5$$

$$f_{medium}(x) = 0.4x - 1, \quad 2.5 \leq x \leq 5$$

$$f_{medium}(x) = -0.4x + 3, \quad 5 \leq x \leq 7.5$$

$$f_{high}(x) = 0.4x - 2, \quad 5 \leq x \leq 7.5$$

$$f_{high}(x) = -0.4x + 4, \quad 7.5 \leq x \leq 10$$

$$f_{very\ high}(x) = 0.4x - 3, \quad 7.5 \leq x \leq 10$$

که در آن  $f_{VL}$ ،  $f_L$ ،  $f_M$ ،  $f_H$ ،  $f_{VH}$  و  $f_{VL}$  توابع عضویت در مجموعه های فازی هستند. پس از اینکه سطح هر داده تعیین شد، مرحله ترکیب توابع هم سطح فرا می رسد که برای این منظور ابتدا باید توابع را تنزیل داد تا ضریب اطمینان به مقدار داده شده افزایش یابد. در واقع عملیات تنزیل زمانی استفاده می شود که یک منبع اطلاعات یک BPAm<sup>۱</sup> را فراهم می آورد که این منبع به اندازه  $\alpha$  قابلیت اطمینان دارد. در نتیجه  $(1-\alpha)$  به عنوان درصد تنزیل<sup>۲</sup> در نظر گرفته می شود و BPAm<sup>۳</sup> جدید به صورت زیر تعریف می شود:

1. Basic Probability Assignment  
2. Discounting Rate

$$m'(A) = \alpha m(A), \quad \forall A \subset \theta, \quad A \neq \theta \quad \text{رابطه ۹}$$

$$m'(\theta) = 1 - \alpha + \alpha m(\theta)$$

تمام توابع جرم باید به وسیله  $\alpha$  که ضریب تنزیل خوانده می شود، تنزیل داده شوند. جایی که  $m$  تابع جرم برای یک شاهد است،  $m^\alpha$  نشان دهنده تابع تخصیص احتمال اولیه تنزیل یافته است و ضریب تنزیل  $(0 \leq \alpha \leq 1)$ ، تعیین کننده میزان قابلیت اطمینان شواهد است. شایان ذکر است که قبل از ترکیب نهایی باید مقدار همپوشانی معیارها نیز محاسبه شود که برای این منظور از رابطه ۱۰ استفاده می شود.

$$m'(A) = \alpha m(A), \quad \forall A \in \theta, \quad A \neq \theta \quad \text{رابطه ۱۰}$$

$$m'(\{Y, A\}) = \frac{S(Y \cap A)}{S(X \cap A)} \times (1 - \alpha m(A)), \quad Y \neq A, \quad Y \in X, \quad X \subset \theta$$

سپس وارد مرحله ترکیب می شویم. تئوری دمپستر- شافر در زمینه ایجاد تعارض هنگام ترکیب اصلاح می شود و با توجه به اینکه در پژوهش حاضر نیز تعارض هایی وجود دارد، روش متوسط گیری مورفی به منظور غلبه بر تعارض ها به کار می رود. به پیشنهاد مورفی چنانچه تمام شواهد هم زمان در دسترس باشند، می توان متوسط جرم را محاسبه کرد و جرم های نهایی را از طریق ترکیب ارزش های متوسط گیری شده در چندین مرتبه به دست آورد. وی بیان کرد که برای ترکیب، وزن های متوسط گیری شده را  $n - 1$  بار با یکدیگر ترکیب می کنیم. در نتیجه به کمک این روش می توان از وابستگی بیش از حد به یک بخش از شواهد متعارض جلوگیری کرد. این قاعده می تواند دو تابع تخصیص احتمال اولیه  $m_1$  و  $m_2$  را برای بازه جدید تابع تخصیص احتمال اولیه، ترکیب کند.

شایان ذکر است که قاعده ترکیب دمپستر، توابع باور چندگانه را از طریق  $BPA(m)$  ترکیب می کند. این توابع باور بر اساس چارچوب یکسان تشخیص تعریف می شوند، اما مبتنی بر استقلال استدلال ها یا بدنه شواهدند. قاعده ترکیب دمپستر- شافر به صورت  $m = m_1 \oplus m_2$ ، نشان داده می شود و به طور خاص ترکیب از طریق دو  $m_1$  و  $m_2$ ، به صورت زیر به دست می آید:

$$A \neq \emptyset \text{ و } m_{12}(\emptyset) = 0 \quad \text{رابطه ۱۱}$$

$$m_{12}(A) = \frac{\sum_{B \cap C = A} m_1(B) m_2(C)}{1 - K}$$

$$k = \sum_{B \cap C = \emptyset} m_1(B) m_2(C)$$



### یافته‌های پژوهش

در این بخش به دلیل حجم زیاد نتایج هر چهار شرکت بازرگانی، برای نمونه تنها نتایج یکی از شرکت‌ها آورده شده است

### محاسبه وزن معیارها

با توجه به ماتریس تصمیم جدول ۱، به طور خلاصه می‌توان برای به دست آوردن وزن شاخص‌ها، گام‌های زیر را طی کرد.

گام اول؛ محاسبه  $P_{ij}$ : پس از محاسبه  $P_{ij}$  و به دست آوردن مقادیر آن، سایر مراحل را به صورت زیر طی می‌کنیم.

گام دوم؛ محاسبه مقدار آنتروپی ( $E_j$ ): با توجه به مقادیر به دست آمده از محاسبه  $P_{ij}$  و رابطه ۴، مقدار آنتروپی به دست می‌آید. مقادیر آنتروپی هر شاخص در جدول ۲ آورده شده است.

بخش اول جدول ۲. مقادیر به دست آمده (گام ۲ تا ۵)

ردیف	معیارها	مقدار آنتروپی ( $E_j$ )	مقدار عدم اطمینان ( $d_j$ )	وزن معیار ( $W_j$ )	وزن‌های ذهنی	وزن تعدیل شده
۱	B <sub>1</sub>	۰/۹۶۶	۰/۰۳۴	۰/۲۴۵	۰/۲۳۳۳	۰/۳۱۳
۲	B <sub>2</sub>	۰/۹۶۳	۰/۰۳۷	۰/۲۶۳	۰/۲۳۳۳	۰/۳۳۶
۳	B <sub>3</sub>	۰/۹۸۵	۰/۰۱۵	۰/۱۰۶	۰/۲۳۳۳	۰/۱۳۵
۴	B <sub>4</sub>	۰/۹۸۲	۰/۰۱۸	۰/۱۳	۰/۱۸۳۴	۰/۱۳
۵	B <sub>5</sub>	۰/۹۷۷	۰/۰۲۳	۰/۱۶۶	۰/۰۶۶۷	۰/۰۶۱
۶	B <sub>6</sub>	۰/۹۸۷	۰/۰۱۳	۰/۰۹۱	۰/۰۵	۰/۰۲۵

بخش دوم جدول ۲. مقادیر به دست آمده (گام ۲ تا ۵)

ردیف	معیارها	مقدار آنتروپی ( $E_j$ )	مقدار عدم اطمینان ( $d_j$ )	وزن معیار ( $W_j$ )	وزن‌های ذهنی	وزن تعدیل شده
۷	B <sub>7</sub>	۰/۸۵۶	۰/۱۴۴	۰/۲۹۳	۰/۴	۰/۳۵۵
۸	B <sub>8</sub>	۰/۷۳۵	۰/۲۶۵	۰/۵۴	۰/۳	۰/۴۹۲
۹	B <sub>9</sub>	۰/۹۱۸	۰/۰۸۲	۰/۱۶۷	۰/۳	۰/۱۵۲

بخش سوم جدول ۲. مقادیر به دست آمده (گام ۲ تا ۵)

ردیف	معیارها	مقدار آنتروپی ( $E_j$ )	مقدار عدم اطمینان ( $d_j$ )	وزن معیار ( $W_j$ )	وزن‌های ذهنی	وزن تعدیل شده
۱	B۱۰	۰/۹۹۶	۰/۰۰۴	۰/۰۲۴	۰/۱۶۶۷	۰/۰۲۷
۲	B۱۱	۰/۹۶۵	۰/۰۳۵	۰/۱۸۴	۰/۱۳۳۳	۰/۱۷
۳	B۱۲	۰/۹۷۵	۰/۰۲۵	۰/۱۳	۰/۱۵	۰/۱۳۶
۴	B۱۳	۰/۹۹۲	۰/۰۰۸	۰/۰۴۳	۰/۱۵	۰/۰۴۵
۵	B۱۴	۰/۹۴۵	۰/۰۵۵	۰/۲۹۳	۰/۱۸۳۳	۰/۳۷۲
۶	B۱۵	۰/۹۶۳	۰/۰۳۷	۰/۱۹۷	۰/۱۱۶۷	۰/۱۵۹
۷	B۱۶	۰/۹۷۶	۰/۰۲۴	۰/۱۲۹	۰/۱	۰/۰۹

بخش چهارم جدول ۲. مقادیر به دست آمده (گام ۲ تا ۵)

ردیف	معیارها	مقدار آنتروپی ( $E_j$ )	مقدار عدم اطمینان ( $d_j$ )	وزن معیار ( $W_j$ )	وزن‌های ذهنی	وزن تعدیل شده
۸	B۱۷	۰/۹۵۷	۰/۰۴۳	۰/۲۳۷	۰/۲۶۶۶	۰/۲۵
۹	B۱۸	۰/۹۴۱	۰/۰۵۹	۰/۳۲۶	۰/۳۱۶۷	۰/۴۰۸
۱۰	B۱۹	۰/۹۷	۰/۰۳	۰/۱۶۳	۰/۲۵	۰/۱۶۱
۱۱	B۲۰	۰/۹۵	۰/۰۵	۰/۲۷۴	۰/۱۶۶۷	۰/۱۸۱

گام سوم؛ محاسبه مقدار عدم اطمینان ( $d_j$ ): مقادیر عدم اطمینان با توجه به مقادیر آنتروپی و رابطه ۵ به دست می‌آید. این مقادیر در جدول ۲ آورده شده است.

گام چهارم؛ محاسبه اوزان ( $W_j$ ): وزن هر شاخص با توجه به مقادیر عدم اطمینان و طبق رابطه ۶ به دست می‌آید. وزن هر شاخص ( $W_j$ ) در جدول ۲ نشان داده شده است.

گام پنجم؛ محاسبه وزن‌های تعدیل شده ( $W'_j$ ): وزن‌های تعدیل شده با توجه به مقادیر ( $W_j$ ) و وزن‌های ذهنی ( $\lambda_j$ ) براساس رابطه ۷ به دست می‌آید.

### تعیین سطح امنیت معیارها

در این مرحله پس از تعیین وزن معیارها، گروه دوم داده‌ها در زمینه سطح امنیت هر یک از معیارها با استفاده از گروه تصمیم شرکت‌های بازرگانی‌ای که حاضر به همکاری در این زمینه بودند، جمع‌آوری شد و وارد رابطه‌های ۸ شدند. جدول ۳ برای نمونه سطح امنیت هر معیار برای یکی از شرکت‌های بازرگانی مطالعه شده را نشان می‌دهد.

جدول ۳. سطح امنیت هر معیار

ردیف	نام متغیر	سطح امنیت معیارهای شرکت
B۱	تصدیق هویت	متوسط
B۲	حریم خصوصی	خیلی زیاد
B۳	تمامیت (درستی)	زیاد
B۴	عدم انکار	متوسط
B۵	اعتبار	متوسط
B۶	در دسترس بودن	خیلی زیاد
B۷	عوامل فنی	زیاد
B۸	عوامل محیطی و اجتماعی	زیاد
B۹	سازمانی و مدیریتی	زیاد
B۱۰	استفاده از صادرکننده گواهی دیجیتالی	خیلی کم
B۱۱	استفاده از هانی پات	خیلی کم
B۱۲	اجرای تاریخ انقضا و دوره زمانی برای پسورد	کم
B۱۳	الزام اجرای پسورد پیچیده	خیلی کم
B۱۴	مسدودکردن اتصال نواحی ممنوع فایروال	زیاد
B۱۵	نیاز به نشان یا امضا برای دسترسی فیزیکی به ساختمان	خیلی کم
B۱۶	نیاز به ثبت تمام دسترسی‌های فیزیکی به سرور به صورت کتبی	خیلی کم
B۱۷	آزمایش مودم‌های موجود	زیاد
B۱۸	بررسی وجود نرم‌افزارهای مخرب	متوسط
B۱۹	آزمون پورت‌های باز	کم
B۲۰	بررسی سایت‌های مشابه	خیلی کم

### تعیین سطح کلی امنیت

در این مرحله بعد از تعیین سطح امنیت هر معیار، وارد مرحله ترکیب معیارهای هم‌گروه می‌شویم. برای این منظور چارچوب تشخیص را با پنج فرضیه زیر در نظر می‌گیریم:

$$\theta = \{ \text{خیلی زیاد (VH)}, \text{زیاد (H)}, \text{متوسط (M)}, \text{کم (L)}, \text{خیلی کم (VL)} \}$$

هر یک از فرضیه‌ها توصیف‌کننده سطح امنیت در تجارت الکترونیک‌اند و به‌عنوان شواهد در تئوری دمپستر- شافر استفاده می‌شوند. با وجود این باید در نظر داشت که این شواهد برای

ترکیب با یکدیگر مقدماتی و مبهم‌اند، در نتیجه قبل از ترکیب باید آنها را تنزیل داد. برای تنزیل دادن شواهد از رابطه ۹ استفاده می‌شود و میزان همپوشانی بین متغیرها را از رابطه ۱۰ به دست می‌آید و در نهایت نوبت به مرحله ترکیب می‌رسد. بعد از ترکیب شواهد، ممکن است اطمینان ۱۰۰ درصد به عنصری قانونی خاص تخصیص یابد؛ بنابراین در صورت مواجه شدن با این گونه تعارض‌ها چندین راه معرفی شده است که در پژوهش حاضر از ایده پیشنهادی مورفی استفاده شده است. نتایج این محاسبات در جدول ۴ آورده شده است.

جدول ۴. سطح کلی امنیت در تجارت الکترونیک در شرکت بازرگانی

H,VH	M,H	L,M	VL,L	VH	H	M	L	VL	ترکیب شواهد در شرکت
۰/۰۱۶	۰/۰۰۴	.	.	۰/۰۲۵	۰/۶۴	۰/۳۱۵	.	.	B <sub>۱</sub> , B <sub>۲</sub> , B <sub>۳</sub> , B <sub>۴</sub> , B <sub>۵</sub> , B <sub>۶</sub>
۰/۱۱	.	.	.	۰/۱۱	۰/۷۸	.	.	.	V <sub>۱</sub> , V <sub>۲</sub> , ..., V <sub>۱۴</sub>
۰/۰۲	۰/۰۱	.	.	۰/۰۱	۰/۷۱	۰/۲۵	.	.	V <sub>۱۵</sub> , V <sub>۱۶</sub> , ... V <sub>۲۰</sub>
۰/۰۱	.	.	.	۰/۰۱	۰/۹۸	.	.	.	V <sub>۲۱</sub> , V <sub>۲۲</sub> , ..., V <sub>۳۵</sub>
.	.	.	۰/۳۳	.	.	.	۰/۳۷	۰/۳	B <sub>۱۰</sub> , B <sub>۱۱</sub> , ..., B <sub>۱۶</sub>
.	۰/۰۰۷	۰/۰۰۸	۰/۰۷	.	۰/۰۷۲	۰/۳۰۶	۰/۴۸۷	۰/۰۵	B <sub>۱۷</sub> , ..., B <sub>۲۰</sub>
۰/۰۲۶	۰/۰۰۴	۰/۰۰۱	۰/۰۶۷	۰/۰۲۶	۰/۵۳	۰/۱۴۵	۰/۱۴۳	۰/۰۵۸	میانگین

### نتیجه‌گیری و پیشنهادها

درباره تعیین ساختار مناسب می‌توان به الزام قرار گرفتن کلیه عوامل روی چرخه عمر اشاره کرد که این موضوع از دو عامل بی‌ثباتی محیط تجارت الکترونیک و مطرح شدن تهدیدهای روزانه ناشی می‌شود. در این چرخه، پس از تعیین انواع الزامات امنیتی، اقدام بعدی تدوین سیاست‌های امنیتی است، این سیاست‌ها با توجه به سه شاخه اصلی مباحث فنی، محیطی / اجتماعی و مدیریتی / سازمانی تعیین می‌شوند. در مرحله بعد به زیرساخت‌های امنیتی و پیاده‌سازی سیاست‌های امنیتی اختصاص دارد و در نهایت آنچه برای آزمون‌های امنیتی لازم است، تعیین می‌شود.

در مرحله تعیین وزن‌ها، نتایج نشان داد در زیرگروه الزامات امنیتی، معیار محرمانگی، حریم خصوصی و تصدیق هویت بیشترین اهمیت را نسبت به سایر معیارهای دارند. در این میان کمترین اهمیت به معیار در دسترس بودن اختصاص یافت. البته در بررسی دیدگاه شخصی متخصصان می‌توان گفت که معیارهای تصدیق هویت، محرمانگی و حریم خصوصی و درستی، بیشترین اهمیت را نسبت به سایر معیارها کسب کرده‌اند. در گروه معیارهای سیاست‌های امنیتی، عوامل محیطی و فنی بیشترین اهمیت را به دست آوردند و براساس وزن‌دهی ذهنی متخصصان، عوامل فنی بیشترین اهمیت را بین سایر معیارها کسب کرد.

در بین معیارهای زیرمجموعه مشخصات زیرساخت‌های امنیتی و پیاده‌سازی، معیارهای مسدودکردن اتصال نواحی ممنوع فایروال و استفاده از هانی‌پات اهمیت بیشتری دارند و معیار استفاده از صادرکننده گواهی دیجیتال، کمترین اهمیت را نسبت به سایر موارد این گروه کسب کرد. از سوی دیگر در وزن‌دهی ذهنی متخصصان، محدودکردن اتصال نواحی ممنوع فایروال و استفاده از صادرکننده گواهی دیجیتال از عوامل دیگر با اهمیت‌تر بود. در بین زیرمعیارهای آزمون‌های امنیتی دو معیار، بررسی وجود نرم‌افزارهای مخرب و آزمون مودم‌های موجود، بیشترین میزان اهمیت را به دست آوردند و آزمون پورت‌های باز در این گروه کمترین میزان اهمیت را کسب کرد.

در پایان شایان ذکر است که سطح کلی امنیت هر چهار شرکت بالا و متوسط ارزیابی شده است. البته باید در نظر داشت که این شرکت‌ها در بحث الزامات و تعیین آنها به خوبی عمل می‌کنند، اما در زمینه مباحث زیرساخت‌ها و آزمون‌های امنیتی ضعف دارند و نیازمند بازنگری‌اند.

### پیشنهادها

به شرکت‌های بازرگانی فعال در عرصه تجارت الکترونیک، پیشنهاد می‌شود واحدی به نام واحد پشتیبانی فرایندهای الکترونیک یا واحد توسعه الکترونیک، ایجاد کنند؛ این واحد باید تمام امور تجارت الکترونیک، از جمله مباحث پژوهش و توسعه، ایجاد چرخه عمر امنیت، پیاده‌سازی زیرساخت‌ها و موارد دیگر را برعهده داشته باشد.

به سیاست‌گذاران دولتی پیشنهاد می‌شود که الزامات و زیرساخت‌های امنیتی مناسب برای پیاده‌سازی گسترده تجارت سیار را در ایران بررسی کنند. با توجه به اینکه پس از تجارت الکترونیک، یکی از شیوه‌های نوین، تجارت سیار است و قاعدتاً در صورتی که به شیوه‌ای اصولی پیاده‌سازی شود، فواید زیادی برای کشور خواهد داشت؛ توجه به این حوزه برای پژوهش‌های آتی بسیار مفید خواهد بود.

به شرکتهای بازرگانی پیشنهاد می‌شود که تجارت الکترونیک به صورت شبکه اکسترانت را با شرکای ثابت خود پیاده‌سازی کنند و زیرساخت‌های امنیتی مناسب آن را ایجاد کنند تا از این طریق هزینه‌های خود را کاهش دهند و فرایند تجاری خود را آسان کنند.

### References

- Aljifri, H. A., Pons, A. & Collins, D. (2003). Global e-commerce: a framework for understanding and overcoming the trust barrier. *Information Management & Computer Security*, 11(3): 130-138.
- Ghasemi Shabankar, K., Mokhtari, V. & Amini Lari, M. (2008). *Security & E-Commerce*. Paper Presented at The 4th National Scientific Exhibition of E-Commerce. (in Persian)
- Goel, S. & Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems*, 19(4): 281-295.
- Goseva-Popstojanova, K., Anastasovski, G., Dimitrijevikj, A., Pantev, R. & Miller, B. (2014). Characterization and classification of malicious Web traffic. *Computers & Security*, 42: 92-115.
- Huynh, V. N. (2009). Discounting and combination scheme in evidence theory for dealing with conflict in information fusion. In *Modeling Decisions for Artificial Intelligence* (pp. 217-230): Springer Berlin Heidelberg.
- Jafari, M. (2007). *Cyber Space Security Foundations* (First Ed.). Tehran: Oloum Paye press. (in Persian)
- Jarupunphol, P. & Buathong, W. The Future of E-Commerce Security.
- Keersebilck, P. & Vanhoucke, W. (2006). Smart Card (In-) Security. *8th International Conference on Development and Application Systems*.
- Khodadad Hosseini, H. & Fathi, S. (2003). Providing a method for prioritizing Iranian industries based on international reconstruction capability & e-commerce. *Journal of Business Research*, 25: 147-168. (in Persian)
- Knapp, K. J., Morris R. F., Marshall, T. E. & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, 28(7): 493-508.
- Kraft, T. A. & Kakar, R. (2009). E-commerce security. In *Proceedings of the Conference on Information Systems Applied Research*, Washington DC, USA.

- Liu, D. (2011). E-commerce system security assessment based on grey relational analysis comprehensive evaluation. *International Journal of Digital Content Technology and its Applications*, 5(10): 279-284.
- Mahboub Eshratabadi, H., Mirkamali, M., Esmail Manap, SH. & Mehri, D. (2014). Study of The Barriers of Development of Information And Communication Technologies (ICTs) In Comprehensive Universities and their Solutions: The Case of University of Tehran. *Journal of Information Technology Management*, 5(4): 139-160. (in Persian)
- Merete Hagen, J., Albrechtsen, E. & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4): 377-397.
- Monavarian, A., Manian, A., Movahedi, M. & Akbari, M. (2014). Evaluation of influential factors on development of e-commerce: case of Tehran SMEs. *Journal of Information technology management*, 6(1): 145-160. (in Persian)
- Mousavi, P., Yousefizenouz, R. & Hassanpoor, A. (2015). Identifying organizational information security risks using fuzzy Delphi. *Journal of information technology management*, 7(1): 163-184. (in Persian)
- Rial, A. (2013). *Privacy-preserving e-commerce protocols*. Doctoral dissertation, Doctoral Dissertation, KU Leuven University, Belgium. Retrieved from: <https://www.cosic.esat.kuleuven.be/publications/thesis-220.pdf>.
- Sabaghkermani, M. & Esfidani, M. (2006). A Survey on the Impact of Competitive Factors on the Globalization & E-Commerce.
- Sanayei, A. (2005). *The E-Commerce in Third Millennium* (Second Ed.). Isfahan: Jahad Daneshgahi. (in Persian)
- Sengupta, A., Mazumdar, C. & Barik, M.S. (2005). E-Commerce security-A life cycle approach. *Sadhana*, 30(2-3): 119-140.
- Sentz, K. & Ferson, S. (2002). *Combination of evidence in Dempster-Shafer theory* (Vol. 4015). Albuquerque, NM: Sandia National Laboratories.
- Shahibi, M. S. & Fakeh, S. K. W. (2011). Security Factor and Trust in E-Commerce Transactions. *Australian Journal of Basic and Applied Sciences*, 5(12): 2028-2033.
- Tajfar, A.H., Mahmoudi Maymand, M., Rezasoltani, F. & Rezasoltani, P. (2015). Ranking the barriers of implementing information security management system and investigation of readiness rate of exploration management. *Journal of information technology management*, 6(4): 551-566. (in Persian)

- Tyukala, M., Pottas, D., Van De Haar, H. & Von Solms, R. (2006). The Organizational Information Security Profile-A Tool to Assist the Board. Retrieved from: [http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/79\\_Paper.pdf](http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/79_Paper.pdf).
- Zhang, Y., Deng, X., Wei, D. & Deng, Y. (2012). Assessment of E-Commerce security using AHP and evidential reasoning. *Expert Systems with Applications*, 39(3): 3611-3623.
- Zuccato, A. (2004). Holistic Security Requirement Engineering for Electronic Commerce. *Computers & Security*, 23(1): 63-76.
- Zuccato, A. (2007). Holistic security management framework applied in electronic commerce. *Computers & Security*, 26(3): 256-265.