فصلنامه علمی-پژوهشی مطالعات مدیریت کسب و کار هوشمند- سال هفتم ـ شماره ۲۵ـ پاییز ۱۳۹۷
صفحات ۱۸۲-۱۴۷

مروری سیستماتیک بر رویکردهای سرمایه‌گذاری در امنیت اطلاعات

محمد لگزیان*
پریسا موسوی**

چکیده

امنیت اطلاعات جنبه بسیار مهم سیستم‌های اطلاعاتی است. در زمینه فنّاورانه امنیت اطلاعات پژوهش‌های بسیاری انجام شده است، اما با گسترش نیازهای امنیتی، توجه به نقش مدیریت در امنیت اطلاعات نیز اهمیت قابل‌توجهی پیدا کرده است. سرمایه‌گذاری در امنیت اطلاعات سازمان‌ها یکی از مباحث مدیریتی این حوزه است. ازاین‌رو در این پژوهش برای بررسی موضوع ارزیابی سرمایه‌گذاری در امنیت اطلاعات و یافتن روش‌های مناسب برای آن، مروری سیستماتیک بر رویکردهای استفاده‌شده در این حوزه انجام شده است. از اهداف دیگر این پژوهش مطالعه روند تحول در رویکردهای مورداستفاده در سال‌های ۲۰۰۶تا ۲۰۱۷ است. به‌منظور انجام این مرور سیستماتیک کلیه مطالعات انجام‌گرفته در زمینه سرمایه‌گذاری در امنیت اطلاعات با استفاده از کلیدواژه‌های مرتبط، از پایگاه داده‌های اشپرینگر ،آی ای ای اکسپلوره ، وب آو ساینس، ساینس دایرکت استخراج شده، درنهایت تعداد۱۴۶ مقاله مرتبط به این موضوع موردبررسی قرار گرفته است. نتایج پژوهش هشت رویکرد عمده (تئوری بازی‌ها، رویکرد مبتنی بر ریسک، سیستم‌های پشتیبان تصمیم، حداکثر سازی مطلوبیت، نرخ بازده سرمایه‌گذاری، تکنیک ارزش خالص فعلی، نظریهٔ مطلوبیت مورد انتظار، نظریه گزینه‌های واقعی)را در این رابطه شناسایی کرده است. با توجه به نتایج این پژوهش در سال‌های اخیر اقبال بیشتری به‌سوی استفاده از تئوری بازی‌ها بوده است.

واژگان کلیدی: سرمایه‌گذاری امنیت اطلاعات،اقتصادسنجی امنیت اطلاعات، بازگشت سرمایه‌گذاری‌های امنیت اطلاعات، مرور سیستماتیک.

---

* عضو هیئت علمی، گروه مدیریت، دانشکده علوم اداری و اقتصادی ، دانشگاه فردوسی، مشهد.
** دانشجو دکترای مدیریت فناوری اطلاعات، گروه مدیریت، دانشکده علوم اداری و اقتصادی، دانشگاه فردوسی مشهد (نویسنده مسئول)؛p.mousavi@mail.um.ac.ir

تاریخ دریافت:۱۳۹۷/۰۵/۰۵ **تاریخ پذیرش:۱۳۹۷/۰۸/۲۸**

مقدمه

از زمان‌های قدیم اهمیت دسترسی به اطلاعات و نیز امنیت و حفاظت از اطلاعات برای حکمرانان مطرح بوده است و دستیابی به اطلاعات نظامی و کشوری گاه موجب نابودی قومی می‌شده است. در سازمان‌ها نیز گسترش روزافزون استفاده از اطلاعات، آن را به یک دارایی واقعی و گران‌بهای سازمانی تبدیل کرده است(دور و الویسی[1]، ۲۰۱۶). با توسعه فناوری اطلاعات و استفاده از اطلاعات به‌عنوان یک ابزار تجاری و سرمایه سودآور، بحث امنیت اطلاعات بعد جدیدی به خود می‌گیرد. در عصر حاضر و هم‌زمان با بزرگ شدن شرکت‌ها و سازمان‌ها و افزایش وابستگی آن‌ها به سیستم‌های کامپیوتری، موضوع مدیریت امنیت اطلاعات اهمیت قابل‌توجهی پیدا کرده است. سازمان‌ها، باارزش‌ترین دارایی خود را جهت پردازش و ذخیره‌سازی در اختیار تجهیزات فناوری اطلاعات قرار داده‌اند. وابستگی به این فناوری باعث شده است تا اگر در ارائه خدمات خللی پیش آید، سازمان‌ها نتوانند به کار خود ادامه دهند.

همگام با رشد سیستم‌های اطلاعاتی و اینترنت تهدیدات مرتبط با امنیت اطلاعات نیز به‌مرورزمان تکامل‌یافته‌تر می‌گردند. حتی اگر با پیشرفت فنّاوری‌های تأمین امنیت، از طریق پیشرفت معماری، پروتکل‌ها، الگوریتم‌ها و ابزارهای ریاضی، پیچیده‌تر و قوی‌تر شوند، به دلیل پیشرفت فن‌آوری موازی حمله بدافزارها، حذف کامل آسیب‌پذیری‌های امنیتی باز هم امکان‌پذیر نیست. زیان‌های هنگفت ناشی از کلاه‌برداری‌های امنیتی، امنیت اطلاعات را به موضوعی حیاتی و جذاب در دنیای کسب‌وکار تبدیل کرده (اسپانوس و آنجلیس[2]، ۲۰۱۶). علاوه بر این، وضعیت امنیت اطلاعات سازمان، به‌طور مستقیم بر بسیاری از جنبه‌های سازمان تأثیر می‌گذارد. بنابراین یکی از مهم‌ترین مسائلی که سازمان‌های امروزی با آن مواجه‌اند، چگونگی حفاظت خود در مقابل حملات احتمالی سایبری است(فیلدرا و همکاران[3]، ۲۰۱۶). ولی برخی از خطرات امنیتی نسبت به هزینه‌ای که کنترلشان به سازمان تحمیل می‌کند، اهمیت

1. Dor & Elovici
2. Spanos & Angelis
3. Fieldera et al.

پایینی دارند و برای سازمان بهتر است که آن‌ها را نادیده بگیرد. به عبارتی، سرمایه‌گذاری در حوزه امنیت اطلاعات نیاز به‌نوعی ارزیابی منفعت – هزینه دارد. سرمایه‌گذاری امنیت فناوری اطلاعات سرمایه‌گذاری‌هایی است که یک شرکت برای تقویت دفاع از سیستم‌های اطلاعاتی خود و محافظت از اطلاعات محرمانه خود در برابر حملات احتمالی دارد اسپانوس و آنجلیس، ۲۰۱۶).

پژوهشگران بر این باورند که اکثر سازمان‌ها بدون توجه به تهدیدات فناوری اطلاعات، هزینه‌های بسیاری برای توسعه این فناوری صرف می‌کنند و اغلب با اجرای راهبردهای مقطعی (مانند نصب آنتی‌ویروس، دیوار آتش و...) سعی دارند تا سازمان و اطلاعات خود را حفظ کنند. بسیار مشاهده شده است سازمان‌ها خسارت شدیدی را از این بابت متحمل شده‌اند، اما متأسفانه همین روش را هم چنان ادامه می‌دهند(پیکام و سلیمی فرد[1]، ۲۰۱۶).

موضوع امنیت دارایی‌های اطلاعاتی در تحقیقات بسیاری موردتوجه قرار گرفته است، ولی ملاحظات اقتصادی مربوط به سرمایه‌گذاری‌های امنیت اطلاعات هنوز آن‌چنان‌که باید موردتوجه قرار نگرفته است و بررسی اقتصادی امنیت اطلاعات موضوع تحقیقاتی جدیدتری است که تهدیدات و خطرات اطلاعاتی حال و آینده سازمان را موردبررسی قرار داده، آن‌ها را اولویت‌بندی کرده و اقدامات متقابل مناسبی را پیشنهاد می‌دهد که ازلحاظ اقتصادی مقرون‌به‌صرفه‌اند(دور و الویسی، ۲۰۱۶). بنابراین حوزه اقتصاد امنیت اطلاعات باهدف بهبود پیامدهای مالی در مواجهه و مقابله با ریسک‌ها و حملاتی که امنیت اطلاعات سازمان را تهدید می‌کند، به وجود آمده است. این حوزه از یک‌سو به موضوعات روز امنیت اطلاعات می‌پردازد و از سوی دیگر، بینش‌های جدیدی را برای اقتصاددانان و مدیران استراتژیک سازمان فراهم می‌آورد. اقتصاد امنیت اطلاعات اخیراً به یک‌رشته تحقیقاتی در حال رشد تبدیل شده است که برای مدیریت تصمیمات امنیتی در سازمان‌ها بسیار حائز اهمیت است. این زمینه بینش ارزشمندی نه‌تنها برای کارشناسان امنیت اطلاعات بلکه برای سیاست‌گذاران،

1. Pikam & Salimi fard

اقتصاددانان و مدیران کسب‌وکار فراهم می‌کند(آسو آمینه ژاد و همکاران[1]، ۲۰۱۶)

در این پژوهش با انجام یک مرور سیستماتیک بر مقالات مرتبط با حوزه سرمایه‌گذاری امنیت اطلاعات، به بررسی روش‌های مورداستفاده در این پژوهش‌ها و فاکتورهای کلیدی این حوزه پرداخته شده است. این پژوهش در نظر دارد، مقالاتی که در این حوزه منتشرشده‌اند را بررسی کرده و روش‌ها و روندهای سرمایه‌گذاری در حوزه امنیت اطلاعات را ارزیابی نماید و در پی پاسخ به این سؤال است که بر اساس ادبیات موجود در زمینه سرمایه‌گذاری مدیریت امنیت اطلاعات، روش بهینه سرمایه‌گذاری در امنیت اطلاعات چیست؟ بر این اساس در بخش دوم مقاله به مبانی نظری پژوهش پرداخته شده است، در بخش سوم روش پژوهش شرح داده شده است، در بخش چهارم نتایج پژوهش ارائه شده است و در بخش پنجم نتیجه‌گیری و بحث پیرامون نتایج ارائه گردیده است.

مبانی نظری پژوهش

تعریف امنیت اطلاعات مسئله دشواری است. درواقع آنچه ما باید تعریف کنیم اهداف امنیتی (مانند محرمانه بودن، یکپارچگی) است(تیسیاکیس و استفانیدس[2]، ۲۰۰۵). به‌طورکلی امنیت اطلاعات به حفاظت و نگهداری از اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز تعبیر می‌گردد. این فعالیت‌ها شامل دسترسی، استفاده، خواندن، خراب کردن، افشاء ، نسخه‌برداری تغییر و دست‌کاری است. درواقع محرمانگی، یکپارچگی و در دسترس بودن اطلاعات از مباحث اصلی امنیت اطلاعات هستند.

اَندرسون معتقد است زمانی که در مورد امنیت اطلاعات بحث می‌شود، نباید تنها به بحث درباره فناوری امنیت اطلاعات پرداخت، بلکه لازم است انگیزه‌های اقتصادی هم در نظر گرفته شوند(تاناکا و همکاران[3]، ۲۰۰۵)

1. Asou Aminnezhad et al.
2. Tsiakis & Stephanides
3. Tanaka et al.

سرمایه‌گذاری امنیت اطلاعات

مفهوم سرمایه‌گذاری یک هدف دارد: ایجاد بازده. این بازده را می‌توان در قالب سرمایه، زمان و مزایا (ملموس و ناملموس) مشاهده کرد. اما محاسبه دارایی‌های ناملموس دشوار است و برای محاسبه آن، باید به معادل پولی تبدیل شود. یک سازمان جهت به‌کارگیری اقدامات متقابل امنیتی برای بهبود سطح امنیت دارائی‌های اطلاعاتی خود، بایستی هزینه‌هایی را متحمل شود. ازآنجایی‌که این هزینه‌ها مزایای ملموس و ناملموسی را برای سازمان به ارمغان خواهند آورد، سرمایه‌گذاری در امنیت اطلاعات نامیده می‌شوند.

هدف اصلی مطالعه اقتصاد امنیت اطلاعات، کنترل و اندازه‌گیری مزایای حاصل از سرمایه‌گذاری در امنیت، تعیین عوامل کلیدی در ارزیابی قابلیت سوددهی سرمایه‌گذاری در امنیت اطلاعات و تخمین میزان سرمایه‌گذاری و مشخص کردن زمانی است که بازدهی قابل‌انتظار است. در بسیاری از مطالعات انجام‌شده سرمایه‌گذاری به‌عنوان عاملی در نظر گرفته می‌شود که سبب افزایش امنیت می‌شود، بر این اساس برای رسیدن به امنیت مطلق (امنیت ۱۰۰ درصد)، هزینه‌های امنیت به‌صورت نمایی افزایش خواهند یافت.به‌منظور دستیابی به یک تصمیم سرمایه‌گذاری امنیتی، باید تحلیلی پیرامون دارایی‌های فیزیکی و منطقی داشت و شدت و احتمال آسیب‌رسانی تهدیدها را برای یافتن بهترین روش مقابله با آن ارزیابی نمود. دارایی‌های فیزیکی و منطقی سازمان را می‌توان به پنج دسته: اطلاعاتی، نرم‌افزاری، سخت‌افزاری، انسانی و سیستمی تقسیم کرد. سرمایه‌گذاری در حوزه امنیت اطلاعات به‌عنوان یک تصمیم مهم این حوزه، با عدم اطمینان زیادی روبرو است و باید به‌طورجدی موردتوجه قرار گیرد. مشکلات امنیت اطلاعات سه نوع تأثیر اقتصادی بر سازمان‌ها خواهد داشت:

- تأثیر اقتصادی فوری که هزینه تعمیر و یا جایگزینی سیستم‌ها و اختلال در عملیات تجاری و جریان نقدی را به همراه خواهد داشت.
- تأثیر کوتاه‌مدت اقتصادی و از دست دادن روابط قراردادی یا مشتریان موجود به علت عدم توانایی ارائه محصولات یا خدمات و تأثیر منفی بر شهرت سازمان.

- تأثیرات اقتصادی بلندمدت و کاهش ارزش قیمت سهام و بازار سازمان(تیسیاکیس و استفانیدس، ۲۰۰۵).

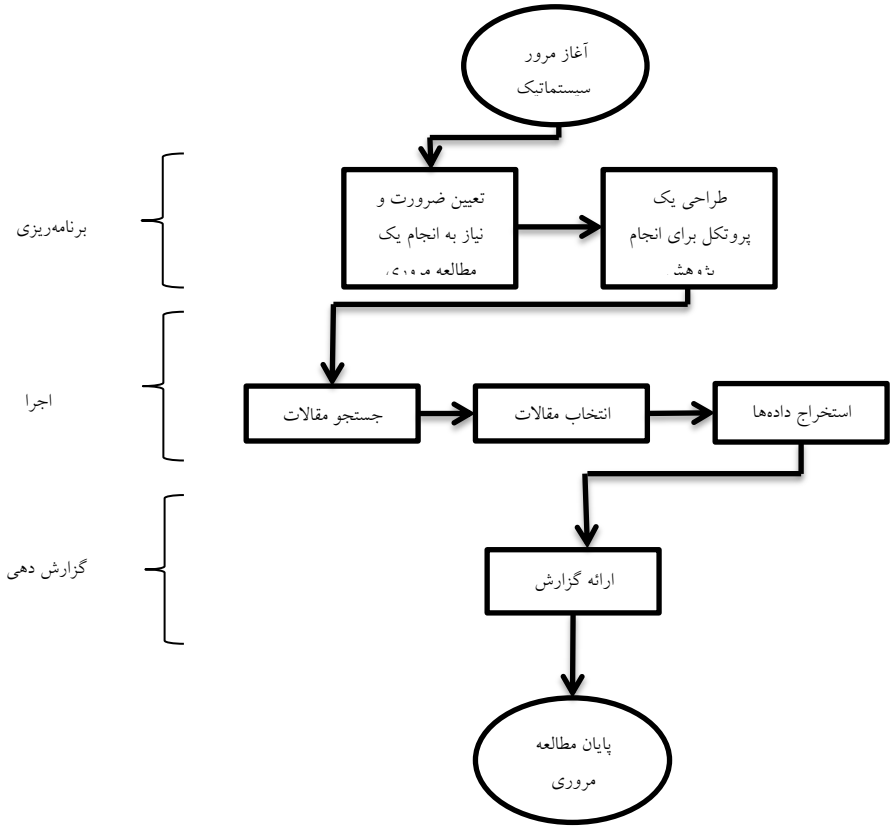
روش پژوهش

مرور سیستماتیک یک روش بسیار قدرتمند برای محققان است که اطلاعات مربوط به تحقیق در یک حوزه خاص را به شکل خلاصه ارائه می‌دهد. در دهه‌های اخیر تحقیقات بسیاری از این نوع در حوزه‌های مختلف علمی مثل پزشکی، علوم فیزیکی، علوم اجتماعی، اقتصاد و علوم کامپیوتر انجام شده است.

روش انجام مرور سیستماتیک در این پژوهش، روش‌هایی است که در(باربارا[1]، ۲۰۰۴) و (کیچنهام و چارترز[2]، ۲۰۰۷) شرح داده شده است. اگرچه این دستورالعمل‌ها در حوزه مهندسی نرم‌افزار ارائه‌شده‌اند ولی شامل اصول اساسی، عمومی و معتبر برای هر مرور سامانمند هستند، بدین‌جهت در این پژوهش نیز به کار گرفته‌شده‌اند.

بر اساس دستورالعمل‌های فوق، مرور سیستماتیک سه مرحله دارد: مرحله برنامه‌ریزی، مرحله اجرا و مرحله گزارش دهی. شکل ۱ این مراحل را نشان می‌دهد.

1. Barbara
2. Kitchenham & Charters



شکل ۱. مراحل انجام مطالعه مروری(اسپانوس و آنجلیس، ۲۰۱۶)

مرحله برنامه‌ریزی

اولین گام از مرحله برنامه‌ریزی، تعیین ضرورت انجام یک مرور سیستماتیک است. همان‌طور که پیش‌ازاین نیز توضیح داده شده است، اگرچه مطالعات متعددی پیرامون تأثیرات حوادث امنیت اطلاعات وجود دارد، اما در مورد چگونگی تعیین سرمایه‌گذاری بهینه در حوزه امنیت اطلاعات هنوز سؤالاتی وجود دارد(دور و الویسی، ۲۰۱۶). با بررسی سیستماتیک مطالعاتی که به این موضوع پرداخته‌اند می‌توان به بینش عمیق‌تری در این حوزه دست یافت. بنابراین

این پژوهش با مرور پژوهش‌های پیشین اطلاعاتی را به‌ویژه در مورد روش‌شناسی مورداستفاده برای بهینه‌سازی سرمایه‌گذاری حوزه امنیت اطلاعات به پژوهشگران ارائه می‌دهد.
گام دوم مرحله برنامه‌ریزی، طراحی و تعیین پروتکل پژوهش است. اساساً پروتکل تمام فرایند مرحله اجرایی را همراه با تحلیل اقدامات، تعریف می‌کند. این اقدامات عبارت‌اند از:

تعریف سؤالات پژوهش

تعریف پرسش‌های پژوهش، گام بسیار مهمی در هر بررسی سیستماتیک است. پاسخ دادن به این سؤالات، هدف اصلی یک مقاله مروری است. سؤالات موردبررسی در پژوهش حاضر به شرح زیراست:

۱) تعداد پژوهش‌های انجام‌شده پیرامون سرمایه‌گذاری بهینه در امنیت اطلاعات چقدر است؟
۲) برای انجام فرایند پشتیبانی از تصمیم در سرمایه‌گذاری امنیت اطلاعات (در سازمان‌ها) چه روش‌هایی و رویکردهایی وجود دارد؟
۳) در سال‌های مختلف تعداد پژوهش‌های انجام‌شده حوزه سرمایه‌گذاری در امنیت اطلاعات چه روندی را طی نموده است(افزایشی یا کاهشی) ؟
۴) در رویکردهای مورداستفاده فرایند پشتیبانی از تصمیم در سرمایه‌گذاری امنیت اطلاعات آیا گرایش و جهت‌گیری خاصی به سمت استفاده از یک رویکرد و روش وجود دارد؟

انتخاب استراتژی جستجو(تعیین منطق و کلیدواژه‌های مناسب جستجو برای پایگاه داده‌ها)

انتخاب استراتژی پژوهش شامل دو مرحله انتخاب روش جستجو و تعریف معیارهای ورود و خروج مقالات به مطالعه است.

انتخاب روش جستجو

قدم اول تصمیم‌گیری در مورد استراتژی جستجو شامل انتخاب روش جستجو است که می‌تواند یکی از موارد جستجوی گسترده‌ی خودکار در کتابخانه‌های دیجیتال، جستجو دستی در نشریات و کنفرانس‌های خاص، فن گلوله‌ی برفی و یا ترکیبی از این روش‌ها

باشد((اسپانوس و آنجلیس، ۲۰۱۶). در پژوهش حاضر روش جستجوی وسیع شامل انتخاب منابع دیجیتالی مناسب و تعیین اصطلاحات کلیدی جستجو است. انتخاب کلمات کلیدی بر اساس بررسی مقالات مهم مربوطه به این حوزه بوده است. اقتصادسنجی امنیت اطلاعات[1]، اقتصاد امنیت اطلاعات[2]، سرمایه‌گذاری در امنیت اطلاعات[3] و سرمایه‌گذاری امنیت اطلاعات[4] کلیدواژه‌هایی هستند که در این پژوهش در پایگاه داده‌های IEEE ، Web of Science ،Springer، Science Direct مورد جستجو و بررسی قرار گرفته‌اند.

تعریف معیارهای ورود / خروج به مطالعه

معیارهای انتخاب یا رد مقالات در هر بررسی سامانمند باید واضح و مشخص باشد. در پژوهش حاضر معیار ورود مقالاتی هستند که در بازه زمانی ۲۰۰۶ تا ۲۰۱۷ منتشر و به بررسی چگونگی سرمایه‌گذاری در امنیت اطلاعات پرداخته‌اند و کلیدواژه‌های بیان‌شده در بخش قبل در عنوان مقاله وجود داشته است. بر این اساس مقالاتی که صرفاً به سرمایه‌گذاری فناوری اطلاعات در سازمان‌ها پرداخته بودند از پژوهش حذف شدند.

بررسی اولیه نتایج

این مرحله شامل خواندن عنوان، چکیده و کلیدواژه‌های مقالات جستجو شده و حذف مقالات نامرتبط است.

حذف مقالات تکراری

برخی مقالات در چندین پایگاه اطلاعاتی وجود دارند. در این مرحله مقالات تکراری از مطالعه حذف می‌شوند.

درنهایت تعیین مقالات نهایی برای استخراج داده‌ها

در آخر و پس از انجام مراحل گفته‌شده، مقالات نهایی برای انجام پژوهش تعیین می‌شوند.

1. Information security Econometrics
2. Information security Economic
3. Information Security investing
4. Information Security investment

مرحله اجرا

در این بخش مراحل اجرای پژوهش شرح داده می‌شود.

جستجو و انتخاب مقالات

در این پژوهش در مرحله اول و در فرآیند جستجو اولیه، تعداد ۱۴۶ مقاله انتخاب گردید. به‌منظور انجام مرور سیستماتیک کلیه مطالعات انجام‌گرفته در زمینه موضوع این پژوهش با استفاده از کلیدواژه‌های پژوهش از پایگاه داده‌های Springer، IEEE-Explore ، Web of Science، Science direct بر اساس جدول۱ استخراج شده است.

جدول۱. پایگاه داده‌ها و مقالات اولیه

پایگاه داده	تعداد مقالات اولیه
Science direct	۳۸
Web of knowledge	٦۸
IEEE-Explore	۲۷
Springer	۱۳
مجموع مقالات	**۱٤٦**

پس از خواندن عناوین و چکیده مقالات، ۳۶ مقاله نامرتبط حذف شد و ۱۱۰ مقاله موردبررسی بیشتر قرار گرفت و با حذف مقالات غیر مرتبط و یا تکراری، ۶۵ مقاله دیگر حذف و ۴۶ مقاله انتخاب و موردبررسی کامل قرار گرفت. با خواندن مقالات و بررسی منابع آن‌ها، ۹ مقاله دیگر به مجموعه اضافه شد و نهایتاً **55** مقاله برای انجام مرور انتخاب گردید. برای کمک به توضیح این فرآیند، شکل ۲ مراحل اجرای پژوهش را نشان می‌دهد.

شکل ۲. مراحل اجرای پژوهش

استخراج و ترکیب داده‌ها

فرایند استخراج داده‌ها از ۵۵ مقاله انتخابی انجام شد.

مرحله گزارش

در این بخش نتایج حاصل از مرور سیستماتیک ارائه‌شده است. در جدول۲ ، اطلاعات استخراج‌شده از مقالات نشان داده شده است.

جدول ۲. مقالات استخراج‌شده در پژوهش

شناسه مقاله	عنوان مقاله	سال انتشار	رویکرد
مقالات استخراج‌شده از Science direct			
SC1(Huang et al., 2014)	Optimal Information Security Investment in a Healthcare Information Exchange: An Economic Analysis	2014	UM
SC2(Ryan &	Expected benefits of	2006	ROI

		information security investments	Ryan, 2006)
game theory	2016	Decision support approaches for cyber security investment	SC3 (Fielder et al., 2016)
game theory	2014	Network externality and incentive to invest in network security	SC4(Liao & Chen, 2014)
DSS	2016	A Model of the Information Security Investment Decision-Making Process	SC5(Dor & Elovici, 2016)
game theory	2015	Game of information security investment: Impact of attack types and network vulnerability	SC6 (Wu et al., 2015)
expected utility theory	2008	An economic analysis of the optimal information security investment in the case of a risk-averse firm	SC7(Derrick Huang et al., 2008)
Event methodology efficient market theory	2011	Firms' information security investment decisions: Stock market evidence of investors' behavior	SC8 (Chai et al., 2011)
risk-based approach theory	2011	Profit-maximizing firm investments in customer information security	SC9(Lee et al., 2011)
game theory	2011	Knowledge sharing and investment decisions in information security	SC10(Liu et al., 2011)
UM	2013	Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints	SC11(Huang & Behara, 2013)
expected utility approach	2016	An economic model to evaluate information	SC12(Sanjaya Mayadunnea &

		security investment of risktaking small and medium enterprises	Parkb, 2016)
Resource-based theory	2015	Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources	SC13(Huseyin Cavusoglu et al., 2015)
DSS	2015	Managing the investment in information security technology by use of a quantitative modeling	SC14(Bojanc, Jerman-Blazic, & Tekavcic, 2012)
game theory	2013	A differential game approach to information security investment under hackers' knowledge dissemination	SC15(Xing Gao et al., 2013)
risk-based approach	2010	Information security initiatives: counting the cost	SC16(Everett, 2010)
game theory	2017	Information sharing vs. privacy: A game theoretic analysis	SC17(Ezhei & Tork Ladani, 2017)
مقالات استخراج‌شده از Springer			
game theory	2015	Information security investment for competitive firms with hacker behavior and security requirements	SP1(Gao & Zhong, 2015)
ROI	2006	Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to	SP2(Hausken, 2006)

		vulnerability	
UM	2014	Returns to information security investment: Endogenizing the expected loss	SP3(Hausken, 2014)
risk-based approach	2011	Risk-neutral evaluation of information security investment on data centers	SP4(S. L. Wang et al., 2011)
game theory	2017	A game-theoretic analysis of information security investment for multiple firms in a network	SP5(Qian et al., 2017)
game theory	2017	Security investment and information sharing in the market of complementary firms: impact of complementarity degree and industry size	SP6(Liu et al., 2017)
game theory	2017	Optimal Information Security Investment in Modern Social Networking	SP7 (Trufanov, Kinash, Tikhomirov, Berestneva, & Rossodivita, 2017)
مقالات استخراج‌شده از Web of Science			
Game theory	2014	A game-theoretic analysis of information sharing and security investment for complementary firms	WOS1(Gao, Zhong, & Mei, 2014)
BSC perspective	2012	An analysis on effects of information security investments: a BSC perspective	WOS2(Kong et al., 2012)
game theory	2008	Decision-Theoretic and Game-Theoretic Approaches to IT	WOS3(H. Cavusoglu et al., 2008)

		Security Investment	
game theory	2013	Information Security Investment When Hackers Disseminate Knowledge	WOS4(X. Gao, W. J. Zhong, & S. Mei, 2013)
Real Options	2008	Investments in Information Security: A Real Options Perspective with Bayesian Postaudit	WOS5(Herath & Herath, 2008)
Time Series Models	2009	Quantifying the Benefits of Investing in Information Security	WOS6(Khansa & Liginlal, 2009)
risk-based approach	2008	A Value-at-Risk Approach to Information Security Investment	WOS7(J. Wang et al., 2008)
مقالات استخراج‌شده از IEEE-Explore			
ROI	2008	APPLYING ROI ANALYSIS TO SUPPORT SOA INFORMATION SECURITY INVESTMENT DECISIONS	IE1(Buck & Diane, 2008)
game theory	2015	Analyzing Information Security Investment in Networked Supply Chains	IE2(Gu, Mei , & Zhong 2015)
ROI	2014	Economic and financial analysis of investments in information security	IE3(Zvonko et al., 2014)
ROI	2009	Forecasting for Return on Security Information Investment: New Approach on Trends in Intrusion Detection and Unwanted Internet Traffic	IE4(Pontes, Guelfi, & Alonso, 2009)
NPV and RoI	2010	Information Security Investment Decision by Fuzzy Economics	IE5(Sheen, 2010)

game theory	2008	Information Security Investment Game with Penalty Parameter	IE6(Wei Sun, Xiangwei Kong, Dequan He, & You, 2008)
expected risks	2008	Towards an Optimal Information Security Investment Strategy	IE7(Z. Wang & Song, 2008)
game theory	2016	Optimal Information Security Investment Analyses with the Consideration of the Benefits of Investment and Using Evolutionary Game Theory	IE8(Q. Wang, Zhu, & China., 2016)
game theory	2010	Study on the Organization Information Security Investment Decision-Making Based on the Limited Strategy Game Theory Perspective	IE9(Zeshuang & jing., 2010)
real options approach	۲۰۱۲	Valuing information security investment A real options approach	IE10(Jun Wan, Bin Ding, YunFei Ren, Zheng, & Guo., 2012)
Kano's theory	2016	Which IT Security Investments Will Pay Off for Suppliers? Using the Kano Model to Determine Customers' Willingness to Pay	IE11(Rabea Sonnenschein, André Loske, & Buxmann., 2016)
DSS	2012	Investment analysis of Information Security Management in Croatian seaports	IE12(Saša Aksentijević , Edvard Tijan , & Hlača., 2012)
techno-business modeling	2010	Justifying information security investments in web software: (Quantitative techno-	IE13(Josip Zoric , Arne Helme , Håvard Kvalheim, &

		business modeling approach)	Sundve., 2010)
game theory	2017	Investment strategy analysis of information systems with different security levels	IE14(Pan, Zhong, & Mei, 2017)
game theory	2015	Cyber-Investment and Cyber-Information Exchange Decision Modeling	IE15(Tosh, Molloy, Sengupta, Kamhoua, & Kwiat, 2015)
مقالات استخراج‌شده از بررسی منابع مقالات			
game theory	2007	Strategic games on defense trees	UN1(Bistarelli, Dall'Aglio, & Peretti., 2007)
ROI, NPV	2006	An Overview of Economic Approaches to Information Security Management	UN2(Su, 2006)
risk-based approach	2012	Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System	UN3(Bojanc & Jerman-Blazic, 2012)
ROI, NPV	2006	Budgeting Process for INFORMATION SECURITY EXPENDITURES	UN4(Gordon & Loeb, 2006)
UM	2010	Extending the Gordon&Loeb model for information security investment.	UN5(Willemson, 2010)
Real option	2015	The impact of information sharing on cybersecurity underinvestment: A real options perspective	UN6(Gordon, Loeb, Lucyshyn, & Zhou, 2015)

Real option	2007	Making cost effective security decision with real option thinking.	UN7(Jingyue & Xiaomeng, 2007)
ROI	2015	Maintaining Cyber Security: Implications, Cost and Returns	UN8(Kesswani & Kumar, 2015)
Survey	2007	Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms	UN9(Wei Liu, Hideyuki Tanaka, & Matsuura., 2007)

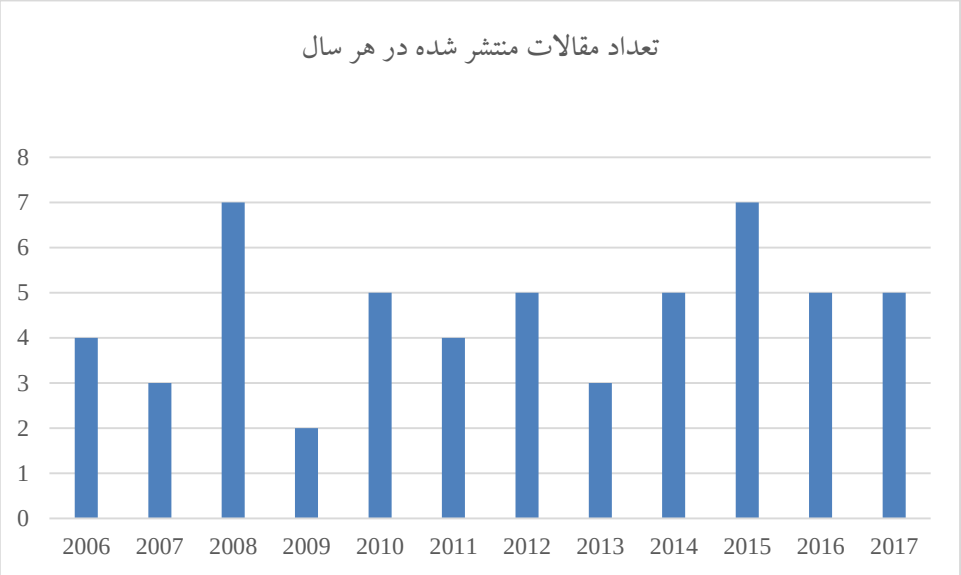
یافته‌ها

در این بخش با استفاده از بررسی‌های انجام‌شده در مرحله قبل به سؤالات مطرح‌شده در پژوهش پاسخ‌داده‌شده است.

- نتیجه سؤال ۱: میزان پژوهش‌هایی که پیرامون سرمایه‌گذاری بهینه در امنیت اطلاعات انجام‌شده چقدر است؟

نمودار ۱ بیانگر این است که در سال‌های اخیر تا حدودی تمایل و گرایش بیشتری به پژوهش‌های حوزه سرمایه‌گذاری بهینه در امنیت اطلاعات وجود دارد و این حوزه رسمیت بیشتری یافته و تعداد پژوهش‌ها در این زمینه نوسان کمتری داشته است.

با توجه به پیشرفت سریع فناوری اطلاعات در سال‌های اخیر نقش سیستم‌های اطلاعاتی در سازمان‌ها پررنگ‌تر شده است و از سوی دیگر عرصه رقابت شدید میان سازمان‌ها این امر را می‌طلبد که تصمیمات اقتصادی آن‌ها با توجه و برنامه‌ریزی بیشتری همراه باشد. ازاین‌رو بدیهی است مطالعاتی که در بهینه‌سازی تصمیمات سرمایه‌گذاری امنیت اطلاعات به سازمان یاری رساند بیشتر موردتوجه قرار گیرند.



نمودار ۱. تعداد پژوهش‌های انجام‌شده در سال‌های مختلف

❖ نتیجه سؤال۲: چه روش‌ها و رویکردهایی برای فرایند پشتیبانی از تصمیم در سرمایه‌گذاری امنیت اطلاعات در سازمان‌ها وجود دارد؟

با بررسی مقالات و تجزیه‌وتحلیل داده‌های استخراج‌شده از آن، روش‌های مورداستفاده در حوزه سرمایه‌گذاری در امنیت مشخص شد. ۸ رویکرد کلی این حوزه و توضیح مختصری از هر یک از آن‌ها به شرح زیر است:

- تئوری بازی‌ها[1]: تئوری بازی، تعاملات استراتژیک بین تصمیم‌گیرندگان یا بازیکنان را از طریق مدل‌های ریاضی به نام بازی‌ها موردبررسی قرار می‌دهد(گرونبائک و همکاران[2]، ۲۰۱۲).
- رویکرد مبتنی بر ریسک[3]: در این رویکرد، تصمیم‌گیرندگان می‌توانند به‌جای دنبال کردن راه‌حلی که تنها هزینه‌های مورد انتظار را به حداقل برساند، بر اساس

1. Game theory
2. Gronbaek
3. Risk based approach

اولویت‌بندی ریسک‌ها، یک تصمیم مناسب در سرمایه‌گذاری داشته باشند(جی وانگ و همکاران[1]، ۲۰۰۸).

- سیستم‌های پشتیبان تصمیم[2]: ابزارهای قدرتمندی هستند که روش‌های علمی برای پشتیبانی از تصمیم‌های پیچیده را با فنون توسعه‌یافته در فناوری اطلاعات ادغام می‌کنند. آن‌ها خصوصاً در شرایطی که مقدار اطلاعات موجود مانعِ ادراک شهودی فرد تصمیم‌گیرنده است و آنگاه‌که دقت و بهینه بودن مهم هستند، بسیار باارزش‌اند. DSSها با گردآوری منابع اطلاعاتی گوناگون، فراهم کردن دسترسی هوشمند به دانشِ مرتبط و کمک به فرایند سازمان‌دهی و بهینه‌سازی تصمیم‌ها، به نارسایی‌های ادراکی انسان کمک می‌کنند.
- حداکثر سازی مطلوبیت(UM) :حداکثر سازی مطلوبیت یک مکانیزم تصمیم‌گیری است که به دنبال به حداکثر رساندن سود و ارزش کسب‌شده از یک سرمایه‌گذاری است(جکیوتسالیتیس و استاتوپولوس[3]، ۲۰۱۵).
- نرخ بازده سرمایه‌گذاری[4] (ROI): نرخ بازده سرمایه‌گذاری برابر است با (اختلاف بین منافع به‌دست‌آمده و هزینه‌های انجام‌شده تقسیم‌بر هزینه‌های انجام‌شده) ضربدر ۱۰۰ (زرندی فرد, ۱۳۹۳).
- فن ارزش خالص فعلی[5] (NPV) : فن NPV (ارزش خالص فعلی) یکی از فنونی است که در ارزیابی پروژه‌ها استفاده می‌شود. این فن واگذاری تعهد منفعلانه مدیریت، به استراتژی عملیاتی منجر می‌شود (مثل شروع فوری پروژه و عملیاتی کردن آن به‌طور مستمر تا پایان عمر مفید مورد انتظار)، همچنین تأثیر هم‌افزایی را

1. J. Wang et al.
2. Decision Support System
3. Gkiotsalitis & Stathopoulos
4. Return On Investment
5. Net Present Value

نادیـده می‌گیرد (مثل ارتباط سودآور با پروژه‌های دیگر). بنابراین این فن می‌تواند نتایج ذیـل را داشته باشد: ۱ (متوقف کردن زودهنگام پروژه‌هایی که به‌طور اقتصـادی بـرای سـازمان منفعت دارند یا ۲ (ادامه پروژه‌هایی که نامناسـب اسـت و درواقـع پافشـاری در آن خطرنـاک است(کیلی و فلاتو[1]، ۱۹۹۹؛ مشباکی و همکاران[2]، ۲۰۱۰)

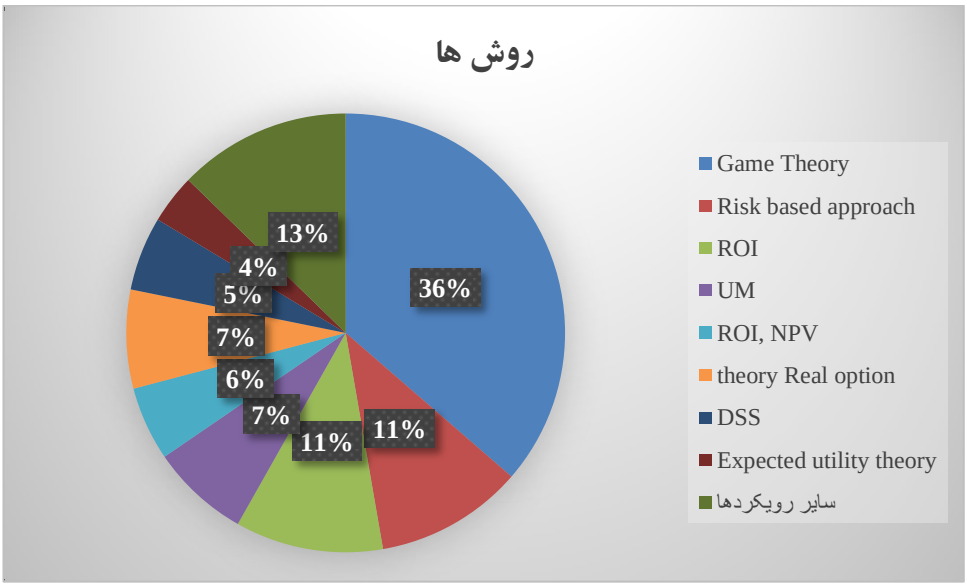
- نظریهٔ مطلوبیت مورد انتظار[3] : بر اساس نظریهٔ مطلوبیت مورد انتظار سرمایه‌گذاران ریسـک گریزنـد و ریسـک گریـزی معـادل معقـر بـودن تـابع مطلوبیـت آن‌ها اسـت(نظری و همکاران[4]، ۲۰۱۴).
- نظریه گزینه‌های واقعی[5]: نظریه گزینه‌های واقعی یکی از ابزارهای علم مدیریت (علـم تصمیم‌گیری) اسـت کـه در جهت رفع محدودیت‌های تحلیل ارزش فعلی خالص سنتی ارائه شده اسـت.

مفهوم گزینه واقعی مبتنی بر این حقیقت است که مـدیریت، همان‌طور کـه اطلاعـات بیشتر را به دست می‌آورد، انعطاف‌پذیری لازم بـرای جـایگزینی تصـمیمات را دارد. اگـر شرایط آینده مناسب باشد، پروژه ممکن است جهت استفاده از این شرایط گسترده‌تر شود .به عبارتی گزینه واقعی یک تصمیم پویا است(مشباکی و همکاران[6]، ۲۰۱۰).

1. Keil & Flatto
2. Mashbaki
3. Expected utility theory
4. Nazari et al.
5. Real option theory
6. Mashbaki et al.

جدول ۳. روش‌های مورداستفاده در حوزه سرمایه‌گذاری در امنیت اطلاعات

روش مورداستفاده	تعداد مقالات با این رویکرد	درصد مقالات
Game Theory	۲۰	۳۶
Risk based approach	۶	۱۱
ROI	۶	۱۱
UM	۴	۷
ROI, NPV	۳	۵
Real option theory	۴	۷
DSS	۳	۵
Expected utility theory	۲	۴
سایر رویکردها	۷	۱۳



شکل۳. روش‌های به‌کاررفته در پژوهش‌های پیشین

با نگاهی به نتایج، می‌توان نتیجه گرفت که رویکردهای تئوری بازی‌ها و ارزیابی ریسک و *ROI* بیشتر موردتوجه بوده‌اند.

❖ نتیجه سؤال ۳ و ٤:

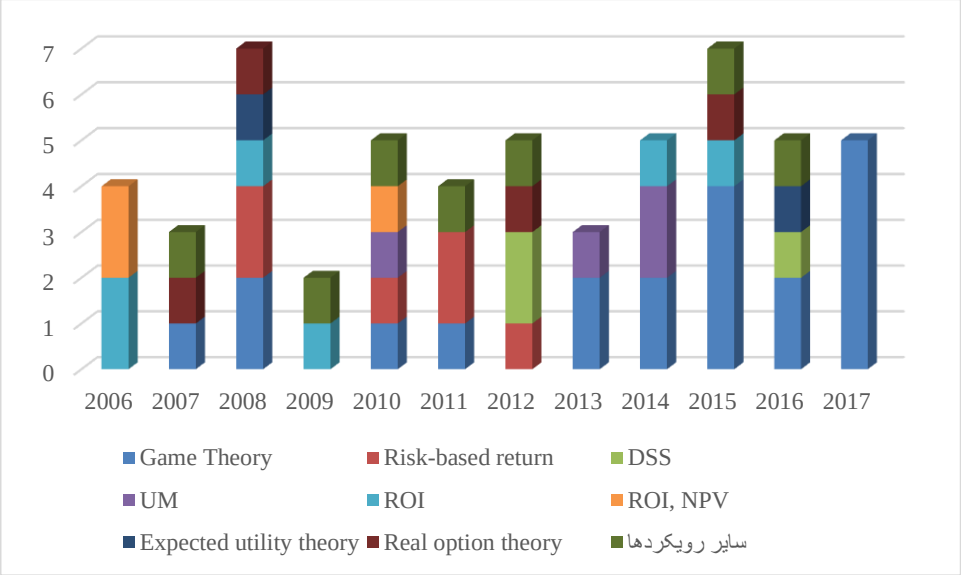
۳) این نوع مطالعات در سال‌های مختلف چه روندی داشته؟ افزایشی یا کاهشی؟

۴) آیا گرایش و جهت‌گیری به سمت استفاده از یک رویکرد خاص وجود دارد؟

در نمودار۳ و جدول ۴ روش‌ها و روند آن‌ها که در بازه زمانی ۲۰۰۶- ۲۰۱۷ بیشتر موردتوجه قرارگرفته‌اند را به ترتیب نمایش می‌دهد.

جدول ٤. روش‌های مورداستفاده در سال‌های مختلف

روش مورداستفاده	۲۰۰۶	۲۰۰۷	۲۰۰۸	۲۰۰۹	۲۰۱۰	۲۰۱۱	۲۰۱۲	۲۰۱۳	۲۰۱۴	۲۰۱۵	۲۰۱۶	۲۰۱۷	مجموع
Game Theory		۱	۲		۱	۱		۲	۲	۴	۲	۵	۲۰
Risk-based return			۲		۱	۲	۱						۶
DSS							۲				۱		۳
UM					۱			۱	۲				۴
ROI	۲		۱	۱					۱	۱			۶
ROI, NPV	۱				۱								۳
Expected utility theory			۱								۱		۲
Real option theory		۱	۱				۱			۱			۴
سایر رویکردها		۱		۱	۱	۱	۱			۱	۱		۷



شکل٤. روش‌های به کار گرفته‌شده در هرسال

با توجه به شکل۲ و نتایج به‌دست‌آمده هرچند نمی‌توان روند مشخص و روشنی برای رویکردهای مختلف یافت ولی در این دسته از مطالعات، توجه و تمایل به استفاده از تئوری بازی‌ها در سال‌های اخیر بیشتر بوده و در این سال‌ها روندی افزایشی دارد. ولی برای سایر روش‌ها روند افزایشی یا کاهشی دیده نمی‌شود.

بحث و نتیجه‌گیری

رشد اطلاعات در دنیای مدرن دیجیتال امروزی، امنیت آن را به موضوعی جدی تبدیل کرده است. در حقیقت تأثیر رویدادهای امنیتی کسب‌وکارها و سازمان‌ها آن‌قدر جدی است که به خطر افتادن امنیت اطلاعات می‌تواند به‌سادگی زندگی روزمره مردم جهان را تحت تأثیر قرار بدهد. بنابراین سرمایه‌گذاری جهانی روی توسعه راهکارهای حفظ امنیت اطلاعات هرساله رو به افزایش است. اما مسئله‌ای که کمتر به آن توجه شده است این است که این سرمایه‌گذاری تا چه میزان به سازمان سود می‌رساند؟ آیا سازمان باید در هر شرایطی هر هزینه‌ای را برای

امنیت اطلاعات خود متحمل شود؟ چه میزان سرمایه‌گذاری در امنیت اطلاعات باید انجام شود؟ پژوهشگران حوزه اقتصاد امنیت اطلاعات در پی پاسخ‌گویی به این سؤالات و ارزیابی تصمیمات استراتژیک پیرامون سرمایه‌گذاری در امنیت اطلاعات هستند.

هر سازمانی برای اطلاعات خود نیاز به سطح معینی از امنیت و روال‌های شفاف و ساده برای به اجرا درآمدن آن و درک چگونگی پیاده‌سازی امنیت اطلاعات در یک محیط عملیاتی دارد. مدیران برای نیل به اهداف تعیین‌شده باید بر سیاست‌های امنیت اطلاعات توجه ویژه داشته باشند. همچنین درک هزینه‌های پیاده‌سازی سیاست‌های امنیتی کارا از اهمیت زیادی برخوردار است.

این مرور سیستماتیک باهدف پاسخ به سؤالاتی پیرامون فرایند تصمیم‌گیری اقتصادی در سرمایه‌گذاری امنیت اطلاعات، انجام شده است. در این پژوهش تعداد ۱۴۶ مقاله موردبررسی قرارگرفته و روش‌های مختلف پشتیبانی از فرایند تصمیم‌گیری در سرمایه‌گذاری‌های امنیت اطلاعات و عوامل اقتصادی مؤثر در هر روش موردبررسی قرار گرفته است. نتایج این پژوهش نشان می‌دهد که ۴۰ درصد مطالعات این حوزه در سال‌های ۲۰۱۴ تا ۲۰۱۷ انجام گرفته است که این نتیجه، اقبال به این حوزه را در سال‌های اخیر نشان می‌دهد. پیش‌ازاین، رویکرد اغلب سازمان‌ها در مواجه با تهدیدات، خرید محصولات امنیتی مانند فایروال و برنامه‌های ضدویروس، و به‌کارگیری آن‌ها در سیستم‌های کامپیوتری بوده است. اما در سال‌های اخیر سازمان‌ها دریافته‌اند که استفاده از گران‌قیمت‌ترین محصولات امنیتی بدون شناخت و تحلیل دقیق نیازهای امنیتی، و به‌روزرسانی مداوم این سیستم‌ها، به‌تنهایی کارساز نخواهد بود. این راهکارها ممکن است باعث شوند امنیت اطلاعات در بعضی حوزه‌ها بیش‌ازحد موردنیاز یا کمتر از حد موردنیاز تأمین شود؛ سازمان‌ها در سال‌های اخیر بیش‌ازپیش دریافته‌اند که محاسبه ارزش اطلاعات ازنظر اقتصادی، بررسی خطرات و محاسبه خسارت‌های احتمالی و تخمین هزینه، سودمندی استفاده از سیستم‌های امنیت اطلاعات، بررسی تهدیدات احتمالی و بررسی راهکارهای مختلف برای آن‌ها ضروری است.

در این مقاله 8 رویکرد مختلف (نظریه گزینه‌های واقعی ، نظریهٔ مطلوبیت مورد انتظار ، فن ارزش خالص فعلی، نرخ بازده سرمایه‌گذاری، حداکثر سازی مطلوبیت، سیستم‌های پشتیبان تصمیم، رویکرد مبتنی بر ریسک و تئوری بازی‌ها) در سرمایه‌گذاری‌های امنیت اطلاعات شناسایی شده است.

هرچند نتایج حاصل از این مقاله نشان می‌دهد که مطالعات پیرامون مبحث سرمایه‌گذاری در امنیت اطلاعات به‌طورکلی روندی افزایشی داشته ولی هنوز هم چندان‌که باید موردتوجه قرار نگرفته است و میزان مطالعات انجام‌شده در این حوزه مهم، نسبت به مطالعاتی که در زمینه‌های فنی امنیت اطلاعات انجام‌شده است ناچیز است. حوزه اقتصاد امنیت اطلاعات در ایران نیز بسیار مورد بی‌توجهی قرار گرفته است. چنین به نظر می‌رسد که سازمان‌ها بدون انجام مطالعات و ارزیابی‌های دقیق و تنها بر اساس قوه شهودی خود نسبت به تعیین میزان سرمایه‌گذاری در امنیت اطلاعات اقدام می‌کنند. به‌عبارت‌دیگر بسیاری از سازمان‌ها به‌ضرورت سرمایه‌گذاری در امنیت اطلاعات واقف‌اند اما در مورد ارزیابی نتایج حاصل از این سرمایه‌گذاری نمی‌توان چنین گفت.

بر اساس نتایج به‌دست‌آمده محققان این حوزه گرایش بیشتری به استفاده از رویکردهای تئوری بازی‌ها، ارزیابی ریسک و ROI دارند. بر اساس نتایج این پژوهش ۳۶ ٪ از پژوهش‌های انجام‌شده در این حوزه در بازه میان سال‌های ۲۰۰۶ تا ۲۰۱۷ از تئوری بازی‌ها استفاده کرده‌اند که به‌کارگیری آن در سال‌های اخیر نیز روندی رو به رشد را نشان می‌دهد. تئوری بازی‌ها ، در تلاش است با کمک گرفتن از ریاضیات، رفتار را در شرایط راهبردی یا بازی‌ها،که در آن‌ها موفقیت فرد یا بنگاه در انتخاب کردن، وابسته به انتخاب دیگران است، تحلیل کند. یک بازی شامل مجموعه‌ای از بازیکنان مجموعه‌ای از حرکت‌ها یا راهبردها و نتیجه مشخصی برای هر ترکیب از راهبردها است. پیروزی در هر بازی تنها تابع احتمالات نیست بلکه اصول و قوانین ویژه خود را دارد و هر بازیکن در طی بازی سعی می‌کند با به‌کارگیری آن اصول خود را به برد نزدیک کند. رویکردهای مبتنی بر ریسک و نرخ بازده سرمایه‌گذاری نیز هرکدام ۱۱٪ از حجم کل رویکردها در مطالعات انجام‌شده را

تشکیل می‌دهند. رویکردهای حداکثر سازی مطلوبیت، نظریه گزینه‌های واقعی و نرخ بازده سرمایه‌گذاری- فن ارزش خالص فعلی هرکدام ۷ ٪ از پژوهش‌ها را دربر می‌گیرد و رویکردهای پشتیبان تصمیم ۵٪ و نظریهٔ مطلوبیت مورد انتظار نیز ۴٪ از مطالعات را به خود اختصاص داده‌اند. بر اساس نتایج به‌دست‌آمده از این پژوهش نمی‌توان در سال‌های موردپژوهش روند مشخصی برای استفاده از این رویکردها یافت.

در این مقاله باهدف تبیین مفاهیم موجود در زمینه سرمایه‌گذاری امنیت اطلاعات و آشنا ساختن فضای علمی کشور با این حوزه جدید، مروری بر روش‌ها و رویکردهای مورداستفاده در این حوزه انجام‌شده است. امروزه ظهور مفهوم‌هایی مثل "اینترنت اشیاء" به روند افزایش حجم داده در سازمان‌ها افزوده و استفاده از حجم عظیم داده‌ها در صنعت و تجارت بسیار رواج پیداکرده است. درعین‌حال بحث امنیتی این "کلان داده"ها اهمیت ویژه‌ای یافته و هزینه‌های هنگفتی را به سازمان‌ها تحمیل کرده است. با در نظر گرفتن این موارد تدوین استراتژی‌هایی برای شناسایی داده‌ها، درک اهمیت آن‌ها و توانایی مدیریت امنیت این داده‌ها با استفاده از تحلیل هزینه- منفعت برای سازمان‌ها بسیار حیاتی است. این پژوهش رویکردهای سرمایه‌گذاری در امنیت اطلاعات را موردبررسی قرار داده است تا پژوهشگران را به انجام پژوهش‌هایی پیرامون سرمایه‌گذاری درست در امنیت اطلاعات هدایت نماید.

این پژوهش با محدودیت‌هایی نیز مواجه بوده است که یکی از آن‌ها محدودیت ذاتی پژوهش‌های مروری یعنی محدودیت در جستجو و بررسی جامع همه پژوهش‌ها است. ممکن است برخی مقالات در مراحل مختلف جستجو نادیده گرفته‌شده و یا حذف‌شده باشند. همچنین این محدودیت که فقط مقالات منتشرشده به زبان انگلیسی موردتوجه قرارگرفته‌اند نیز در این پژوهش وجود دارد.

منابع

Asou Aminnezhad, Ramlan Mahmod, & Abdullah., M. T. (2016). Survey on Economics of Information Security. *IJCSNS International Journal of Computer Science and Network Security, 16*(7).

Barbara, K. (2004). Procedures for Performing Systematic Reviews.

Bistarelli, S., Dall'Aglio, M., & Peretti., P. (2007). Strategic games on defense trees. *Formal Aspects in security and trust lecture*

Bojanc, R., & Jerman-Blazic, B. (2012). Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System. *Paper presented at the 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*.

Bojanc, R., Jerman-Blazic, B., & Tekavcic, M. (2012). Managing the investment in information security technology by use of a quantitative modeling. Information Processing & Management, *48*(6), 1031-1052.

Buck, K., & Diane, D. (2008). Applying ROI Analysis to Support SOA Information Security Investment Decisions.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management, 52*(4), 385-400.

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems, 25*(2), 281-304.

Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems, 50*(4), 651-661.

Derrick Huang, C., Hu, Q., & Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a

risk-averse firm. *International Journal of Production Economics, 114*(2), 793-804.

Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. *Computers & Security, 63*(Supplement C), 1-13.

Everett, C. (2010). Information security initiatives: counting the cost. *Computer Fraud & Security*, 2010(1), 6-7.

Ezhei, M., & Tork Ladani, B. (2017). Information sharing vs. privacy: A game theoretic analysis. *Expert Systems with Applications*, 88, 327-337.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, 86(Supplement C), 13-23.

Gao, X., & Zhong, W. J. (2015). Information security investment for competitive firms with hacker behavior and security requirements. *Annals of Operations Research*, 235(1), 277-300.

Gao, X., Zhong, W. J., & Mei, S. (2013). Information Security Investment When Hackers Disseminate Knowledge. *Decision Analysis*, 10(4), 352-368.

Gao, X., Zhong, W. J., & Mei, S. E. (2014). A game-theoretic analysis of information sharing and security investment for complementary firms. *Journal of the Operational Research Society*, 65(11), 1682-1691.

Gao, X., Zhong, W., & Mei, S. (2013). A differential game approach to information security investment under hackers' knowledge dissemination. Operations Research Letters, 41(5), 421-425.

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

Gkiotsalitis, K., & Stathopoulos, A. (2015). A utility-maximization model for retrieving users' willingness to travel for participating in activities from big-data. *Transportation Research Part C: Emerging Technologies, 58*(Part B), 265-277.

Gordon, L. A., & Loeb, M. P. (2006). Budgeting process for information security expenditures. *Communications of the Acm*, 49(1), 121-125.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy, 34*(5), 509-519.

Grønbæk, L., Lindroos, M., Munro, G., & Pintassilgo, P. Game theory and fisheries. *Fisheries Research*.

Gu, i., Mei , s., & Zhong , W. (2015). Analyzing Information Security Investment in Networked Supply Chains. *Paper presented at the Logistics, Informatics and Service Sciences (LISS), 2015 International Conference* .

Hausken, K. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers, 8*(5), 338-349.

Hausken, K. (2014). Returns to information security investment: Endogenizing the expected loss. *Information Systems Frontiers*, 16(2), 329-336.

Herath, H. S. B., & Herath, T. C. (2008). Investments in Information Security: A Real Options Perspective with Bayesian Postaudit. *Journal of Management Information Systems, 25*(3), 337-375.

Huang, C. D., & Behara, R. S. (2013). Economics of information security investment in the case of concurrent heterogeneous attacks with

budget constraints. *International Journal of Production Economics*, 141(1), 255-268.

Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a Healthcare Information Exchange: An economic analysis. *Decision Support Systems*, 61(Supplement C), 1-11.

Jingyue, L., & Xiaomeng, S. (2007). Making cost effective security decision with real option thinking. *Paper presented at the International Conference on Software Engineering Advances*.

Josip Zoric , Arne Helme , Havard Kvalheim, & Sundve., E. (2010). Justifying information security investments in web software: (Quantitative techno-business modeling approach). *Future Network and Mobile Summit*.

Jun Wan, Bin Ding, YunFei Ren, Zheng, J., & Guo., H. (2012). Valuing information security investment A real options approach. *Paper presented at the Fifth International Conference on Business Intelligence and Financial Engineering*.

Keil, M., & Flatto, J. (1999). Information systems project escalation: a reinterpretation based on options theory. *Accounting, Management and Information Technologies*, 9(2), 115-139.

Kesswani, N., & Kumar, S. (2015). Maintaining Cyber Security: Implications, Cost and Returns. *Computers and People Research*.

Khansa, L., & Liginlal, D. (2009). Quantifying the Benefits of Investing in Information Security. *Communications of the Acm, 52*(11), 113-117.

Kitchenham, & Charters. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering*

Kong, H. K., Kim, T. S., & Kim, J. (2012). An analysis on effects of information security investments: a BSC perspective. *Journal of Intelligent Manufacturing*, 23(4), 941-953.

LAWRENCE A. GORDON, & LOEB, a. M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 5(4), 438–457.

Lee, Y. J., Kauffman, R. J., & Sougstad, R. (2011). Profit-maximizing firm investments in customer information security. *Decision Support Systems*, 51(4), 904-920.

Liao, C.-H., & Chen, C.-W. (2014). Network externality and incentive to invest in network security. *Economic Modelling*, 36(Supplement C), 398-404.

Liu, D., Ji, Y., & Mookerjee, V. (2011). Knowledge sharing and investment decisions in information security. *Decision Support Systems*, 52(1), 95-107.

Mashbaki, A., Poya, A., & Hesar, M. M (2010). The justification of the insistence on the primary decisions of managers in the public sector. *Quarterly Journal of Government Management*, University of Tehran, 2 (5), 159-176.

Nazari, M., Shirzadi, S., and D. Davidi, M. Ah (2014). The Effect of Money Laundering Among Real Investors in Tehran Stock Exchange. Faculty of Management, University of Tehran, *Financial Research*, 16 (1), 147-162.

Pan, C., Zhong, W., & Mei, S. e. (2017, 10-12 March 2017). Investment strategy analysis of information systems with different security levels. *Paper presented at the 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA).*

Pikam, A., & Salimi fard, K. (2016). Providing a framework for investigating the factors affecting the information system's effectiveness through Fuzzy hierarchy analysis. *Quarterly Journal of Information Technology Management Studies*, 61(59), 641-674.

Pontes, E., Guelfi, A., & Alonso, E. (2009). Forecasting for Return on Security Information Investment: New Approach on Trends in Intrusion

Detection and Unwanted Internet Traffic. *IEEE LATIN AMERICA TRANSACTIONS,* 7(4).

Qian, X. F., Liu, X. B., Pei, J., Pardalos, P. M., & Liu, L. (2017). A game-theoretic analysis of information security investment for multiple firms in a network. *Journal of the Operational Research Society, 68*(10), 1290-1305.

Rabea Sonnenschein, André Loske, & Buxmann., P. (2016). Which IT Security Investments Will Pay Off for Suppliers? Using the Kano Model to Determine Customers' Willingness to Pay. *Paper presented at the 49th Hawaii International Conference on System Sciences*.

Rakes, T. R., Deane, J. K., & Paul Rees, L. (2012). IT security planning under uncertainty for high-impact events. *Omega*, 40(1), 79-88.

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.

Ryan, J. J. C. H., & Ryan, D. J. (2006). Expected benefits of information security investments. *Computers & Security*, *25*(8), 579-588.

Sanjaya Mayadunnea, & Park, S. (2016). An economic model to evaluate information security investment of risktaking small and medium enterprises. *Int. J. Production Economics*.

Saša Aksentijević , Edvard Tijan , & Hlaca., B. (2012). Investment analysis of Information Security Management in Croatian seaports. *Paper presented at the Proceedings of the 35th International Convention*.

Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems*, 55(1), 156-164.

Sheen, J. N. (2010). *Information Security Investment Decision by Fuzzy Economics*.

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security, 58*(Supplement C), 216-229.

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems,* 75(Supplement C), 49-62.

Su, X. (2006). *An Overview of Economic Approaches to Information Security Management*.

Tanaka, H., Matsuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy,* 24(1), 37-59.

Tosh, D. K., Molloy, M., Sengupta, S., Kamhoua, C. A., & Kwiat, K. A. (2015, 24-26 Aug. 2015). Cyber-Investment and Cyber-Information Exchange Decision Modeling. *Paper presented at the 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*.

Trufanov, A., Kinash, N., Tikhomirov, A., Berestneva, O., & Rossodivita, A. (2017, 2017//). Optimal Information Security Investment in Modern Social Networking. *Paper presented at the Complex Networks VIII, Cham*.

Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security. *Computers & Security,* 24(2), 105-108.

Wang, J., Chaudhury, A., & Rao, H. R. (2008). A value-at-risk approach to information security investment. *Information Systems Research,* 19(1), 106-120.

Wang, Q., Zhu, J., & China., B. (2016). Optimal Information Security Investment Analyses with the Consideration of the Benefits of

Investment and Using Evolutionary Game Theory. *Paper presented at the Information Management (ICIM), 2016 2nd International Conference on.*

Wang, S. L., Chen, J. D., Stirpe, P. A., & Hong, T. P. (2011). Risk-neutral evaluation of information security investment on data centers. *Journal of Intelligent Information Systems*, 36(3), 329-345.

Wang, Z., & Song, H. (2008). Towards an Optimal Information Security Investment Strategy. Paper presented at the Networking, Sensing and Control, 2008. *IEEE International Conference on*.

Wei Liu, Hideyuki Tanaka, & Matsuura., K. (2007). Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms. *Information and Media Technologies*

Wei Sun, Xiangwei Kong, Dequan He, & You, X. (2008). Information Security Investment Game with Penalty Parameter. *Paper presented at the The 3rd Intetnational Conference on Innovative Computing Information.*

Willemson, J. (2010). Extending the Gordon&Loeb model for information security investment. *Paper presented at the International Conference on Availability, Reliability and Security*.

Wu, Y., Feng, G., Wang, N., & Liang, H. (2015). Game of information security investment: Impact of attack types and network vulnerability. *Expert Systems with Applications*, 42(15), 6132-6146.

Zarandi, H. M., & Fred, S. M T (2014). Considering the return on investment ROI The specialized courses of the municipality of Tehran Quarterly Journal of Economics and Management, 8, 1-16.

Zeshuang, L., & jing., L. (2010). Study on the Organization Information Security Investment Decision-Making Based on the Limited Strategy Game Theory Perspective. *Paper presented at the Second*

International Conference on Computational Intelligence and Natural Computing (CINC).

Zvonko, Č., Saša, A., & Tijan., E. (2014). Economic and financial analysis of investments in information security. *Information and Communication Technology*, 26-30.