تاریخ دریافت مقاله: ۹۸/۰۷/۱۱
تاریخ پذیرش مقاله: ۹۹/۰۳/۲۱

شناسایی و اولویت‌بندی ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر

احسان طاهری پور
دانشجوی کارشناسی ارشد گروه مدیریت فنّاوری اطلاعات، واحد اهواز، دانشگاه آزاد اسلامی، اهواز، ایران
پست الکترونیکی: Taheri2010@gmail.com

فریبا نظری*
استادیار گروه علم اطلاعات و دانش شناسی، واحد اهواز، دانشگاه آزاد اسلامی، اهواز، ایران.
پست الکترونیکی: nazari_lib@yahoo.com

چکیده

هدف پژوهش حاضر، شناسایی و اولویت‌بندی ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر با استفاده از فن آنتروپی شانون بود. پژوهش از لحاظ هدف کاربردی، از لحاظ رویکرد پیمایشی و از نوع مطالعات توسعه‌ای بود. در مرحلهٔ شناسایی ریسک، جامعه آماری تحقیق حاضر، مدیران و کارشناسان فنّاوری اطلاعات در شرکت توسعه نیشکر (و شرکت‌های وابسته) بودند که مستقیماً با بحث امنیت داده‌ها و اطلاعات در شرکت مذکور درگیر می‌باشند. تعداد این افراد ۱۰۰ نفر بود. ابزار جمع‌آوری داده‌ها، سه پرسشنامه محقق ساز بود که بنا به اهداف مختلف طراحی و در میان جامعه آماری توزیع شد. تجزیه و تحلیل از طریق نرم‌افزارهای اس.پی.اس.اس، اسمارت پی.ال.اس و اکسل در دستور کار قرار گرفت. در این فرایند، تحلیل‌هایی همچون تحلیل مسیر و آنتروپی شانون به انجام رسید. سرانجام، نتایج تحقیق منجر به شناسایی ۱۰ ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر شد و بر اساس اولویت‌بندی انجام شده، ریسک زیر به ترتیب اولویت‌های اول تا سوم را کسب کردند: تعهد تأمین‌کننده سرویس ابری، قرداد ضعیف شرکت با تأمین‌کننده سرویس ابری، و محرمانگی داده‌های شرکت.

واژه‌های کلیدی: فن آنتروپی شانون، شرکت توسعه نیشکر، ریسک‌پذیرش رایانش ابری

۱- مقدمه

در سال‌های اخیر رایانش ابری در حال تبدیل شدن به یک فنّاوری مهم در حوزهٔ فنّاوری اطلاعات است. متخصصان این حوزه بر این باورند که رایانش ابری، فرآیندها را در حوزهٔ فنّاوری اطلاعات دگرگون خواهد کرد[۱].

در یک تعریف عمومی، مراکز دادهٔ سخت‌افزاری و نرم‌افزارهای تأمین‌کنندهٔ سرویس پردازشی را «رایانش ابری» می‌نامند. رایانش ابری مدل رایانشی بر پایه شبکه‌های رایانه‌ای مانند اینترنت است که الگویی تازه برای عرضه، مصرف و تحویل خدمات رایانشی (شامل

* نویسنده مسئول

زیرســـاخت، نرم‌افزار، بستر، و ســـایر منابع رایانشی) با به‌کارگیری شبکه ارائه می‌کند. «رایانش ابری» از ترکیب دو کلمه رایانش و ابر ایجاد شـــده است. ابر در اینجا استعاره از شبکه یا شبکه‌ای از شبکه‌های وسیع مانند اینترنت است که کاربر معمولی از پشـــت صحنه و آنچه در پی آن اتفاق می‌افتـــد اطلاع دقیقی ندارد (مانند داخل ابر) در نمودارهای شبکه‌های رایانه‌ای نیز از شکل ابر برای نشان دادن شبکه اینترنت اســـتفاده می‌شود. دلیل تشـــبیه اینترنت به ابر در این اســـت که اینترنـــت همچون ابر جزئیـــات فنی‌اش را از دید کاربران پنهان می‌ســـازد و لایه‌ای از انتزاع را بین این جزئیات فنی و کاربران به وجود می‌آورد. رایانش ابری یک روش نوین پردازش اســـت که در آن منابع قابل گسترش و اغلب مجازی شـــده، به‌صورت یک ســـرویس پردازشی و از طریق شـــبکه‌های ارتباطی مانند شـــبکه‌های محلی و اینترنت عرضه می‌شود. محوریت این مدل، سرویس‌دهی به کاربر بر اســـاس تقاضا است، بدون آن که کاربر نیازی به تجهیزات خاصی برای پردازش داشته یا از محل انجام این پردازش آگاه باشـــد. این سرویس را می‌توان به شبکه برق‌رســـانی تشبیه کرد که مشـــترک بدون نیاز به داشتن اطـــلاع از نحوهٔ تولید برق و مکان دقیـــق تولید آن، تنها با اتصـــال از طریق یک درگاه، انرژی لازم برای اســـتفاده از وسایل الکتریکی خود را تامین می‌کند[۲].

منطق رایانش ابری، اشتراک زمانی است؛ به این معنی که منابع مختلف رایانـــه میان چند کاربر با بهره گرفتن از شگردهای چندبرنامه‌ای و چندوظیفه‌ای به اشتراک گذاشته می‌شود. این راهکار اولین بار در دهه ۱۹۵۰ مورد استفاده قـــرار گرفت؛ زمانی‌کـــه به دلیل قیمت بـــالا و اندازه بزرگ رایانه‌های مرکزی، امکان تهیه رایانه برای هر کاربر وجود نداشـــت، در نتیجه با این روش، چنـــد کاربر به یک رایانه مرکزی دسترسی داشتند و به‌طور مشترک از خدمات آن استفاده می‌کردند. بنابراین می‌توان سرویس‌های ابری را تکامل تدریجی راهکارهای به‌اشـــتراک‌گذاری رایانه‌ها در دهه ۱۹۵۰ دانست[۳].

رایانش ابری روش نوینی برای ارائه منابع محاسباتی و افزایش توان محاســـباتی در سازمان‌هاست و با وجود مزایای فراوانی که دارد، به دلیل موانعی از جمله مســـائل امنیتی فراگیر نشـــده و به دغدغه‌ای برای مدیران فنّاوری اطلاعات سازمان‌ها تبدیل شده است[٤].

از ابتدای ظهور فنّاوری رایانش ابری، موضوع ارزیابی و مدیریت ریســـک این فنّاوری تبدیل به چالشی مهم شده اســـت. این امر در سال‌های اخیر به شکلی پیش رفته است که مدیریت ریسک فنّاوری اطلاعات در سازمان‌های ابری با اهداف تجاری این سازمان‌ها همراستا شود [٥].

پژوهشـــگران طی بررسی های دقیق در حوزه رایانش ابری، نشـــان داده اند که در مســـیر پذیرش رایانش ابری، ریسک گوناگونی از جمله موارد زیر وجود دارد: رابط‌های ناامـــن، فنّاوری مشـــترک، ربودن حســـاب یا ســـرویس، خودی‌های مخرب، عدم رعایت مقررات، مالکیت داده، ادغام خدمات و داده‌ها، و نشت اطلاعات [٦].

در شـــرکت توسعه نیشکر ایران نیز، با توجه به وجود شرکت‌های زیرمجموعه و همچنین به‌کارگیری سیستم‌های اطلاعاتی گوناگون، مدتی است که بحث به‌کارگیری رایانش ابری مطرح شـــده اســـت. اما انجام مصاحبه‌های اولیه با مدیران ارشد فنّاوری اطلاعات این شرکت نشان می‌دهد به دلیل وجود ریسک‌های احتمالی در این عرصه و ناشناخته بودن این ریســـک‌ها، آن‌ها هنوز بـــه یک تصمیم قطعی در زمینه پذیرش رایانش ابری دســـت نیافته‌اند. به همین دلیل پژوهـــش حاضر قصد دارد تا با اتخاذ روشـــی نظام‌مند و علمی، به پرسش‌های اصلی زیر پاسخ دهد:

– ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر کدامند؟

– ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر با اســـتفاده از تکنیک آنتروپی شانون چگونه اولویت‌بندی می شوند؟

پژوهش حاضر با رویکرد پیمایشـــی و با اســـتفاده از مطالعات توسعه‌ای ابتدا در مرحلهٔ شناسایی ریسک، جامعه

آماری مدیران و کارشناسان فنّاوری اطلاعات در شرکت توسعه نیشکر (و شرکت‌های وابسته) شرکت کردند علت انتخاب جامعه آماری فوق درگیری مستقیم این افراد با بحث امنیت داده‌ها و اطلاعات در شرکت مذکور بود. تعداد این افراد ۱۰۰ نفر بود. ابزار جمع‌آوری داده‌ها، سه پرسشنامه محقق ساز بود که بنا به اهداف مختلف طراحی و در میان جامعه آماری توزیع شد. بعد از جمع‌آوری پرسشنامه‌ها، جهت تجزیه و تحلیل از نرم‌افزارهای اس.پی.اس.اس، اسمارت پی.ال.اس و اکسل استفاده شد. در این فرایند، تحلیل‌هایی همچون تحلیل مسیر و آنتروپی شانون به انجام رسید. سرانجام، نتایج تحقیق منجر به شناسایی ۱۰ ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر شد و بر اساس اولویت‌بندی انجام شده، ریسک زیر به ترتیب اولویت‌های اول تا سوم را کسب کردند: تعهد تأمین‌کننده سرویس ابری، قرارداد ضعیف شرکت با تأمین‌کننده سرویس ابری، و محرمانگی داده‌های شرکت.

نوآوری پژوهش حاضر شناسایی و اولویت‌بندی ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر و شرکت‌های وابسته استان خوزستان با استفاده از تکنیک آنتروپی شانون بود.

چهارچوب اصلی مقاله بدین صورت است که، بخش دوم شامل مروری بر مبانی نظری و پژوهش‌های پیشین است و به بررسی رایانش ابری و پژوهش‌های پیشین پرداخته است. در بخش سوم روش‌شناسی پژوهش، در بخش چهارم یافته‌ها، در بخش پنجم تفسیر نتایج و در بخش ششم و آخر به نتیجه‌گیری و ارائه پیشنهادها خواهیم پرداخت.

۲-مروری بر مبانی نظری و پژوهش‌های پیشین

۲-۱- رایانش ابری

رایانش ابری، محاسباتی است که توسط گروه بسیاری از کارسازهای از راه دور که با یکدیگر شبکه شده‌اند انجام می‌گیرد که منجر به ذخیره‌سازی متمرکز داده‌ها و دسترسی برخط به سرویس‌ها و منابع کامپیوتری می‌گردد؛ به‌طور ساده‌تر رایانش ابری دستیابی به منابع محاسباتی از طریق اینترنت است و در عمل به جای این‌که شما اطلاعات را بر روی دیسک سخت خود نگه دارید و یا برنامه‌های کاربردی مورد نیازتان را به‌طور مستمر به روزرسانی نمایید، شما از خدمتی بر روی اینترنت به منظور برآوردن نیازهایی مشابه موارد مذکور استفاده می‌نمایید. رایانش ابری یک الگوی محاسباتی است که در آن تعداد بسیار زیادی از سیستم‌ها به‌صورت شبکه‌های خصوصی و یا عمومی به یکدیگر متصل شده‌اند تا زیرساخت پویا و مقیاس‌پذیری را برای برنامه‌های کاربردی، ذخیره داده‌ها و فایل‌ها فراهم آورند. با ظهور این فنّاوری، هزینه محاسبات، میزبانی برنامه‌های کاربردی، ذخیره‌سازی محتوا و تحویل سرویس‌ها به‌طور قابل توجهی کاهش یافته است. ایده محاسبات ابری در اصل بر مبنای «استفاده مجدد از قابلیت‌های فنّاوری» است [۷]. به‌کارگیری رایانش ابری به شش دلیل زیر به سازمان‌ها معرفی شده است:

هزینه: رایانش ابری هزینه‌های خرید نرم‌افزار، سخت‌افزار، نصب و راه‌اندازی مراکز داده یا محفظه‌های کارسازهای وبگاه (برق روزانه برای تأمین برق و خنک کردن آن‌ها) و همچنین نیاز به کارشناسان فنّاوری اطلاعات برای مدیریت زیرساخت‌ها را از بین می‌برد که این موارد باعث سرعت بخشیدن به کارها می‌شود.

سرعت: بیشتر خدمات رایانش ابری به‌صورت سلف سرویس و براساس نیازهای موجود هستند، بنابراین مقادیر وسیعی از منابع رایانش را می‌توان در چند دقیقه فراهم کرد و تنها با چند کلیک موش، کسب و کاری با انعطاف‌پذیری بسیار زیاد ممکن ساخت و از فشار برنامه‌ریزی کاست.

مقیاس جهانی: از مزایای خدمات رایانش ابری، مقیاس انعطاف‌پذیر است. در اصطلاح ابر این بدان معنی است که، مقدار دقیق منابع فنّاوری اطلاعات (مانند قدرت رایانشی بیشتر یا کمتر، ذخیره‌سازی و پهنای باند) درست در مواقع

مورد نیاز و از موقعیت جغرافیایی مناسب عرضه می‌شود.

بهره‌روی: مراکز داده یا وبـگاه نیازمند محفظه‌گذاری بسیاری هستند که شامل نصب و راه‌اندازی سخت‌افزارها، نصب‌کردن نرم‌افزارها و دیگـر کارهای روزمره مدیریت فنّاوری اطلاعات هستند. رایانش ابری نیاز به تعداد زیادی از ایـن وظایف را حذف می‌کنـد، بنابراین تیم‌های فنّاوری اطلاعات می‌توانند زمان زیادی را برای رسـیدن به اهداف مهم کسب‌وکار خود صرف کنند.

عملکـرد: بزرگ‌ترین خدمات رایانش ابری بر روی یک شـبکه جهانی از مراکز دادهٔ ایمن اجرا می‌شود که به‌طور دائم به آخرین نسخهٔ سخت‌افزار رایانشی سریع و کارآمد ارتقـا می‌یابد. این موضوع مزیت‌هـای زیادی را برای یک مرکز دادهٔ واحد در یک شـرکت بـرزگ به همراه دارد که شامل کاهش تأخیر در شبکه برای برنامه‌ها و صرفه‌جویی در مقیاس بزرگ‌تر می‌شود.

قابلیـت اطمینان: رایانـش ابری امکان پیشـتیبانی از داده‌ها، بازیابی اطلاعات و تداوم کسـب و کار را ساده‌تر و ارزان‌تر می‌سازد، زیرا می‌تون داده را در محل‌های دیگر شبکه ارائه دهنده ابر منعکس کرد [۱].

۲-۲- پیشینه پژوهش

در ادامه، به بررسـی برخی از پیشـینه‌های پژوهشی مرتبط با تحقیق حاضر پرداخته شده است:

عظیمـی و عظیمی [۸]، مقاله‌ای را بـا عنوان «ارزیابی ریسک‌های امنیتی و مدیریت آن در رایانش ابری» به نشر رسـاندند. در چکیده این مقاله آمده اسـت: «رایانش ابری اخیراً به‌عنوان یک الگو برای میزبانی و تحویل سرویس‌ها بر روی اینترنت پدیدار گشـته است. این الگو، یک فنّاوری جدید و به عبارتی دیگر، یـک نگرش صحیح در طرح‌های سـرمایه‌گذاری فنّاوری اطلاعات است که علاوه بر کاهش شـدید هزینه‌ها، عملکرد بهتر و قابلیت‌هـای فراوانی را به ارمغان آورده اسـت. مزایای رایانش ابری به سادگی قابل شناسایی اسـت، این روش حافظه بیشتر، انعطاف پذیری بیشـتر و از همه مهم‌تر کاهش هزینه ها را به دنبال خواهد داشـت. تمامی این مزایا برای کمک به رشـد یک تجارت موفـق لازم هسـتند. امتیازات بارز ابرها توجه بسـیاری از سـازمان‌ها را به خود جلب کرده اسـت، اما جنبه‌ای که هنوز باعث عقب‌نشینی بسیاری از سازمان‌ها در برابر این فنّاوری می‌گردد، نحوه امن‌سازی داده‌ها در ابر و اطمینان از امنیت محیط اسـت. مدیریت امنیت مسـائل کنترل‌های امنیتی را نشـان می‌دهد. این کنترل‌ها برای محافظت از هر نوع ضعفی در سیسـتم و کاهش اثر یـک حمله قرار داده شده‌اند.»

یعقوبی و همکاران [۹]، مقاله‌ای را با عنوان «شناسایی و رتبه‌بندی عوامل ریسـک رایانش ابری در سازمان‌های دولتی» به نشر رسـاندند. در چکیده این مقاله آمده است: «با پیشرفت سریع فناوری‌های پردازشی و ذخیره‌سـازی و موفقیـت اینترنـت، منابع رایانشی ارزان‌تر، قوی‌تر، و قابل دسـترس‌تر از قبل شـده‌اند. این روند فناوری، تحقق یک مدل محاسـباتی جدیـد بـه نـام رایـانش ابـری را امکان‌پـذیر سـاخته است. اخیـراً سازمان‌های دولتی شروع به استفاده از معماری، بسترها و برنامه‌های رایانش ابری جهـت تحویل خدمات و برآورده سـاختن نیازهای زیرمجموعه خود کرده‌اند. بـا وجـود مزایـا و فرصت‌های بسـیار فناوری رایانش ابری، ریسک‌های متعددی وجود دارند که سازمان‌های دولتی باید قبل از مهاجرت به سمت محیط ابری آن‌ها را بشناسند. هـدف از انجام این پژوهش، شناسایی و رتبه‌بندی عوامل ریسک رایـانش ابـری در سـازمان‌های دولتی با استفاده از دیدگاه خبرگان فناوری اطلاعات می باشد. ابتدا، با مرور مقالـه‌هـای کلیدی، لیست جامعی از ریسـک‌ها استخراج و در دو دستهٔ محسـوس و غیـرمحسـوس طبقه‌بندی شدند. سپس، از شش نفر از خبرگان در خصوص این ریسک‌ها و تقسـیم‌بنـدی آن‌ها مصاحبه به عمل آمد و ده ریسـک شناسـایی شـد. پـس از آن، ایـن ریسک‌ها بـا نظرسنجی از ۵۲ خبره و با کمک فرایند تحلیل سلسـله مراتبی فازی رتبه‌بندی گردیدنـد. نتایج نشان می‌دهد که خبرگان، ریسک‌های نامحسوس را

به‌عنوان مهم ترین ریسک‌ها در به کارگیری رایانش ابری در سازمان‌های دولتی شناسایی کرده‌اند. در این میان ریسک «محرمانگی داده» رتبهٔ نخست را به دست آورد.»

نوغان و یاراحمدی [۱۰]، مقاله‌ای را با عنوان «شناسایی و تحلیل مهم‌ترین تهدیدها و ریسک‌ها در مدل‌های سرویس رایانش ابری» به نشر رساندند. در چکیده این مقاله آمده است: «دنیای محاسبات به سرعت به سمت توسعه نرم‌افزارهایی پیش می‌رود که به جای اجرا بر روی رایانه‌های منفرد، به‌عنوان یک سرویس در دسترس مصرف‌کنندگان قرار داده می‌شود. از این دیدگاه، رایانش ابری از دید کاربران نهایی ساختاری شبیه به یک توده ابر دارد که به واسطه آن می‌توانند به برنامه‌های کاربردی از هرجایی از دنیا دسترسی داشته باشند. مشتریان و سازمان‌های استفاده کننده از رایانش ابری با قرار دادن داده‌های خود در ابر، کنترل فیزیکی داده‌ها را از دست خواهند داد، بنابراین ریسک و چالش‌های زیادی در خصوص ذخیره‌سازی داده در ابر و استفاده از سرویس‌های ذخیره‌سازی ابری برای مشتریان وجود دارد. انستیتوی ملی استانداردها و فنّاوری‌ها، سه مدل سرویس را برای رایانش ابری تعریف کرده است. این سه مدل سرویس، به مدل SPI مشهور است و شامل نرم‌افزار به‌عنوان سرویس، بُن‌سازه به‌عنوان سرویس و زیرساخت به‌عنوان سرویس است. هر کدام از این سه مدل سرویس، چالش‌ها و مشکلات امنیتی مربوطه به خود را دارند که می بایست مورد بررسی دقیق قرار گیرند.»

کاظم پوریان ممقانی و میراحمدی [۵]، مقاله‌ای را با عنوان «مدیریت ریسک امنیت فنّاوری اطلاعات در رایانش ابری» به نشر رساندند. در چکیده این مقاله آمده است: «رایانش ابری یک فنّاوری محاسبات جدید مبتنی بر اینترنت است که از رایانش شبکه‌ای، رایانش توزیعی، رایانش موازی، رایانش کاربردپذیر، فنّاوری مجازی سازی و دیگر فنّاوری‌های رایانه‌ای منشأ گرفته است و در آن منابع به اشتراک گذاشته شده مانند نرم‌افزار، بستر، فضای ذخیره‌سازی و اطلاعات، بر اساس درخواست مشتریان فراهم می‌شود. این محیط مانند استخری از منابع محاسباتی است و چندین مزیت ویژه از جمله رایانش در مقیاس بالا، مجازی‌سازی، قابلیت گسترس بالا و قابلیت اطمینان بالا دارد. اما با وجود این مزایا، توجه زیادی به نگرانی‌های امنیتی نشده است و این موضوع مانع از توسعه سریع رایانش ابری می‌شود. در این راستا سه دسته از ریسک امنیتی شناسایی شده‌اند: سیاستی–سازمانی، فنی و قانونی. دو مسئله امنیت حریم خصوصی داده‌ها و در دسترس بودن سرویس، از مسائلی هستند که در مورد امنیت رایانش ابری مطرح می‌شوند. به‌کارگیری یک روش امنیتی به تنهایی قادر نیست مسئله امنیتی رایانش ابری را حل کند؛ بلکه باید فنّاوری‌های گسترده و راهبردهای جدیدی را به کار گرفت تا بتوان از کل سیستم رایانش ابری محافظت کرد. همچنین راهبردهای طبقه بندی و مدیریت خاطرات رایانش ابری نیز معرفی و در مورد هر یک بحث شده است.»

یزدانی [۱۱]، مقاله‌ای را با عنوان «پیمایشی بر چارچوب‌های مدیریت ریسک در رایانش ابری» به نشر رساند. در چکیده این مقاله آمده است: «رایانش ابری به‌عنوان یک بُن‌انگارهٔ رایانشی برجسته در عصر حاضر با ارایه خدمات فنّاوری اطلاعات بر مبنای تقاضای کاربر، دسترسی گسترده در سطح شبکه، اشتراک‌گذاری منابع، برخورداری از قابلیت کشسانی و خدمات قابل مقیاس، توانسته است منشأ تحولی عظیم در صنعت فنّاوری اطلاعات محسوب گردد. این مزایا سبب شده تا رایانش ابری تاثیر چشمگیر خود را در امور مختلف سازمان نمایان سازد. با این وجود، استقرار فضای ابر در سازمان با ریسک و ریسک‌های متعدد به‌عنوان دغدغه‌ای جدی و مانعی برای تجهیز و توسعه زیرساخت سازمان به رایانش ابری مواجه شده است. مدیریت این ریسک‌ها مستلزم به‌کارگیری روشی موثر و کارآمد با پوشش لازم در هردو حوزه مشتریان و عرضه کنندگان خدمات رایانشی

خواهد بود. چارچوب‌های مطرح برای مدیریت ریسک که در حال حاضر به منظور مدیریت ریسک فنّاوری اطلاعات در سازمان‌ها به خدمت گرفته شده، با طبیعت پویا و ویژگی‌های خاص فضای ابر چندان سنخیت نداشته است؛ از این رو پژوهشگران به ارایه روش‌ها و چارچوب‌های پیشنهادی خود جهت مدیریت ریسک رایانش ابری پرداخته‌اند.»

چرنیخ و همکاران [۱۲]، مقاله ای را با عنوان «درک عدم اطمینان در رایانش ابری با ریسک‌های محرمانگی، یکپارچگی و دسترسی» به نشر رساندند. این پژوهش با هدف بررسی و معرفی ریسک‌های نهته در فنّاوری رایانش ابری به انجام رسید. نتایج این تحقیق، ریسک‌های اصلی زیر را در حوزه رایانش ابری معرفی نمود: از دست دادن اطلاعات، محرومیت از دسترسی برای مدت زمان طولانی، و نشت اطلاعات.

مادینی و همکاران [٦]، مقاله‌ای را با عنوان «چارچوبی برای عوامل امنیتی مؤثر بر تصمیم پذیرش رایانش ابری در سازمان‌های دولتی عربستان سعودی» به نشر رساندند. این پژوهش، با هدف ارائه مدلی در خصوص ریسک مؤثر بر پذیرش رایانش ابری در سازمان‌های دولتی عربستان به انجام رسید. نتایج این تحقیق نشان داد که سه دسته از عوامل زیر بر تصمیم پذیرش رایانش ابری در سازمان‌های مذکور تأثیرگذار می‌باشند: عوامل ریسک امنیتی در رایانش ابری (شامل: رابط‌های ناامن، فناوری مشترک، ربودن حساب یا سرویس، خودی‌های مخرب، عدم رعایت مقررات، مالکیت داده، ادغام خدمات و داده‌ها، و نشت اطلاعات)؛ عوامل اجتماعی؛ و مزایای امنیتی ادراک شده

۳- روش‌شناسی پژوهش

این تحقیق، از لحاظ هدف کاربردی، از لحاظ رویکرد پیمایشی و از نوع مطالعات توسعه‌ای می‌باشد. همچنین، لازم به ذکر است که این تحقیق در سه فاز کلی زیر به انجام رسیده است:

مرحلهٔ اول: شناسایی ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر.

مرحلهٔ دوم: غربالگری ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر.

مرحلهٔ سوم: اولویت‌بندی ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر با استفاده از تکنیک آنتروپی شانون.

در مرحلهٔ شناسایی ریسک، جامعه آماری تحقیق، مدیران و کارشناسان فنّاوری اطلاعات در شرکت توسعه نیشکر (و شرکت‌های وابسته) بودند که مستقیماً با بحث امنیت داده‌ها و اطلاعات در شرکت مذکور درگیر می‌باشند. تعداد تقریبی این افراد حدود ۱۰۰ نفر می باشد. بر اساس جدول کرجسی و مورگان، برای جامعه ای با این حجم، به ۸۰ نمونه آماری نیاز بود. در این تحقیق، جهت انتخاب افراد نهایی از میان جامعه آماری، سعی شد از روش «قضاوتی» استفاده شود و مطلع ترین افراد در حوزه موضوع پژوهش، در فرایند تحقیق مشارکت داده شوند. همچنین، در مرحله اولویت‌بندی ریسک با استفاده از تکنیک آنتروپی، با توجه به گستردگی زیاد ماتریس‌ها، ۵ نفر از خبرگان به‌صورت تصادفی انتخاب شدند و داده‌های حاصل از پرسشنامه‌های تکمیل شده توسط آن‌ها، مبنای شروع روش آنتروپی قرار گرفت.

در این پژوهش، از سه پرسشنامه محقق ساز زیر بهره برده شد:

پرسشنامه شماره ۱: این پرسشنامه به‌صورت نیمه باز طراحی شد و هدف از آن شناسایی ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر بود.

پرسشنامه شماره ۲: این پرسشنامه به‌صورت بسته طراحی شد و هدف از آن غربالگری ریسک شناسایی شده در مرحله قبل بود.

پرسشنامه شماره ۳: پرسشنامه سوم به‌صورت بسته طراحی شد و هدف از آن اولویت‌بندی ریسک شناسایی و

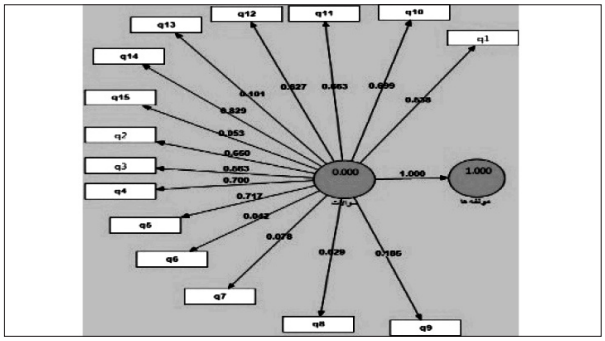
جدول ۱: عوامل اولیه تحقیق

ریسک‌پذیرش رایانش ابری	برچسب
سازوکار ذخیرسازی	Q1
تعهد تأمین‌کننده سرویس ابری	Q2
دسترسی و دسترسی پذیری	Q3
تداوم خدمات فروشنده	Q4
امنیت داده‌ها از بعد نرم‌افزاری	Q5
تخصص ضعیف منابع انسانی	Q6
انتخاب مدل نا مناسب رایانش ابری	Q7
امنیت داده‌ها از بعد نرم‌افزاری	Q8
مکان داده	Q9
قرداد ضعیف شرکت با تأمین‌کننده سرویس ابری	Q10
تخصص تأمین‌کننده سرویس ابری	Q11
محرمانگی داده‌های شرکت	Q12
استراتژی نامناسب شرکت در حوزه رایانش ابری	Q13
فنّاوری های زیرساخت	Q14
جامعیت داده	Q15

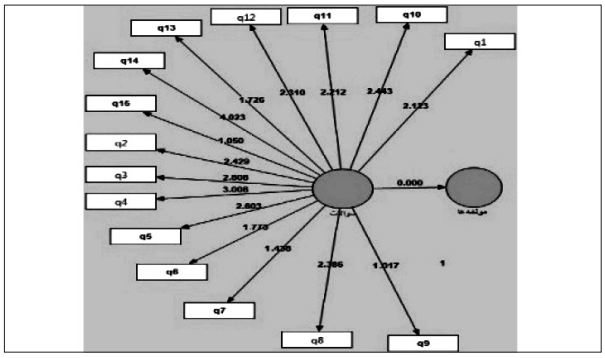
نهایی شده با استفاده از روش آنتروپی بود.

در تحقیق حاضر، به‌منظور بررسی اعتبار (پایایی) پرسشنامه‌ها، از روش «آلفای کرونباخ» استفاده شد و نتیجه این آزمون نشان داد که ضریب آلفای کرونباخ پرسشنامه دوم، ۰/۸۳۱ و ضریب آلفای کرونباخ پرسشنامه سوم، ۰/۸٤۱ می باشد. چون ضریب آلفای کرونباخ هر دو پرسشنامه بالاتر از ۰/۷ به‌دست آمد، از اینرو پایایی هر دو مورد تأیید قرار گرفت.

در مرحلهٔ شناسایی و غربالگری ریسک ناشی از رایانش ابری، از روش‌های تجزیه و تحلیل آماری (توصیفی و استنباطی) استفاده گردید. گفتنی است جهت انجام تجزیه و تحلیل‌های این مرحله، از تحلیل مدل‌سازی معادلات ساختاری و نرم‌افزار smartPLS بهره گرفته شد. همچنین در مرحلهٔ تعیین اولویت‌بندی ریسک ناشی از رایانش ابری نیز، از روش آنتروپی شانون و نرم‌افزار Excel استفاده گردید.



شکل ۱: اندازه‌گیری مدل ساختاری متغیرها در حالت استاندارد



شکل ۲: اندازه‌گیری مدل ساختاری متغیرها در حالت معنی‌داری

۴- یافته‌ها

٤-۱ شناسایی و غربالگری ریسک

بر اساس بررسی پیشینه تحقیق و نظر خواهی از خبرگان (به‌وسیله پرسشنامه شماره ۱)، ۱۵ ریسک‌پذیرش رایانش ابری شناسایی شد که در جدول ۱ قابل مشاهده هستند.

در این تحقیق، جهت غربالگری متغیرها (ریسک)، از مدل‌سازی معادلات ساختاری و نرم‌افزار smartPLS استفاده شد. مهم‌ترین دلیل استفاده از این روش حجم کم نمونه و یا داده‌های غیر نرمال است.

در شکل‌های ۲، خروجی این تحلیل ارائه شده است:

در جدول ۲، به‌طور خلاصه بارهای عاملی در حالت‌های استاندارد و معنی‌داری آورده شده است.

همان‌طور که ملاحظه می‌شود، تعدادی از ریسک‌ها در این مرحله حذف شده و نهایتاً ریسک مندرج در جدول ۳ وارد مرحلهٔ بعد گردیدند.

جدول ۲: نتیجه مرحلهٔ غربالگری ریسک از طریق معادلات ساختاری

ریسک‌پذیرش رایانش ابری	استاندارد	معنی داری	نتیجه
سازوکار ذخیرسازی	۰,۵۳	۲,۱۲	تأیید
تعهد تأمین‌کننده سرویس ابری	۰,۶۵	۲,۴۲	تأیید
دسترسی و دسترسی پذیری	۰,۵۶	۲,۸۰	تأیید
تداوم خدمات فروشنده	۰,۷۰	۳,۰۰	تأیید
امنیت داده‌ها از بعد سخت افزاری	۰,۷۱	۲,۶۰	تأیید
تخصص ضعیف منابع انسانی	۰,۰۴	۱,۷۷	رد
انتخاب مدل نا مناسب رایانش ابری	۰,۰۷	۱,۴۳	رد
امنیت داده‌ها از بعد نرم‌افزاری	۰,۶۲	۲,۳۸	تأیید
مکان داده	۰,۱۸	۱,۰۱	رد
قرارداد ضعیف شرکت با تأمین‌کننده سرویس ابری	۰,۶۹	۲,۴۴	تأیید
تخصص تأمین‌کننده سرویس ابری	۰,۶۶	۲,۲۱	تأیید
محرمانگی داده‌های شرکت	۰,۶۲	۲,۳۱	تأیید
استراتژی نامناسب شرکت در حوزه رایانش ابری	۰,۱۰	۱,۷۲	رد
فنّاوری های زیرساخت	۰,۸۲	۴,۰۲	تأیید
جامعیت داده	۰,۰۵	۱,۰۵	رد

٤-۲-رتبه‌بندی ریســـک نهایی با استفاده از تکنیک آنتروپی

گفتنی اســت که جهت انجام تکنیــک آنتروپی، ۵ مورد از پرسشــنامه‌های تکمیل شده توسط خبرگان، به‌صورت تصادفی انتخاب شــدند و اقدامات زیر بر روی آن‌ها انجام شد

گام اول: ابتدا ماتریس تصمیم تشکیل شد. (جدول ٤)

گام دوم: ماتریس فوق نرمال شد: (جدول ۵)

گام سوم و چهارم: آنتروپی Ej به‌صورت زیر محاسبه گردید:

$$(1)\ Ej= -k\sum_{i=1}^{m} pij \times Ln\ pij\ i = 1,2,\dots,m$$

در ادامه مقدار dj (درجه انحراف) بر اساس فرمول زیر محاسبه شد: (جدول ٦)

جدول ۳: ریسک نهایی

کد	ریسک‌پذیرش رایانش ابری
۱	سازوکار ذخیرسازی
۲	تعهد تأمین‌کننده سرویس ابری
۳	دسترسی و دسترسی پذیری
۴	تداوم خدمات فروشنده
۵	امنیت داده‌ها از بعد سخت افزاری
۶	امنیت داده‌ها از بعد نرم‌افزاری
۷	قرارداد ضعیف شرکت با تأمین‌کننده سرویس ابری
۸	تخصص تأمین‌کننده سرویس ابری
۹	محرمانگی داده‌های شرکت
۱۰	فنّاوری های زیرساخت

جدول ۴: ماتریس اولیه

	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
خبره ۱	۵	۵	۳	۵	۵	۲	۵	۴	۵	۵
خبره ۲	۴	۵	۵	۵	۴	۳	۵	۴	۵	۲
خبره ۳	۵	۵	۵	۵	۵	۴	۵	۵	۳	۵
خبره ۴	۵	۳	۴	۴	۵	۲	۵	۴	۵	۳
خبره ۵	۳	۲	۴	۵	۳	۳	۵	۴	۴	۳

$$(۳)\quad dj=1-Ej$$

گام پنجم: ســـپس مقدار وزن Wj بر اساس فرمول زیر محاسبه شد: (جدول ۷)

$$(۲)\quad Wj=dj/\sum dj$$

بر اســـاس خروجی حاصله، اولویت‌بندی ریســـک بر اساس وزن آن‌ها انجام خواهد شد. به‌طوری که ریسک با وزن بالاتر، رتبه‌های بالاتری کسب خواهند کرد.

۵- تفسیر نتایج

در ایـــن تحقیق، از میان ۸۰ نفـــر خبره‌ای که در تحقیق مشـــارکت داشتند، ۸۳/۷۵ درصد مرد و ۱۶/۲۵ درصد زن بوده‌انـــد. علاوه بر این، از لحـــاظ تحصیلاتی نیز، از میان ۸۰ نفر مذکـــور، ۲۳/۷۵ درصد دارای ســـطح تحصیلاتی

جدول۵: ماتریس نرمال شده

	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
خبره ۱	۰/۲۲۷۲	۰/۲۵	۰/۱۴۲۸	۰/۲۰۸۳	۰/۲۲۷۲	۰/۱۴۲۸	۰/۲	۰/۱۹۰۴	۰/۲۲۷۲	۰/۲۷۷۷
خبره ۲	۰/۱۸۱۸	۰/۲۵	۰/۲۳۸۰	۰/۲۰۸۳	۰/۱۸۱۸	۰/۲۱۴۲	۰/۲	۰/۱۹۰۴	۰/۲۲۷۲	۰/۱۱۱۱
خبره ۳	۰/۲۲۷۲	۰/۲۵	۰/۲۳۸۰	۰/۲۰۸۳	۰/۲۲۷۲	۰/۲۸۵۷	۰/۲	۰/۲۳۸۰	۰/۰۴۱۶	۰/۲۷۷۷
خبره ۴	۰/۲۲۷۲	۰/۱۵	۰/۱۹۰۴	۰/۱۶۶۶	۰/۲۲۷۲	۰/۱۴۲۸	۰/۲	۰/۱۹۰۴	۰/۲۲۷۲	۰/۱۶۶۶
خبره ۵	۰/۰۴۱۶	۰/۱	۰/۱۹۰۴	۰/۲۰۸۳	۰/۰۴۱۶	۰/۲۱۴۲	۰/۲	۰/۱۹۰۴	۰/۱۸۱۸	۰/۱۶۶۶

جدول ۶: محاسبه Ej و dj

	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
Ej	۰/۹۹۶۲۲	۰/۹۹۸۸۰	۰/۹۹۷۰	۰/۹۹۶۲۰	۰/۹۹۶۳۰	۰/۹۹۶۲۰	۰/۹۹۶۰۵	۰/۹۹۶۲۱	۰/۹۹۶۰۸	۰/۹۹۶۱۷
dj	۰/۰۰۳۷	۰/۰۰۱۲	۰/۰۰۳	۰/۰۰۳۷	۰/۰۰۳۷	۰/۰۰۳۸	۰/۰۰۳۹	۰/۰۰۳۷	۰/۰۰۳۹	۰/۰۰۳۸

جدول ۷: خروجی آنتروپی شانون

ردیف	ریسک‌پذیرش رایانش ابری	وزن
۱	سازوکار ذخیرسازی	۰/۰۸۰۶۰۲
۲	تعهد تأمین‌کننده سرویس ابری	۰/۲۸۲۶۷۳
۳	دسترسی و دسترسی پذیری	۰/۰۶۴۸۴۹
۴	تداوم خدمات فروشنده	۰/۰۸۰۸۶۶
۵	امنیت داده‌ها از بعد سخت افزاری	۰/۰۷۹۱۹۷
۶	امنیت داده‌ها از بعد نرم‌افزاری	۰/۰۸۱۸۳۳
۷	قرارداد ضعیف شرکت با تأمین‌کننده سرویس ابری	۰/۰۸۴۲۱
۸	تخصص تأمین‌کننده سرویس ابری	۰/۰۸۰۷۳۵
۹	محرمانگی داده‌های شرکت	۰/۰۸۳۴۹۴
۱۰	فنّاوری های زیرساخت	۰/۰۸۱۵۴۱

کارشناسی، ۶۱/۲۵ درصد دارای سطح تحصیلاتی کارشناسی ارشد، و ۱۵ درصد دارای سطح تحصیلاتی دکتری بوده‌اند. در همین راستا، از میان ۸۰ نفر خبره مشارکت‌کننده در تحقیق، ۳/۷۵ درصد بین ۲۰ تا ۳۰ سال، ۵۲/۵ درصد بین ۳۰ تا ۴۰ سال، ۳۲/۵ درصد بین ۴۰ تا ۵۰ سال و نهایتاً ۱۱/۲۵ درصد نیز بیشتر از ۵۰ سال سن داشته‌اند. از این‌رو، می توان استنباط کرد که بافت غالب خبرگان تحقیق، شامل مردانی در رده سنی ۳۰ تا ۴۰ سال و دارای سطح تحصیلاتی کارشناسی ارشد بوده است.

این تحقیق، بر مبنای پاسخگویی به دو سؤال کلی طراحی و اجرا گردید:

سؤال اول تحقیق به‌صورت زیر طرح گردید: «ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر کدامند؟». جهت پاسخ به این پرسش، سعی شد ابتدا بر اساس بررسی مبانی نظری و پیشینه تحقیق، یک چارچوب نظری کلی در خصوص ریسک‌پذیرش رایانش ابری تعیین شود. ماحصل این کار، شناسایی چندین ریسک در حوزه پذیرش و به‌کارگیری رایانش ابری بود. سپس، سعی شد از طریق توزیع و جمع‌آوری پرسشنامه‌های باز میان خبرگان، ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر به‌صورت بومی شناسایی شوند. نتیجه این کار، دستیابی به ۱۵ ریسک به شرح ذیل بود:

- سازوکار ذخیرسازی
- تعهد تأمین‌کننده سرویس ابری
- دسترسی و دسترسی‌پذیری
- تداوم خدمات فروشنده
- امنیت داده‌ها از بعد نرم‌افزاری
- تخصص ضعیف منابع انسانی
- انتخاب مدل نا مناسب رایانش ابری

- امنیت داده‌ها از بعد سخت‌افزاری
- مکان داده
- قرارداد ضعیف شرکت با تأمین‌کننده سرویس ابری
- تخصص تأمین‌کننده سرویس ابری
- محرمانگی داده‌های شرکت
- راهبرد نامناسب شرکت در حوزه رایانش ابری
- فنّاوری های زیرساخت
- جامعیت داده

گفتنی است که نتایج این تحقیق با نتایج تحقیقات صورت گرفته توسط عظیمی و عظیمی [۸]، یعقوبی و همکاران [۹]، یزدانی (۱۳۹٦)، چرنیخ و همکاران (۲۰۱٦)، مادینی و همکاران [٦] و کومار [۱۳] همخوانی دارد.

سؤال دوم تحقیق نیز به‌صورت زیر طرح گردید: «ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر با استفاده از تکنیک آنتروپی شانون چگونه اولویت‌بندی می شوند؟». هدف از طرح این پرسش، کاربردی تر کردن نتایج تحقیق بود. در این تحقیق، قبل از اولویت‌بندی ریسک، سعی شد ابتدا از طریق به‌کارگیری روش مدل‌سازی معادلات ساختاری، ریسک مورد غربالگری قرار گیرند که ماحصل این کار، حذف ٥ مورد از ریسک بود. در قدم بعد، سعی شد از طریق روش آنتروپی شانون، ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر اولویت‌بندی گردند.

نتیجه این اقدام، اولویت‌بندی ۱۰ ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر بود که در ذیل این ریسک به ترتیب اولویت ارائه شده‌اند:

۱) تعهد تأمین‌کننده سرویس ابری
۲) قرارداد ضعیف شرکت با تأمین‌کننده سرویس ابری
۳) محرمانگی داده‌های شرکت
٤) امنیت داده‌ها از بعد نرم‌افزاری
٥) فنّاوری‌های زیرساخت
٦) تداوم خدمات فروشنده
۷) تخصص تأمین‌کننده سرویس ابری
۸) سازوکار ذخیرسازی
۹) امنیت داده‌ها از بعد سخت‌افزاری
۱۰) دسترسی و دسترسی‌پذیری

۶-نتیجه گیری

همان‌طور که از تفسیر نتایج مشخص است، در شرکت توسعه نیشکر مهم‌ترین ریسک‌پذیرش رایانش ابری، عدم اطمینان در خصوص میزان تعهد تأمین‌کننده سرویس ابری می باشد. چراکه اگر تأمین کننده با تعهد پائین عمل نماید، ریسک و ریسک‌های مختلفی در سیستم کاری شرکت توسعه نیشکر بروز خواهد یافت. علاوه بر این، ریسک قرارداد ضعیف شرکت توسعه نیشکر با تأمین‌کننده سرویس ابری نیز، دیگر ریسک مهم حوزه شناسایی شده است که این امر، هم از لحاظ فنی و هم از لحاظ حقوقی می‌بایست مدنظر شرکت توسعه نیشکر قرار گیرد. در همین راستا، ریسک محرمانگی داده‌های شرکت توسعه نیشکر نیز، جزو سه ریسک اصلی پذیرش رایانش ابری شناخته شده است که این امر، به احتمال درز برخی از اطلاعات و داده‌های محرمانه شرکت در فضای ابری اشاره دارد.

بر اساس نتایج حاصل از این تحقیق، مشخص شد که در شرکت توسعه نیشکر، مانند هر شرکت یا سازمان دیگر، پذیرش و به‌کارگیری فنّاوری‌های رایانس ابری می تواند با ریسکی همراه باشد که این پژوهش موفق شد ۱۰ ریسک اصلی و مهم پذیرش رایانش ابری در شرکت توسعه نیشکر را به‌صورت دقیق شناسایی کرده و اولویت‌بندی نماید. بر اساس نتایج تجزیه و تحلیل داده‌ها، ریسک «تعهد تأمین‌کننده سرویس ابری»، «قرداد ضعیف شرکت با تأمین‌کننده سرویس ابری» و «محرمانگی داده‌های شرکت» جزو مهم‌ترین ریسک‌پذیرش رایانش ابری در شرکت توسعه نیشکر هستند که در این راستا، مدیران ارشد شرکت مذکور (علی‌الخصوص مدیران ارشد فنّاوری اطلاعات)، می‌بایست در جهت کاهش و یا رفع چنین ریسکی برنامه‌ریزی نموده و سعی در خنثی‌سازی اثرات احتمالی آن‌ها بر شرکت توسعه نیشکر داشته باشند.

با توجـــه به نتایج حاصله از تحقیـــق، در جهت کاهش ریســـک‌پذیرش رایانش ابری در شـــرکت توسعه نیشکر، پیشـــنهادهای زیر به مدیران ارشـــد این شرکت قابل ارائه می باشد:

- در شرکت توسعه نیشکر، سعی شود جهت پیاده‌سازی خدمات رایانش ابری تأمین‌کننده‌هایی انتخاب شوند که از تعهد کاری بالایی برخوردار هستند.
- در شرکت توسعه نیشکر، قراردادهای محکم و متقنی با شرکت یا شرکت‌های تأمین‌کننده خدمات رایانش ابری منعقد گردد و همه جوانب در آن در نظر گرفته شود.
- در شرکت توسعه نیشکر، حین طراحی، پیاده‌سازی و به‌کارگیری خدمـــات رایانش ابری، محرمانگی داده‌های شـــرکت به‌صورت ویژه مورد توجه متخصصان قرار داشته باشد.
- در شرکت توسعه نیشـــکر، حین طراحی، پیاده‌سازی و به‌کارگیـــری خدمات رایانش ابـــری، امنیت داده‌های شرکت از بعد نرم‌افزاری مورد توجه ویژه متخصصان قرار داشته باشد.
- در شرکت توسعه نیشکر، فنّاوری های زیرساخت جهت طراحی و پیاده‌سازی سرویس‌های فراهم آید.
- در شرکت توسعه نیشکر، سعی شود جهت پیاده‌سازی خدمات رایانش ابری تأمین‌کننده‌هایی انتخاب شوند که خدمات پس از فروش مداوم و منظمی را ارائه می کنند.
- در شرکت توسعه نیشکر، سعی شود جهت پیاده‌سازی خدمات رایانش ابری تأمین‌کننده‌هایی انتخاب شوند که از تخصص و تجربه کاری بالایی برخوردار هستند.
- در شرکت توسعه نیشکر، در فرایند طراحی و به‌کارگیری خدمات رایانش ابری، به ســـازوکار ذخیرسازی داده‌ها توجه ویژه مبذول گردد و راه‌های افشاء و درز اطلاعات و داده‌های شرکت پیش‌بینی و مسدود کردد.
- در شرکت توسعه نیشکر، حین طراحی، پیاده‌سازی و به‌کارگیری خدمات رایانش ابری، امنیت داده‌های شرکت از بعد سخت‌افزاری مورد توجه ویژه متخصصان قرار داشته باشد.
- در شرکت توسعه نیشکر، سعی شود خدمات رایانش ابری از طریق شبکه قابلیت دسترسی و دسترسی‌پذیری مناسبی داشته باشند.

مراجع

[۱] مقـــدم، رضا، «رایانـــش ابری»، تهران: انتشـــارات مؤسســـه فرهنگی هنری دیباگران تهران.۱۳۹۴.

[۲] اربابـــی، بهرام؛ افتخاری‌فر، مهدی، «بررســـی چالش‌هـــای امنیتی در رایانش ابری»، تهران: انتشارات آثار فکر.۱۳۹۵.

[۳] بنی رســـتم، حمید، «مفاهیم پایه رایانش ابری»، تهران: انتشـــارات اندیشکده متین.۱۳۹۵

[۴] زرگر، ســـیدمحمد؛ شـــهریاری، زهرا، «ارائهٔ مدلی پویا برای پذیرش فنّاوری رایانش ابری با اســـتفاده از تکنیک دیماتل و رویکرد پویایی سیســـتم»، فصلنامه علمی-پژوهشی مدیریت فنّاوری اطلاعات، دوره ۱۰، شماره ۱، صص ۱۱۶-۹۳، ۱۳۹۷.

[۵] کاظم پوریان ممقانی، ســـعید؛ میراحمدی، جعفر، «مدیریت ریســـک امنیت فنّـــاوری اطلاعات در رایانش ابری»، ســـومین کنفرانـــس بین‌المللی پژوهش در مهندســـی، علوم و فنّاوری، باتومی - کشور گرجستان، موسسه سرآمد همایش کارین.۱۳۹۵.

[6] Madini, O. Alassafi., Abdulrahman, Alharthi., Robert, J. Walters., Gary, B. Wills, "A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies", Telematics and Informatics, 34 , pp. 996–1010.2017.

[۷] حســـینی، فاطمـــه، «شبیه‌ســـازی محیـــط رایانش ابـــری»، تهران: انتشـــارات انس.۱۳۹۶.

[۸] عظیمی، عاطفه؛ عظیمی، ریحانه، «ارزیابی ریســـک‌های امنیتی و مدیریت آن در رایانش ابری»، اولین همایش ملی پژوهش‌های مهندسی رایانه، تهران، مرکز توسعه پایدار علم و صنعت فرزین.۱۳۹۳.

[۹] یعقوبی، نورمحمد؛ جعفری، حمیدرضا؛ شکوهی، جواد. «شناسایی و رتبه‌بندی عوامل ریســـک رایانش ابری در ســـازمان‌های دولتی»، پژوهشـــنامه پردازش و مدیریت اطلاعات، دوره ۳۰، شماره ۳، صص ۷۸۴-۷۵۹، ۱۳۹۴.

[۱۰] نوغـــان، نیما؛ یاراحمدی، علی، «شناســـایی و تحلیـــل مهم‌ترین تهدیدها و ریسک‌ها در مدل‌های سرویس رایانش ابری»، کنفرانس بین المللی پژوهش‌های نویـــن در علوم مهندســـی، تهران، موسســـه مدیریت دانش شـــباک، دانشـــگاه تهران.۱۳۹۵.

[۱۱] یزدانی، عطاءاله، «پیمایشـــی بر چارچوب‌های مدیریت ریسک در رایانش ابری»، چهارمین کنفرانس ملی فنّاوری اطلاعات، کامپیوتر و مخابرات، مشـــهد، دانشگاه تربت حیدریه.۱۳۹۶.

[12] Tchernykh, Andrei., Uwe, Schwiegelsohn., El-ghazali, Talbi., Mikhail, Babenko,"Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability", Journal of Computational Science, Available online 22 November 2016, In Press, Corrected Proof.2016.

[13] Kumar, Guddu (9 September 2019). "A Review on Data Protection of Cloud Computing Security, Benefits, Risks and Suggestions" (PDF). United International Journal for Research & Technology. 1 (2): 26. Retrieved 9 September 2019.