مدلی پویا جهت ارزیابی امنیت سیستم‌های اطلاعاتی با استفاده از رویکرد پویایی‌شناسی سیستم‌ها

محسن شفیعی نیک‌آبادی*
دانشگاه سمنان، سمنان، ایران
shafiei@semnan.ac.ir

امیر حکاکی
دانشگاه سمنان، سمنان، ایران
a.hakaki@semnan.ac.ir

سارا غلامشاهی
دانشگاه سمنان، سمنان، ایران
saragholamshahi@yahoo.com

تاریخ دریافت: ۱۳۹۸/۰۴/۱۲
تاریخ اصلاحات: ۱۳۹۹/۰۴/۰۵
تاریخ پذیرش: ۱۳۹۹/۰۶/۱۰

چکیده

در دهه‌های اخیر امنیت اطلاعات از اهمیت بالایی برخوردار است. این درحالی است که بسیاری از پروژه‌های ارتقاء امنیت اطلاعات در سازمان‌ها به دلیل عدم اطلاع دقیق از ریسک‌ها و عوامل مؤثر با شکست مواجه می‌شوند. پژوهش حاضر جهت شناسایی شاخص‌های تأثیرگذار بر امنیت سیستم‌های اطلاعاتی داده‌های لازم پس از مطالعات کتابخانه‌ای و مطالعات میدانی به صورت مصاحبه باز با ۱۲ نفر از خبرگان که با روش نمونه‌گیری قضاوتی و هدفمند انتخاب شده‌اند جمع‌آوری شده است. نمودار روابط علی پژوهش پس از شناسایی ابعاد و شاخص‌های ریسک با استفاده از نظرات خبرگان ترسیم شده و در نهایت مطابق با مدل‌سازی پویایی‌های سیستم، مدل پویای پژوهش با استفاده از نرم‌افزار ونسیم (Vensim) طراحی شده است. مدل‌سازی پویایی‌های سیستم درک بهتری از رفتار سیستم ایجاد می‌نماید و بوسیله آن می‌توان ساختارها و سیاست‌های جدیدی را تدوین نمود. برای اعتبارسنجی مدل از آزمون شرایط حدی استفاده شده و نتایج نشان از تأیید اعتبار مدل ارائه شده دارد. برای انجام شبیه‌سازی داده‌های لازم با استفاده از داده‌های شرکت مهندسین مشاور افق گردآوری شده است. نتایج شبیه‌سازی در مدت ۱۲ ماه نشان می‌دهد در بین ریسک‌های شناسایی‌شده بیشترین اهمیت مربوط به ریسک فنی می‌باشد؛ ریسک داده، انسان و فیزیکی در رتبه‌های بعدی قرار می‌گیرند؛ کم اهمیت‌ترین ریسک مربوط به محیط می‌باشد. در نهایت، چهار سناریو استفاده از نرم‌افزارهای امنیتی، تعیین سطوح دسترسی کاربران، استفاده از برق اضطراری، استفاده از نظارت تصویری و آموزش کارکنان جهت بهبود رفتار سیستم معرفی شده است.

واژگان کلیدی

امنیت سیستم‌های اطلاعاتی؛ پویایی‌های سیستم؛ مدل‌سازی؛ شبیه‌سازی؛ ونسیم.

۱- مقدمه

امروزه اطلاعات با ارزش‌ترین دارایی هر سازمان محسوب می‌شود و باید آن را کالایی اساسی در هر سازمان دانست، همانند الکتریسیته که بدون آن بسیاری از کسب و کارها نمی‌توانند به سادگی جریان داشته باشند [۱۴]. توسعه سیستم‌های اطلاعاتی همچون شمشیر دولبه‌ای است که از یک سو منافع بسیاری را برای بشر به ارمغان آورده و از سوی دیگر به سبب مقوله امنیت اطلاعات، زیان‌های جبران‌ناپذیری را به‌دنبال داشته است [۱، ۱۵]. در سال‌های اخیر امنیت اطلاعات به‌عنوان یکی از موضوع‌های کلیدی صنعت IT مطرح می‌شود [۱۶]. امنیت اطلاعات به‌عنوان حفاظت از اطلاعات سیستم‌ها و خدمات در برابر بلایا، اشتباهات و دستکاری، به منظور به حداقل رساندن احتمال بروز و تأثیر مشکلات امنیتی تعریف شده است [۱۷]. به‌عبارت دیگر، امنیت به مجموعه‌ای از تدابیر، روش‌ها و ابزارهایی گفته می‌شود که برای جلوگیری از دسترسی و تغییرات غیرمجاز در نظام‌های رایانه‌ای و ارتباطی به‌کار می‌رود [۱۸]. براساس بررسی مؤسسه امنیت کامپیوتری در مورد جرایم رایانه‌ای و امنیتی ۷۳۸ سازمان در سال ۲۰۱۰، زیان سالانه ناشی از حوادث امنیتی سیستم‌های اطلاعاتی، صد و نود میلیون دلار گزارش شده است [۱۵]. همچنین به گزارش این مؤسسه، در آمریکا درصد سازمان‌هایی که بخشی (۳ درصد یا بیشتر) از بودجه IT خود را به موضوع امنیت اطلاعات اختصاص داده‌اند، از ۴۰ درصد در سال ۲۰۰۶ به ۵۵ درصد در سال ۲۰۰۸ افزایش داشته است که نشان‌دهنده اهمیت ویژه امنیت اطلاعات در سازمان‌های امروزی می‌باشد. اگرچه فناوری‌های مورد استفاده برای امنیت اطلاعات طی ده سال گذشته پیشرفت زیادی داشته است، اما هنوز هم سطح امنیتی کامپیوترها و شبکه‌ها، بهبود قابل توجهی پیدا نکرده است [۱۷] و سازمان‌ها در برخی از موارد برای پیاده‌سازی سیاست‌های امنیت اطلاعات با شکست مواجه می‌شوند. در سال‌های اخیر مدل‌های متعددی برای امنیت اطلاعات ارائه شده‌اند که معمولاً این مدل‌ها بر مبنای

* نویسنده مسئول

محاسبات فنی از طریق کنترل دسترسی‌ها بنا می‌شوند [۱۹]. به منظور حل مسأله امنیت سیستم‌های اطلاعاتی تاکنون تحقیقات زیادی صورت گرفته است. اما عمده این تحقیقات به علت نگاه تک بعدی و غیرسیستمی به مسأله امنیت اطلاعات، نتوانسته‌اند به‌طور کامل و همه جانبه به آن بپردازند. نکته حائز اهمیت این است که این مطالعات اغلب یک نگرش ایستا از امنیت اطلاعات را اتخاذ می‌نماید. درحالیکه سیستم امنیت اطلاعات در واقعیت یک سیستم پیچیده و پویا است که شامل بسیاری از متغیرهای وابسته به هم بوده [۲۰] و نادیده گرفتن پویایی‌های سیستم‌های امنیت اطلاعات منجر به ساده‌سازی بیش از حد این سیستم‌ها می‌شود و مدل‌هایی که بر این مبنا به‌دست می‌آیند، اغلب واقع‌گرایانه نبوده و تفاسیر نادرستی را ارائه می‌دهند. این موارد نشان‌دهنده نیاز به یک مدل پویای سیستمی برای ارزیابی امنیت اطلاعات می‌باشد چرا که ارزیابی به‌عنوان یکی از نگرش‌های علمی و یکی از مهم‌ترین فعالیت‌های مدیریت در راستای کمی‌نمودن روابط متغیرها و معیارهای مهم به‌عنوان اساس برنامه‌ریزی، تحلیل، کنترل فعالیت‌ها و تصمیمات مدیریت به شمار می‌رود. هدف رویکرد مدل‌سازی پویایی‌های سیستم که بر پایه قواعد ریاضی تئوری کنترل و دینامیک غیرخطی بنا شد و به موجب آن می‌توان فعل و انفعالات پویا و غیرخطی در سیستم‌های دنیای واقعی را درک و تجزیه و تحلیل کرد؛ ارائه سیاست‌های جدید به منظور بهبود رفتار سیستم [۲۱]، کاهش ریسک و پیش‌بینی صحیح رفتار سیستم در مقابل راهبردهای مختلف می‌باشد [۲۲]. همچنین سادگی ایجاد تغییر در مدل و قابلیت انجام آنالیز حساسیت، این روش را از دیگر روش‌های تحلیل مدل‌سازی جذاب‌تر نموده است [۲]. در نتیجه، پژوهش حاضر با هدف "ارائه مدلی پویا از مؤلفه‌های اثرگذار بر ارزیابی امنیت سیستم‌های اطلاعاتی" انجام شده است. بر همین مبنا این تحقیق دارای سه مرحله اساسی می‌باشد:

مرحله اول: شناسایی مؤلفه‌های اثرگذار بر ارزیابی امنیت سیستم‌های اطلاعاتی براساس مبنای نظری پژوهش و نظر خبرگان.

مرحله دوم: ترسیم نمودار علی و معلولی مؤلفه‌های شناسایی‌شده با استفاده از نظرات خبرگان.

مرحله سوم: ترسیم مدل پویای پژوهش با هدف تحلیل وضعیت سیستم و پیش‌بینی سیاست‌های آینده با استفاده از نرم‌افزار ونسیم.

۲- پیشینه پژوهش

۲-۱- ابعاد و شاخص‌های امنیت سیستم‌های اطلاعاتی

مفهوم و اهمیت ایمنی و امنیت از همان آغاز زندگی بشر وجود داشت، بشر همیشه برای بقا و ادامه زندگی سعی نموده است که جهت حفاظت از خود و دارایی‌هایش، آگاهی‌ها و دانش خود را نسبت به محیط و خطرات اطراف خود افزایش دهد [۳]. یک سیستم اطلاعاتی برای تولید، جمع‌آوری، سازماندهی (پردازش)، ذخیره، بازیابی و اشاعه اطلاعات در یک سازمان طراحی شده است [۴] و منظور از امنیت اطلاعات، حفاظت از سیستم‌های اطلاعاتی در مقابل دسترسی غیرمجاز یا تغییر اطلاعات است [۵]. از اوایل دهه ۱۹۹۰ مطالعات در ارتباط با مسأله امنیت اطلاعات و جنبه‌های مختلف آن همچون سوء استفاده‌های داخلی، حملات خارجی، سیاست‌های مورد استفاده، جرم و جنایت‌های کامپیوتری و امنیت رمز عبور آغاز شده است [۲۰] به‌طور خاص مفهوم امنیت اطلاعات شامل محرمانه‌بودن، یکپارچگی، در دسترس‌بودن و صحت بدون در نظر گرفتن فرم اطلاعات اعم از الکترونیکی، چاپ، و یا اشکال دیگر می‌باشد [۶، ۲۳] و پنج جزء امنیت سیستم‌های اطلاعاتی شامل مبدأ، روش، کانال، گیرنده و نتیجه می‌شود که منظور از مبدأ در واقع منبع تهدید، روش به معنای نحوه تأثیر تهدید، کانال به معنای تأثیر تهدید، گیرنده به معنای هدف اطلاعات و نتیجه آسیب و اثر تهدید می‌باشد. به‌طور کلی امنیت در سیستم‌های اطلاعاتی مطابق با جدول ۱ دارای هفت لایه است به‌طوریکه لایه‌های پایینی از لایه‌های بالایی پشتیبانی کرده و لایه‌های بالایی متکی بر لایه‌های پایینی می‌باشند.

جدول ۱- مدل هفت لایه امنیت سیستم‌های اطلاعات [۲۳]

امنیت داده و اطلاعات	لایه ۷
امنیت سیستم نرم‌افزاری	لایه ۶
امنیت شبکه ارتباطات	لایه ۵
امنیت سیستم سخت‌افزاری	لایه ۴
امنیت فیزیکی	لایه ۳
مدیریت امنیت	لایه ۲
امنیت قانونی	لایه ۱

با توجه به مدل هفت لایه امنیت سیستم‌های اطلاعاتی (جدول ۱)، تهدیدهای در سیستم‌های اطلاعاتی می‌توانند توسط عوامل عمدی یا غیرعمدی ایجاد گردند؛ این تهدیدها شامل تهدیدهای انسانی (حملات به شبکه، گسترش کدهای مخرب، بمب‌های الکترونیکی، دسترسی‌های غیرمجاز و اشتباهات غیر عمدی مانند بی‌دقتی در نگهداری و بهره‌برداری خطا) تهدیدهای سیستم (خطا در سیستم، شبکه و سرویس‌ها مانند خطا در سخت‌افزار یا نرم‌افزار و یا اختلال در پایگاه داده)، تهدیدهای محیطی (آتش‌سوزی غیرعمدی، ارتعاشات، تداخلات الکترومغناطیسی، گرد و غبار، سیل، زلزله، رعد و برق) و تهدیدهای روانی مدیریت (نقض در راهبرد، قوانین برنامه‌نویسی، آگاهی کارکنان و ساختار سازمان) می‌شود [۱۰، ۲۳]. عوامل انسانی ضعیف‌ترین و سست‌ترین عنصر آسیب‌پذیر در مدل‌های امنیت سیستم‌های اطلاعاتی می‌باشند [۲۴]. مطالعات پژوهش‌های پیشین نشان می‌دهد تهدیدهای داخلی سیستم‌های اطلاعاتی اغلب بسیار مهم‌تر از تهدیدهای خارجی بوده و بیشتر از جانب افرادی می‌باشد که یا دانش قبلی از سیستم داشته‌اند و یا دارای شریک جرمی در داخل شرکت بوده‌اند؛ ریسک‌های انسانی شناسایی‌شده عبارتند از: ۱) ریسک عمدی انسانی، رویدادها و اتفاقاتی که چه از داخل سازمان و چه از خارج از آن منشاء انسانی و عمدی دارند؛ برخی از ریسک‌های عمدی انسان شامل سوء استفاده از اطلاعات، سرقت و کلاهبرداری، جرایم کامپیوتری، نرم‌افزار مخرب، دسترسی غیرمجاز، کدهای مخرب، ویروس، بمب‌ها، اخلال‌گری

الکترونیکی، آتش‌سوزی عمدی و قطع برق عمدی می‌شود [۲۵]. ریسک غیرعمدی انسانی (اتفاقات با منشاء انسانی غیرعمدی) شامل بی‌دقتی، سهل‌انگاری، توانایی کم پرسنل، کار زیاد، بی‌مسئولیتی، عدم آگاهی و به‌روزرسانی اطلاعات، عدم بکارگیری صحیح تجهیزات، عدم نصب صحیح نرم‌افزارها و برنامه‌های کاربردی، آلوده‌شدن غیرعمدی شبکه به ویروس و دسترسی ناخواسته به اطلاعات محرمانه می‌شود [۲۶]. همچنین، هدف از امنیت اطلاعات در بخش فیزیکی حفاظت از اطلاعات در مقابل دسترسی افراد غیرمجاز به تجهیزات فیزیکی ثبت و مدیریت اطلاعات و جلوگیری از سرقت و دستبرد یا تخریب آنها می‌باشد؛ تجهیزاتی که قابل دیدن، لمس‌کردن، ربودن و انتقال فیزیکی را دارند، می‌توانند امنیت فیزیکی را مورد تهدید قرار دهند [۷]. ریسک فیزیکی شامل خطر آسیب سخت‌افزاری، آسیب‌های زیرساخت، آسیب به تجهیزات فناوری اطلاعات و زیرساخت شبکه، سرقت، تخریب و دستکاری می‌شود [۲۷]. تهدیدها و ریسک فنی سیستم‌های اطلاعاتی شامل تهدیدهای نرم‌افزاری و سخت‌افزاری می‌باشد؛ از جمله مشکلات سخت‌افزاری می‌توان به آسیب‌پذیری شبکه، توپولوژی نامناسب شبکه اطلاعاتی، عدم هماهنگی در تجهیزات مورد استفاده، مشکلات مربوط به تجهیزات ارتباطات شبکه و قطع و وصل برق اشاره کرد و از مشکلات نرم‌افزاری می‌توان به آسیب پایگاه داده، نفوذ به دیوار محافظ اطلاعات معروف به دیوار آتش، بدافزارها (ویروس‌ها، تروجان‌ها،کرم‌ها)، انتشار غیرمجاز یا تخریب داده‌ها، جاسوسی بوسیله ابزارهای دیجیتالی، عدم هماهنگی میان نرم‌افزار و سخت‌افزار اشاره نمود [۲۸، ۲۹]. تهدیدها و ریسک‌های محیطی جز عواملی هستند که هر سیستمی را تهدید می‌نمایند برخی از عوامل محیطی شامل آتش‌سوزی غیرعمدی، تداخل الکترومغناطیسی، گرد و غبار، ارتعاش، بلایای طبیعی، قطع طولانی‌مدت برق، مواد شیمیایی، نشت مایعات و استهلاک تجهیزات و لوازم می‌باشد [۲۵]. رشد فزاینده حجم داده‌های ذخیره شده در سازمان‌ها از یک سو و کلیدی‌ترشدن نقش آن‌ها در تصمیم‌گیری‌ها از سوی دیگر، سبب شده است تا ضروری حفاظت داده‌ها برای مدیران توجیه‌پذیر و از اهمیت بالایی برخوردار باشد. از جمله تهدیدها و ریسک‌های مربوط به داده‌ها و اطلاعات می‌توان به محیط انتقال داده‌ها، حذف یا تغییر داده و به اشتراک‌گذاری داده‌ها اشاره نمود [۲۵].

در پژوهشی با هدف شناسایی و سنجش تأثیر عواملی که سیستم‌های اطلاعاتی سازمان‌ها را با خطر سرقت، نابودی و یا تغییر اطلاعات مواجه می‌سازند با مرور پژوهش‌های پیشین و روش‌های پرکاربرد مدلی ارائه شده است که در آن امنیت نیروی انسانی، امنیت فیزیکی و امنیت اطلاعات سه اصل اساسی می‌باشند؛ نتایج حاصل از پژوهش نشان می‌دهد مؤلفه عدم آگاهی کاربران بیشترین تهدید و پس از آن امنیت نیروی انسانی دومین تهدید برای امنیت اطلاعات سیستم‌های رایانه‌ای می‌باشد [۷].

با هدف ارائه چارچوبی برای عوامل انسانی مرتبط در امنیت سیستم‌های اطلاعاتی مشخص گردید عوامل انسانی ضعیف‌ترین و سست‌ترین عنصر آسیب‌پذیر در مدل‌های امنیت سیستم‌های اطلاعاتی می‌باشند؛ همچنین، نتایج نشان می‌دهد حمایت مدیریت عالی، آموزش امنیتی، فرهنگ امنیتی، مهارت امنیتی، تقویت خط و مشی امنیتی، تجربیات و خودباوری افراد از فاکتورهای مؤثر بر اثربخشی امنیت سیستم‌های اطلاعاتی می‌باشد [۱۰].

به منظور ارائه مدلی مبتنی بر وقوع و پیشگیری برای کاهش تهدیدات امنیت اطلاعات در سازمان‌ها مشخص گردید که نقض امنیت اطلاعات و حریم خصوصی مسأله مهمی در سازمان‌ها می‌باشد؛ این مطالعه نشان می‌دهد کارمندان عمداً یا ناخواسته بخش قابل توجهی از تهدیدات مرتبط با اطلاعات سازمان را به خود اختصاص می‌دهند. در نهایت نتایج حاصل از تحلیل اطلاعات نشان می‌دهد که هنجارهای ذهنی، کنترل رفتارهای ادراک و نگرش کارمندان بر نیات آنها در مواجهه با سیستم‌های اطلاعاتی تأثیر می‌گذارد [۳۰].

بطور کلی مطالعات نشان می‌دهد در دنیای امنیت اطلاعات که سیستم‌ها بطور مداوم با تهدیدها و ریسک‌های اطلاعاتی روبرو هستند شناسایی این تهدیدها می‌توان کمک شایانی برای مدیران سازمان باشد. در پژوهشی با هدف مطالعه تهدیدهای سیستم‌های اطلاعاتی مشخص گردید در گام نخست مهم‌ترین چیزی که در این تهدید برای سیستم اطلاعاتی بایستی مورد سنجش قرار گیرد انگیزه یا هدف تهدیدکننده می‌باشد و در گام دوم بایستی روشی که ممکن است مورد استفاده قرار گیرد، بررسی شود. به همین منظور شناسایی ابعاد تهدیدات و ریسک‌های امنیت اطلاعات در سازمان از اهمیت ویژه‌ای برخوردار است [۳۱].

۲-۲- مدل‌سازی پویایی‌های سیستم

مدل‌سازی پویایی‌های سیستم توسط پروفسور جی فارستر استاد دانشگاه MIT در دهه ۱۹۵۰ توسعه یافت [۳۲،۲۲] تا به‌عنوان روشی برای بررسی رفتار پویای سیستم‌ها با تأکید بر روابط میان عناصر تشکیل‌دهنده سیستم مورد استفاده قرار گیرد [۳۳]. رویکرد پویایی‌های سیستم درک بهتری از رفتار سیستم ایجاد می‌نماید تا به‌وسیله آن بتوان ساختارها و سیاست‌های جدیدی را به منظور بهبود رفتار سیستم تدوین نمود [۳۴]. لازمه مدل‌سازی پویایی‌های سیستم، برخورداری از تفکر سیستمی است که عبارت است از مجموعه‌ای از فعالیت‌های زنجیره‌وار که از فعالیت‌های مفهومی شروع شده و به فعالیت‌های محاسباتی و فنی ختم می‌شود [۹]. در اولین گام از مدل‌سازی پویایی‌های سیستم برای درک بهتر ساختار سیستم‌ها وجود یک زبان مدل‌سازی ضروری است، در پویایی‌های سیستم به این زبان نمودارهای علّی می‌گویند که یکی از مهم‌ترین ابزارها در ترسیم ساختار بازخوردی سیستم می‌باشد. این نمودارها شامل متغیرهایی است که توسط فلش‌هایی نحوه تأثیر هریک بر دیگری نشان داده می‌شود [۱۸]. علامت + فلش نشان‌دهنده قطبیت مثبت و یا همراستایی میان متغیرها بوده و علامت - فلش نشان‌دهنده قطبیت منفی میان متغیرها می‌باشد [۳۵]. روابط علّی در جریان‌های رفت و برگشتی تشکیل حلقه‌های علّی می‌دهند [۹]. در یک حلقه‌ی علّی اگر افزایش یا کاهش یک متغیر پس از طی‌شدن حلقه منجر به افزایش یا کاهش مجدد آن شود، آن حلقه‌ی علّی مثبت بوده و در غیر این

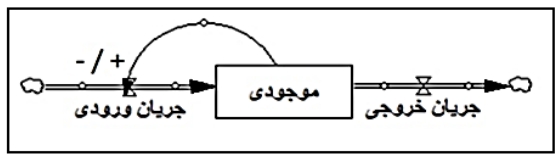
صورت حلقه منفی می‌باشد [۳۶]. مدل‌سازی پویایی‌های سیستم از جنس دانش عددی و مهندسی می‌باشد؛ از محدودیت‌های نمودارهای علّی عدم نمایش ساختار موجودی و جریان‌های سیستم و روابط ریاضی میان متغیرها می‌باشد. برای رفع این مشکل از دیاگرام موجودی- جریان استفاده می‌شود. جدول ۲ نمادهای مورد استفاده در این مدل‌سازی را نشان می‌دهد.

جدول ۲- نمادهای مورد استفاده در نمودارهای موجودی- جریان

نام	نماد
موجودی	
جریان	
چشمه/چاه	
اتصال دهنده‌ها	
پارامتر	

منبع جدول: [۳۰]

مطابق با جدول ۲، موجودی‌ها بیانگر تجمع بوده و با مستطیل نشان داده می‌شوند، جریان ورودی و خروجی یک متغیر موجودی، به‌وسیله فلش نشان داده می‌شود [۳۷]. متغیرهای موجودی تنها از طریق متغیرهای جریان تغییر می‌کنند [۲۲]. برای ترسیم مدل جریان- موجودی از نرم‌افزار ونسیم استفاده می‌شود. این نرم‌افزار محصول شرکت Ventana System است و نوعی ابزار مدل‌سازی می‌باشد که قادر به مجسم‌نمودن، پردازش، شبیه‌سازی، تحلیل و بهینه‌سازی مدل‌های مربوط به سیستم‌های پویا می‌باشد و به گونه‌ای ساده و انعطاف‌پذیر امکان شبیه‌سازی مدل‌های داری حلقه و متغیرهای جریان و موجودی را فراهم می‌نماید. در این نرم‌افزار پس از تعریف روابط و ساخته‌شدن مدل می‌توان رفتار سیستم را در طول زمان شبیه‌سازی خواهد بود. شکل ۱ متغیرهای موجودی، جریان ورودی و خروجی را در نرم‌افزار ونسیم نشان می‌دهد.



شکل ۱- ترکیب متغیرهای موجودی، جریان ورودی و جریان خروجی [۳۷].

در ریاضیات مدل‌سازی پویایی‌های سیستم از متغیر موجودی (حالت) به‌عنوان انتگرال و از متغیر جریان به‌عنوان نرخ یا مشق یاد می‌شود. رابطه ۱ مقدار موجودی را پس از گذشت زمان t نشان می‌دهد [۳۷].

$$Stock(t) = \int_{t_0}^{t} [Inflow(s) - Outflow(s)ds + Stock(t_0)$$ **رابطه ۱)**

مطابق با رابطه ۱، Stock(t0) نشان‌دهنده موجودی اولیه متغیر حالت می‌باشد. با توجه به رابطه ۱ می‌توان نتیجه گرفت میزان تغییرات متغیر موجودی در واحد زمان مطابق با رابطه ۲ برابر است با خالص تغییر متغیر موجودی یا اختلاف نرخ جریان ورودی با جریان خروجی است [۳۶].

$$d(stock)/dt = Inflow(t) - Outflow(t)$$ **رابطه ۲)**

۳- روش‌شناسی پژوهش

پژوهش حاضر از منظر هدف کاربردی، از منظر متغیر کمی بوده و از دید ماهیت و روش در دسته پژوهش‌های توصیفی- تحلیلی قرار می‌گیرد. شکل ۲ مراحل انجام این پژوهش را به نشان می‌دهد.

شکل ۲- مراحل انجام پژوهش

۳-۱- مفهوم‌سازی سیستم

مفهوم‌سازی سیستم، شامل تعیین مرز مدل با توجه به اهداف تعیین شده می‌باشد [۱۱]. پس از انجام مطالعات کتابخانه‌ای و شناسایی اولیه ابعاد و شاخص‌های امنیت سیستم‌های اطلاعاتی در قالب ریسک‌های موجود، از مطالعات میدانی به منظور استخراج، جرح و تعدیل متغیرهای نهایی استفاده شده است. جهت جمع‌آوری داده‌ها از ابزار مصاحبه باز استفاده شده است. جامعه آماری پژوهش در این مرحله شامل مجموعه‌ای از خبرگان و کارشناسان می‌باشد که یکی از دو شرط ذیل را برخوردار باشند؛ ۱) دارابودن حداقل مدرک تحصیلی کارشناسی‌ارشد مرتبط با حوزه‌های امنیت اطلاعات، نرم‌افزار و شبکه ۲) برخورداری از حداقل ده سال سابقه کاری مرتبط با حوزه‌های امنیت سیستم‌های اطلاعاتی. از میان واجدین شرایط، با ۱۲ نفر نمونه‌های آماری که به صورت قضاوتی- هدفمند انتخاب شده‌اند مصاحبه باز انجام شده است. جدول ۳ وضعیت جمعیت‌شناختی نمونه آماری را در این مرحله نشان می‌دهد.

جدول ۳- وضعیت جمعیت‌شناختی نمونه آماری در مرحله مفهوم‌سازی

مشخصات توصیفی		فراوانی	درصد توزیع
تحصیلات	کارشناسی‌ارشد	۷	۵۸/۴
	دکتری	۵	۴۱/۶
سابقه کار	۱۰ – ۱۵ سال	۱۰	۸۳/۴
	بالاتر از ۱۵ سال	۲	۱۶/۶

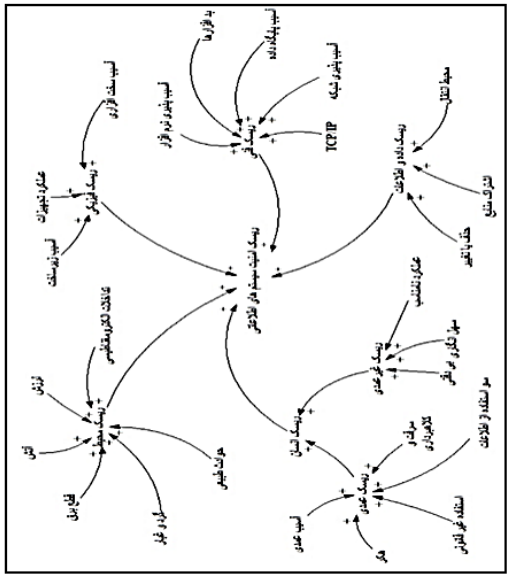
در نهایت، ابعاد و شاخص‌های نهایی مدل براساس مبانی نظری پژوهش و نظرات خبرگان با توجه به هدف پژوهش تعیین می‌گردد (جدول ۴).

جدول ۴- ابعاد و شاخص‌های امنیت سیستم‌های اطلاعاتی

ردیف	ابعاد	شاخص‌ها	منبع
۱	ریسک محیط	آتش‌سوزی	[۲۳]،[۲۵]
		لرزش	[۲۳]،[۲۵]
		استهلاک سیستم ناشی از گرد و غبار	[۲۳]،[۲۵]
		تداخل الکترومغناطیسی	[۲۳]،[۲۵]
		حوادث طبیعی	[۲۳]،[۲۵]
		قطع برق	[۲۳]،[۲۵]
۲	ریسک فنی	آسیب‌پذیری نرم‌افزاری	[۲۵]،[۲۸]
		آسیب‌پذیری سخت‌افزاری	[۲۵]
		خطا در جریان TCP/IP	[۲۵]،[۲۸]
		بدافزارها	[۲۷]،[۲۸]
		آسیب‌پذیری شبکه	[۲۸]
		آسیب پایگاه داده	[۲۸]
۳	ریسک فیزیکی	آسیب سخت‌افزاری سیستم	[۲۷]
		آسیب زیرساخت	[۲۷]
		عملکرد تجهیزات	[۲۷]
۴	ریسک انسان	ریسک عمدی	[۲۶]
		هکر وکراکر	[۲۵]
		جرایم کامپیوتری	[۲۵]
		سو استفاده از اطلاعات	[۲۵]
		سرقت و کلاه‌برداری	[۲۷]
		استفاده غیر قانونی	[۲۶]
		ریسک غیرعمدی	[۲۶]
		بی‌دقتی	[۲۶]
		سهل انگاری	[۲۶]
		توانایی پرسنل	[۲۶]
۵	ریسک داده	حذف یا تغییر داده	[۲۷]
		محیط انتقال داده	[۲۵]
		اشتراک‌گذاری منابع	[۲۵]

۴- صورت‌بندی مدل

در این مرحله روابط علّی و حلقه‌های بازخوردی میان متغیرهای شناسایی‌شده در مرحله مفهوم‌سازی سیستم ترسیم می‌گردد. نمودارهای علّی، ابزاری مهم برای نشان دادن روابط میان متغیرها [۶، ۱۲] و ساختار یک سیستم [۱۳] به منظور مدل‌سازی رفتارهای پویای سیستم می‌باشد [۱۱]. در این مرحله روابط علّی براساس مطالعات کتابخانه‌ای و میدانی پژوهش ترسیم شده و با استفاده از نظرات خبرگان، پس رفع نقص‌ها و ارائه پیشنهادها به تأئید رسیده است. شکل ۳ نمودار علّت و معلولی شاخص‌های امنیت سیستم‌های اطلاعاتی در پنج بعد ریسک محیط، ریسک فنی سیستم، ریسک فیزیکی سیستم، ریسک انسان و ریسک داده نمایش می‌دهد.



شکل ۳- نمودار علّت و معلولی شاخص‌های امنیت سیستم‌های اطلاعاتی

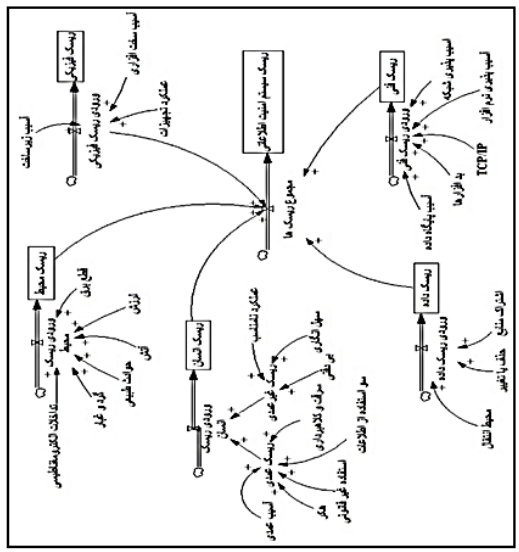
برای هرچه نزدیک‌ترشدن به روابط ریاضی حاکم میان متغیرها با تعریف متغیرهای سطح و نرخ دیاگرام موجودی- جریان ترسیم می‌گردد تا درک بهتری از مدل حاصل شود. جدول ۵ لیست متغیرهای مدل پویای امنیت سیستم‌های اطلاعاتی و نوع آن‌ها شناسایی‌شده نشان می‌دهد.

جدول ۵- لیست متغیرهای مدل پویای امنیت سیستم‌های اطلاعاتی

ردیف	نام متغیر	نوع
۱	ریسک امنیت سیستم‌های اطلاعاتی	موجودی
۲	مجموع ریسک‌ها	جریان
۳	ریسک محیط	موجودی
۴	ورودی ریسک محیط	جریان
۵	آتش	ثابت
۶	لرزش	ثابت
۷	استهلاک سیستم ناشی از گرد و غبار	ثابت
۸	تداخلات الکترومغناطیسی	ثابت
۹	حوادث طبیعی	ثابت
۱۰	قطع برق	ثابت
۱۱	ریسک فیزیکی	موجودی
۱۲	ورودی ریسک فیزیکی	جریان
۱۳	آسیب سخت‌افزاری سیستم	ثابت
۱۴	آسیب زیرساخت	ثابت
۱۵	عملکرد تجهیزات	ثابت
۱۶	ریسک فنی	موجودی
۱۷	ورودی ریسک فنی	جریان
۱۸	آسیب‌پذیری نرم‌افزاری	ثابت
۱۹	آسیب‌پذیری سخت‌افزاری	ثابت
۲۰	خطا در جریان TCP/IP	ثابت
۲۱	بدافزارها	ثابت
۲۲	آسیب‌پذیری شبکه	ثابت

ردیف	نام متغیر	نوع
۲۳	آسیب پایگاه داده	ثابت
۲۴	ریسک انسان	موجودی
۲۵	ورودی ریسک انسان	جریان
۲۶	ریسک عمدی	کمکی
۲۷	هکر وکراکر	ثابت
۲۸	جرایم کامپیوتری	ثابت
۲۹	سو استفاده از اطلاعات	ثابت
۳۰	سرقت و کلاه‌برداری	ثابت
۳۱	استفاده غیر قانونی	ثابت
۳۲	ریسک غیر عمدی	کمکی
۳۳	بی‌دقتی	ثابت
۳۴	سهل‌انگاری	ثابت
۳۵	توانایی پرسنل	ثابت
۳۶	ریسک داده و اطلاعات	موجودی
۳۷	ورودی ریسک داده و اطلاعات	جریان
۳۸	حذف یا تغییر داده	ثابت
۳۹	محیط انتقال داده	ثابت
۴۰	اشتراک‌گذاری منابع	ثابت

مطابق با جدول ۵، هر یک از ابعاد امنیت سیستم‌های اطلاعاتی یک متغیر موجودی و یک متغیر جریان به خود اختصاص می‌دهند. بر همین اساس با استفاده از نمودار علّی (شکل ۳)، متغیرهای مدل پویای پژوهش (جدول ۵) و نظرات خبرگان و کارشناسان مدل پویای پژوهش در نرم‌افزار ونسیم مطابق با شکل ۴ ترسیم می‌گردد.



شکل ۴- مدل پویای ریسک امنیت سیستم‌های اطلاعاتی

در مرحله بعد نوبت به تعیین روابط ریاضی مدل ترسیم شده در شکل ۴ می‌رسد. بر همین اساس رابطه ۳ فرمول ریاضی متغیرهای موجودی را در هر یک از ابعاد نشان می‌دهد.

رابطه ۳) ۰ + جریان ورودی در هر یک از ابعاد = متغیر موجودی هر یک از ابعاد

منظور از صفر در رابطه ۳ مقدار اولیه متغیر موجودی هر یک از ابعاد در شروع شبیه‌سازی می‌باشد. متغیر جریان در هر یک از ابعاد حاصل مجموع متغیرهای ثابتی است که هر یک به صورت مجزا رویدادهای بوقوع پیوسته و تهدیدکننده امنیت سیستم‌های اطلاعاتی را نشان می‌دهند. رابطه ۴ فرمول ریاضی متغیرهای جریان را در هر یک از ابعاد نشان می‌دهد.

رابطه ۴) ... + متغیر ثابت ۲ + متغیر ثابت ۱ = متغیر جریان هر یک از ابعاد

شایان ذکر است به منظور درک بهتر از ریسک انسان دو متغیر کمکی ریسک عمدی و ریسک غیرعمدی جهت تفکیک متغیرهای ثابت در این بعد در نظر گرفته شده‌اند. در نهایت، برای بدست‌آوردن مجموع رویدادهای تهدیدکننده امنیت سیستم‌های اطلاعاتی در بازه زمانی موردنظر یک متغیر موجودی برای امنیت سیستم‌های اطلاعاتی در نظر گرفته می‌شود که ورودی آن متغیر جریانی به نام مجموع ریسک‌ها می‌باشد. رابطه ۵ فرمول ریاضی متغیر جریان مجموع ریسک‌ها را به‌عنوان ورودی متغیر موجودی ریسک امنیت سیستم‌های اطلاعاتی نشان می‌دهد.

رابطه ۵) جمع همه ریسک‌ها (فنی+فیزیکی+انسانی+داده+محیط) = ریسک کل

۴-۱- اعتبارسنجی مدل و شبیه‌سازی مدل

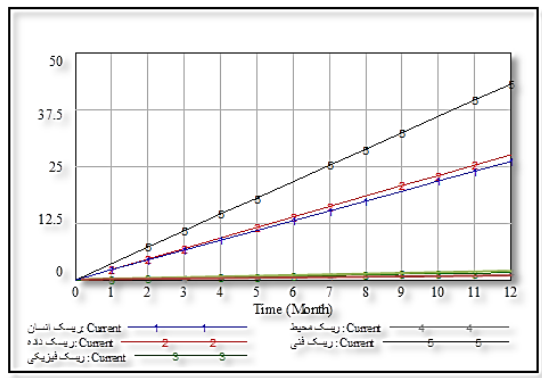
پس از طراحی اولیه، مدل بایستی تعیین اعتبار گردد [۳۸]. آزمون‌های متعددی در زمینه اعتبارسنجی مدل‌های پویا مطرح شده است که به دو دسته آزمون‌های ساختاری و رفتاری تقسیم می‌شوند [۳۹]. اعتبار ساختاری به معنای ایجاد روابطی در مدل است به گونه‌ای رسا و کافی، نشان‌دهنده روابط جهان واقعی باشند و اعتبار رفتاری بدین معناست که رفتار مدل به اندازه کافی نشان‌دهنده رفتار پدیده در جهان واقعی باشد. متداول‌ترین تست‌ها شامل مقایسه با نقاط مرجع، پایداری تحت شرایط حدی و آنالیز حساسیت می‌باشد. آزمون استفاده‌شده در این پژوهش با توجه به هدف تحقیق که مدل‌سازی امنیت سیستم‌های اطلاعاتی است از نوع آزمون شرایط حدی می‌باشد. شرایطی که ممکن است هرگز در جهان واقعی مشاهده نگردد. این آزمون نشان می‌دهد که آیا سیستم رفتار قابل انتظاری از خود نشان می‌دهد یا خیر. بنابراین مدل در دو شرایط حدی مورد بررسی قرار می‌گیرد؛ ۱) کلیه عوامل مؤثر بر امنیت اطلاعات در بهترین حالت خود قرار می‌گیرد. یعنی در واقع مقدار ریسک‌های فیزیکی، ریسک فنی، ریسک انسان، ریسک داده و ریسک محیط برابر کمترین مقدار یعنی صفر در نظر گرفته می‌شود. ۲) کلیه عوامل مؤثر بر امنیت اطلاعات در بدترین حالت خود قرار می‌گیرد. یعنی در واقع مقدار ریسک‌های فیزیکی، ریسک فنی، ریسک انسان، ریسک داده و ریسک محیط برابر بیشترین مقدار در نظر گرفته می‌شود. با آزمودن در شرایط حدی مشخص می‌شود که در مورد اول مقدار ریسک امنیت اطلاعاتی به صفر و در مورد دوم ریسک امنیت اطلاعاتی به بیشترین حد خود می‌رسد.

بر همین اساس پایایی و اعتبار مدل مورد تأیید قرار گرفته و نتایج حاصل از مدل مورد نظر قابل استناد می‌باشد.

جهت شبیه‌سازی به منظور استفاده کاربردی از مدل‌سازی پویایی‌های سیستم داده‌های مورد نیاز پژوهش از داده‌های موجود در شرکت مهندسین مشاور افق گردآوری شده است. هچنین، پژوهش حاضر بجای اندازه‌گیری شاخص‌های ارزیابی در یک زمان ایستا به شبیه‌سازی آنها در یک دوره زمانی ۱۲ ماهه پرداخته شده است تا رفتار بلندمدت سیستم جهت اطمینان از پایداری یا ناپایداری آن با ارائه سناریوهای بهبود و بررسی کیفیت جواب‌ها مورد بررسی قرار گیرد.

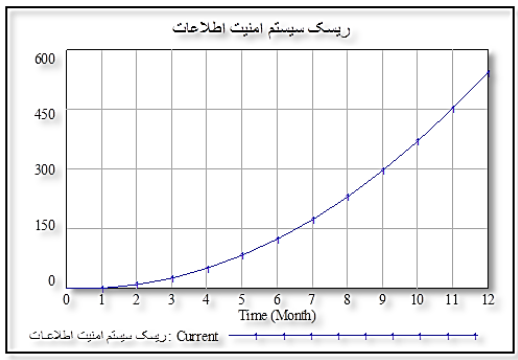
۴-۲- تحلیل سیاست‌ها

در بیشتر موارد هدف از مدل‌سازی پویایی‌های سیستم تحلیل اثرگذاری سیاست‌های مختلف بر رفتار سیستم و عوامل تشکیل‌دهنده آن می‌باشد تا با استفاده از آن بتوان سیاست‌های مناسبی را با هدف بهبود رفتار سیستم شناسایی نمود [۱۱]. به همین منظور مدل در یک بازه زمانی ۱۲ ماهه با استفاده از داده‌های تحلیل‌شده مربوط به شرکت مهندسین مشاور افق اجرا می‌شود. در این مرحله فرض بر این است که سیاست‌های فعلی تغییری نکنند تا بتوان با استفاده از مشاهده رفتار سیستم طی ۱۲ ماه آینده اقدامات لازم را جهت بهبود رفتار سیستم پیش‌بینی نمود. براساس نتایج بدست‌آمده پس از اجرای مدل ریسک در هر پنج بعد محیطی، فنی، فیزیکی، انسانی و داده مطابق با شکل ۵ افزایش می‌یابد.



شکل ۵- مقایسه ریسک‌ها در هر یک از ابعاد مورد مطالعه حاصل از اجرای مدل

مطابق با شکل ۵، مقایسه شیب هر یک از ابعاد و تعداد خطاها در پایان دوره میزان اهمیت هر کدام را تعیین می‌نماید. بر همین اساس درصورتیکه از اقدامات بازدارنده استفاده نشود ریسک فنی در مقایسه با دیگر ریسک‌ها در پایان دوره افزایش قابل ملاحظه‌ای دارد؛ و ریسک‌های داده، انسان در رتبه‌های بعدی قرار دارند. ریسک فیزیکی و محیطی که نمودارهای آنها تقریباً بر هم منطبق می‌باشد در پایین‌ترین رتبه قرار دارند. ریسک امنیت اطلاعات که حاصل از برآیند تمامی ریسک‌ها می‌باشد مطابق با شکل ۶ بیشترین افزایش را به خود اختصاص می‌دهد.



شکل ۶- نمودار ریسک سیستم امنیت اطلاعاتی پس از اجرای مدل

۴-۲-۱- سناریو اول: استفاده از نرم‌افزارهای امنیتی

از اقداماتی که برای کاهش ریسک فنی می‌توان پیشنهاد نمود استفاده از نرم‌افزارهای امنیتی مانند آنتی‌ویروس شبکه و فایروال‌ها می‌باشد. در این سناریو از آنتی‌ویروس برای ارتقاء سطح امنیت سیستم استفاده شود. از آنجایی‌که آسیب‌پذیری نرم‌افزار بر ریسک فنی سیستم تأثیر مثبت دارد، بنابراین با استفاده از آنتی‌ویروس‌ها، آسیب‌پذیری نرم‌افزار کاهش و متعاقباً ریسک فنی کاهش می‌یابد که با توجه به پویابودن مدل، در نهایت ریسک سیستم امنیت اطلاعاتی کاهش می‌یابد.

۴-۲-۲- سناریو دوم: تعیین سطوح دسترسی

از راه‌حل‌هایی که جهت کاهش ریسک انسان استفاده می‌گردد استفاده از تعیین سطوح دسترسی می‌باشد. در صورتیکه برای کاربران مختلف دسترسی متفاوت و متناسب تعریف گردد خطای عمدی و غیرعمدی انسان کاهش قابل توجه‌ای خواهد داشت و نتیجتاً ریسک انسان کاهش می‌یابد.

۴-۲-۳- سناریو سوم: استفاده از سیستم برق اضطراری

از عواملی که منجر به افزایش ریسک محیط قطع عمدی یا غیرعمدی برق سیستم‌ها می‌باشد. یک عامل بازدارنده جهت کاهش این ریسک استفاده از سیستم‌های برق اضطراری با حداقل دو ساعت توان برق‌دهی می‌باشد. در صورت استفاده از سیستم برق اضطراری به هنگام قطع برق سیستم‌ها به هر علتی، تا دو ساعت برق‌رسانی به سیستم انجام می‌گردد.

۴-۲-۴- سناریو چهارم: استفاده از سیستم نظارت تصویری

خطر سرقت، تخریب، آسیب‌های زیرساخت، آسیب به تجهیزات فناوری اطلاعات و زیرساخت شبکه از عواملی افزایش ریسک فیزیکی و ریسک کل سیستم اطلاعاتی می‌باشند. استفاده از دوربین های مدار بسته یک بازدارنده قوی در مقابل این تهدیدات می‌باشند. در صورت استفاده از این سیستم‌ها در صورت بروز هر کدام از این خطرات شبکه هشدارهای لازم را به کاربران و مدیران ارسال نموده تا بتوان از بروز این تهدیدات جلوگیری نمود.

۴-۲-۵- سناریو پنجم: آموزش دوره‌ای کارکنان

ریسک انسان به دو صورت عمدی و غیر عمدی طبقه‌بندی می‌شود. ریسک غیرعمدی یکی از عواملی است که توسط استفاده‌کنندگان از سیستم‌ها بوجود می‌آید. ریسک‌های غیرعمدی مانند سهل‌انگاری، بی‌دقتی یا عدم توانایی پرسنل می‌باشد. برگذاری دوره‌های آموزشی به صورت ماهانه، فصلی، سالانه و غیره جهت کاهش این ریسک بسیار مؤثر می‌باشد.

۵- نتیجه‌گیری و پیشنهادات

پژوهش حاضر با هدف ارائه مدلی پویا از مؤلفه‌های اثرگذار بر ارزیابی امنیت سیستم‌های اطلاعاتی با رویکرد پویایی‌های سیستم و با استفاده نرم‌افزار ونسیم انجام شده است تا با استفاده از آن بتوان وضعیت موجود سیستم را ارزیابی نمود و سیاست‌های بهینه آینده را پیش‌بینی نمود. جهت اعتبارسنجی مدل پژوهش از آزمون شرایط حدی استفاده شده است که نشان می‌دهد پایایی و اعتبار مدل مورد تأیید می‌باشد. امنیت سیستم‌های اطلاعاتی نقش کلیدی در موفقیت یک سازمان دارد. در این راستا استقرار یک سیستم ارزیابی امنیت در بهبود مستمر امنیت سیستم‌های اطلاعاتی امری ضروری می‌باشد. بسیاری از محققان بر این عقیده‌اند که بهبود مستمر در سازمان تنها با تکیه بر ارزیابی می‌باشد. با توجه به اهمیت اطلاعات در جوامع امروزی، اهمیت ارزیابی امنیت آن نیز چندین برابر شده است. به همین منظور در این پژوهش ابتدا کلیه شاخص‌های تأثیرگذار در امنیت اطلاعات با استفاده از ادبیات پژوهش، نظرات خبرگان و کارشناسان شناسایی می‌شوند. در بسیاری از تحقیقات انجام شده همچون [۱۷]، [۱۸] و تحقیقات دیگر تنها به یک یا دو بعد از امنیت سیستم‌های اطلاعاتی توجه شده است و همه ابعاد آن در نظر گرفته نشده است. همچنین، بر خلاف دید قالب در مورد امنیت سیستم‌های اطلاعاتی، امنیت اطلاعات فقط اتخاذ روش‌های رمزنگاری، نصب دیواره آتش و رمز عبور نمی‌باشد چراکه این موارد تنها بعد فنی امنیت اطلاعات تشکیل می‌دهند. اگرچه ممکن است سازمان‌ها حداکثر کنترل‌های فنی امنیتی را در سازمان پیاده کرده باشند، یک کاربر ناآگاه می‌تواند برای امنیت سیستم‌های اطلاعاتی بسیار خطرناک باشد. نتیجتاً در این پژوهش علاوه بر بعد فنی، ریسک‌های انسانی نیز مدنظر قرار گرفته شده است. به‌طور کلی امنیت سیستم‌های اطلاعاتی یک فرایند مهندسی سیستم پیچیده است. به همین دلیل پژوهش حاضر به غیر از مسائل فنی و انسانی، فاکتورهای مربوط به ریسک محیط، ریسک فیزیکی و ریسک داده را نیز مدنظر قرار داده است. در اولین گام از پژوهش پس از مطالعه کتب، مقالات داخلی و خارجی و ادبیات پژوهش هر یک از ابعاد امنیت سیستم‌های اطلاعاتی و شاخص‌های آنها شناسایی شده است. بر همین اساس تهدیدات سیستم‌های اطلاعاتی می‌تواند توسط عوامل آگاهانه یا اتفاقی ایجاد گردد [۲۳]. در یک دسته‌بندی کلی تهدیدات سیستم‌های اطلاعاتی عبارتند از ۱) ریسک انسان: شامل حملات به شبکه، گسترش کدهای مخرب، بمب الکترونیکی، دسترسی‌های غیرمجاز، بی‌دقتی در نگهداری و بهره‌برداری خطا. ۲) ریسک فیزیکی شامل آسیب سخت‌افزاری، آسیب‌های زیرساخت، آسیب به تجهیزات فناوری اطلاعات و زیرساخت شبکه، سرقت، تخریب و دستکاری. ۳) ریسک فنی شامل ارتباطات شبکه، قطع و وصل برق، آسیب پایگاه‌داده، نفوذ به دیوار آتش، بدافزارها. ۴) ریسک محیط همچون آتش، تداخلات الکترومغناطیسی، گردوغبار، ارتعاشات، سیل، زلزله، رعد و برق. ۵) ریسک‌داده شامل محیط انتقال، حذف یا تغییر داده و به اشتراک‌گذاری داده‌ها.

پژوهش حاضر کلیه ابعاد شناسایی‌شده را در طراحی مدل پویای پژوهش در نظر گرفته است. به همین منظور در گام نخست مؤلفه‌های اثرگذار بر امنیت اطلاعات را در ابعاد مختلف براساس پیشینه پژوهش و نظرات خبرگان شناسایی و سپس دیاگرام علی عوامل مورد مطالعه با توجه به نظرات کارشناسان و خبرگان ترسیم شده است. در نهایت مدل پویای ارزیابی امنیت سیستم‌های اطلاعاتی در نرم‌افزار ونسیم ترسیم شده است. با ترسیم نمودار علی نهایی پژوهش، بررسی نمودار مشخص نمود که ریسک محیط، ریسک عمدی و ریسک فنی بیشترین تعداد عوامل را در قلمرو مطالعاتی مورد نظر شناسایی کرده‌اند. بر همین اساس می‌توان بیان نمود یکی از ریسک‌های مرتبط با سیستم‌های اطلاعاتی ریسک محیط با شش عامل اثرگذار دارایی بیشترین تعداد احتمالات مخرب می‌باشد و ریسک عمدی و فنی با ۵ عامل در رتبه‌های بعدی قرار می‌گیرند. به منظور کاهش ریسک عمدی در سازمان‌ها براساس نظر خبرگان بررسی و کنترل کارکنان و دستگاه‌های سازمان پیشنهاد می‌شود. همچنین، برقراری سیستم نظرات مستقیم مانند دوربین‌های نظارتی و طبقه‌بندی اطلاعات می‌تواند کمک شایانی در کاهش ریسک عمدی داشته باشد. این در حالی است که ریسک محیطی اساساً به دو دسته تقسیم می‌شود. عواملی که از کنترل پرسنل خارج است و عوامل کنترل‌پذیر. در مورد عوامل خارج از کنترل پرسنل مانند قطعی برق یا زلزله گاهاً راهکارهایی برای سازمان‌ها وجود دارد؛ از جمله استفاده از اتاق‌های امن در مقابل زلزله یا آتش‌سوزی و سیستم‌های برق پشتیبان پیشنهاد می‌شود. یکی از نکاتی که بسیاری از کارشناسان بر آن تأکید فراوان داشته‌اند این است که بخش بسیاری از ریسک فنی در سیستم‌های اطلاعاتی مربوط به استفاده از دستگاه‌های قدیمی و یا فرسوده می‌باشد. در حقیقت فقدان سیاست‌های نوگرایی و بروزرسانی سخت‌افزار سیستم‌های اطلاعاتی یکی از ضعف‌های اساسی در سازمان‌ها محسوب می‌شود. همچنین، یکی دیگر از مشکلات مرتبط با ریسک فنی سیستم‌های اطلاعاتی مسائل مرتبط با تحریم‌های ایران می‌باشد. این تحریم‌ها باعث می‌شود واردات سخت‌افزار مورد نیاز با مشکلات فراوانی روبرو باشد. بر همین اساس به مدیران شرکت‌ها پیشنهاد می‌شود تا سیاست‌ها مربوط به سیستم‌های اطلاعاتی سازمان را بطور مداوم رصد نموده و در صورت نیاز در قالب برنامه‌های کوتاه‌مدت و میان‌مدت سعی کنند در جهت تحقق اهداف بلند مدت سخت‌افزار مورد

نیاز سازمان را تهیه نمایند. نکته قابل توجه این است که در تحقیقاتی مانند [۱۵]، [۱۹] و سایر تحقیقات تنها بعد ایستا ارزیابی امنیت اطلاعات در نظر گرفته شده است و به بعد پویا آن توجهی نشده است. برای این منظور، این پژوهش از مدل‌سازی پویایی‌های سیستم به منظور ارزیابی امنیت سیستم‌های اطلاعاتی استفاده نموده است. پس از اجرای مدل پویای پژوهش نتایج حاصل از شبیه‌سازی داده‌های گردآوری‌شده از شرکت مهندسین مشاور افق طی یک دوره ۱۲ ماهه نشان می‌دهد در بین ریسک‌های شناسایی‌شده کم اهمیت‌ترین ریسک، ریسک محیط می‌باشد که با گذشت زمان تغییر چندانی نمی‌کند و می‌توان از آن صرف‌نظر کرد. بررسی نتایج مربوط به ریسک محیط تبیین می‌کند از آنجایی‌که کنترل این عوامل اثرگذار بر این ریسک از دست مدیران و خارج می‌باشد و سازمان‌ها تنها بایستی سعی کنند با سیاست‌های بنیادین اقدامات احتیاطی را پیش‌بینی نمایند و مسائل امنیتی مذکور را رعایت کنند. همچنین پر اهمیت‌ترین ریسک که غیرقابل چشم‌پوشی است مربوط به ریسک فنی می‌باشد؛ ریسک داده، ریسک انسانی و فیزیکی در رتبه‌های بعدی از منظر اهمیت قرار می‌گیرند. همانطور که پیش‌تر مهم‌ترین ریسک اثرگذار بر امنیت سیستم‌های اطلاعاتی ریسک فنی می‌باشد که می‌تواند آمار خطرات و حملات به سیستم‌های اطلاعاتی را بطور مؤثری افزایش دهد. یکی از مهم‌ترین راهکارهای مربوط به حوزه فنی سیستم‌های اطلاعاتی استفاده از سرورهای مرکزی، نرم‌افزارهای امنیتی و فضاهای ذخیره‌سازی مستقل می‌باشد. همچنین، با توجه به نظرات خبرگان، کارشناسان و مدیران امنیت سیستم‌های اطلاعاتی چهار سناریو به منظور بهبود رفتار سیستم مورد مطالعه در نظر گرفته شده است که عبارتند از: استفاده از نرم‌افزارهای امنیتی، تعیین سطوح دسترسی برای کاربران، استفاده از برق اضطراری، استفاده از نظارت تصویری (دوربین مداربسته) و آموزش دوره‌ای کارکنان.

با توجه به نتایج بدست‌آمده و نظرات خبرگان و کارشناسان به مدیران سازمان‌ها و مسئولین مرتبط با بخش‌های امنیت اطلاعات توصیه می‌شود به دو بعد ریسک محیطی و انسانی توجه ویژه‌ای داشته باشند. چراکه در اکثر سازمان‌ها معمولاً به‌طور طبیعی به ریسک فنی توجه می‌شود. به منظور کاهش ریسک محیطی اقداماتی همچون ارتقای امنیتی فضای مورد استفاده برای نگهداری سرورها و هاردهای ذخیره‌ساز پیشنهاد می‌شود. در این شرایط چنانچه به هر دلیلی اطلاعات سیستم از بین رود می‌توان از هاردهای پشتیبان استفاده نمود. همچنین، کلاس‌های آموزشی کارکنان سازمان اهمیت ویژه‌ای در کاهش ریسک‌های اطلاعاتی داشته باشد. افزایش آگاهی و ارتقای اطلاعات کارکنان باعث می‌شود تا ایشان از اقدامات پر مخاطره و هیجانی در رابطه با اطلاعات خودداری نموده و ریسک امنیتی اطلاعات افزایش می‌یابد. همچنین تعریف سطح دسترسی برای کارکنان سبب می‌شود تا تمامی افراد مشغول در سازمان بطور نامحدود به اطلاعات دسترسی نداشته باشند و هر یک از افراد تنها به اطلاعات مورد نیاز دسترسی داشته باشند. این راهبرد باعث می‌شود تا امنیت اطلاعات بصورت سطح‌بندی شده حفظ شود. مطالعات مسائل و مشکلات امنیتی سازمان‌ها نشان می‌دهد یکی از مهم‌ترین دلایل از دست‌دادن اطلاعات مشکلات مربوط به افت ولتاژ و یا تغییر میزان ولتاژ مورد استفاده دستگاه‌ها مانند هاردها و سرورهای سازمان می‌باشد. به همین منظور استفاده از سیستم‌های محافظتی برقی و برق اضطراری می‌تواند نقش مهمی در کنترل خطرهای حاصل از تغییرات ولتاژ و یا در هنگام قطعی برق ایفا نماید.

با توجه به محدودیت‌ها موجود در انجام این پژوهش و مصاحبه‌های صورت گرفته با خبرگان برای انجام پژوهش‌های آتی می‌توان پیشنهاد نمود تا مدل پژوهش در قلمروهای مکانی دیگر مانند بانک‌ها و سازمان‌های دولتی مورد بررسی و ارزیابی قرار گیرد. همچنین، در نظر گرفتن عوامل بازدارنده و کاهنده ریسک‌های امنیت سیستم‌های اطلاعاتی می‌تواند از دیگر پیشنهادات برای انجام پژوهش‌های آتی باشد. بعلاوه، پژوهشگران می‌توانند با استفاده از تکنیک‌های رتبه‌بندی اهمیت عوامل اثرگذار بر هر یک از ریسک‌ها را مطالعه نمایند و یا با استفاده از هوش مصنوعی سیستم‌های امنیت اطلاعات را بهینه‌سازی نمایند. در نهایت تکرار فرایند مدل‌سازی می‌تواند جزئیات بیشتری را در مدل لحاظ نماید و مدل کامل‌تری را نسبت به قبل ارائه دهد.

۶- مراجع

۱- یوسفی‌زنوز، رضا، سجادی خسرقی، فاطمه. ارزیابی ریسک در پیاده‌سازی سیستم اطلاعات بیمارستانی: مطالعه موردی». مدیریت سلامت، دوره بیستم، شماره ۶۷، ۲۳-۷. (۱۳۹۶)

۲- استرمن، جان. پویایی شناسی سیستم. ترجمه: شهرام میرزایی، احمد اصلی زاده، کیوان شاهقلیان ، علیرضا سلوک دار، علیرضا زنده باف، نشر ترمه. تهران. (۱۳۸۷).

۳- سادوسکای، جورج، اکس دمپزی، جیمز، گرین برگ، آلن، جی مک، باربارا، شوارتز، آلن. راهنمای امنیت فناوری اطلاعات. ترجمه: مهدی میردامادی، زهرا شجاعی و محمدجواد صمدی: شورای عالی اطلاع رسانی. تهران. (۱۳۸۴).

۴- لاودن، کنت سی، لاودن، جین پی. سیستم‌های اطلاعات مدیریت. ترجمه: حبیب رودساز، سینا محمد نبی، امیرحسین بهروز. دانشگاه علامه طباطبائی. تهران. (۱۳۹۱).

۵- استالینگز، ویلیام. مبانی امنیت شبکه. ترجمه: عین‌الله جعفرنژاد قمی ، علوم رایانه. تهران، ایران. چاپ اول. (۱۳۹۳).

۶- حاجی حیدری، نسترن، رحمتی، فاطمه. تحلیل ریسک پروژه‌های فناوری اطلاعات با استفاده از پویایی‌های سیستم. مدیریت تولید و عملیات، دوره نهم، شماره ۱، ۱۳۷-۱۱۹. (۱۳۹۷)

۷- مرادی پور،سهامه، رستم‌پور، احمد. نقش آموزشی نیروی انسانی در افزایش ضریب امنیت و کارایی سیستم‌های رایانه‌ای. کنفرانس ملی امنیت اطلاعات و ارتباطات، خوزستان: مجتمع آموزشی عالی جهاد دانشگاهی. (۱۳۸۹).

۸- قبادی، شهلا. سیستم داینامیک کاربردی از تفکر سیستمی: انتشارات سازمان مدیریت صنعتی. تهران. (۱۳۹۳).

۹- رستمی مازویی، نعمت، رهنمای رودپشتی، فریدون. واکاوی و تبیین اثرات کنشگران فنی و انسانی بر کارکردهای سیستم اطلاعاتی حسابداری مدیریت با استفاده از نظریه کنشگران. حسابداری مدیریت، دوره دوازدهم، شماره ۴۱، ۱۱۰-۹۱. (۱۳۹۸).

۱۰- جعفری، محمدباقر، حمیدی‌زاده، علی، نجف‌آبادی، راضیه. بررسی عوامل مؤثر بر پیروی کارکنان از سیاست‌های امنیت سیستم‌های اطلاعاتی در سازمان. دوره دوم، شماره ۳، ۱۳۱-۱۰۲. (۱۳۹۵)

۱۱- رمضانیان، محمدرحیم، اسماعیل پور، رضا، حدیدی ماسوله، مرجان. ارائه مدل پشتیبانی اجرای پروژه‌های برنامه‌ریزی منابع سازمان با رویکرد پویایی‌شناسی سیستم. نشریه مدیریت فناوری اطلاعات، تابستان، (۲)۷: ۳۰۱-۳۲۴. (۱۳۹۴).
۱۲- آذر، عادل، خدیور، آمنه. کاربرد رویکرد سیستم داینامیک در فرایند رهنگاری و سیاست‌گذاری. سیاست علم و فناوری، (۴)۲: ۲۲-۱. (۱۳۸۹).
۱۳- مداح، مرتضی. بررسی تأثیر پویایی مدیریت دانش بر عملکرد سازمانی با رویکرد کارت امتیازی متوازن و پویایی سیستم. پایان‌نامه کارشناسی‌ارشد، دانشگاه یزد. (۱۳۹۰).
14- Boranbayev, A., Boranbayev, S., & Nurbekov, A. Evaluating and Applying Risk Remission Strategy Approaches to Prevent Prospective Failures in Information Systems. In 17th International Conference on Information Technology–New Generations (647-651). Springer, Cham. (2020).
15- Yuan, T. & Chen, P. Data Mining Applications in E-Government Information Security, Procardia Engineering, 29: 235–240. (2012).
16- Richardson, R., & Director, C. S. I. CSI computer crime and security survey. Computer Security Institute, 1, 1-30. (2008).
17- Schneider, B. Secrets & lies: digital security in a networked world. Wiley publishing. (2004).
18- Malekalkalami, M. Evaluating the performance of information security management at the central libraries of public universities in Tehran: according to the international standard-ISO / IEC. Journal of Information Processing and Management, 28(4): 895-916. (2013).
19- Landwehr, C. E. Information assurance technology forecast 2005. IEEE, 4(1): 62-69. (2006).
20- Nazareth, D.L & Choi, J. A system dynamics model for information security management. Information & management, 52(1): 123-134. (2015).
21- Radzicki, M. J. System dynamics and its contribution to economics and economic modeling. System Dynamics: Theory and Applications, 401-415. (2020).
22- Sterman, J. D. Business dynamics: Systems thinking and modeling for a complex world. McGraw Hill. (2000).
23- Wei, L. & Yong, C. Information system security assessment based on system dynamics. Information Journal of security and its applications, 9(2): 73-84. (2015).
24- Gonzalez, J. J., & Sawicka, A. A framework for human factors in information security. In Wseas international conference on information security, (2002).
25- Jouini, M., Ben, L. & Ben, A., Classification of security Threat in information system. Procardia Computer Science, 32(10): 489 – 496. (2014).
26- Yong, L., Qi, L. & Kun, M. A quantitative risk assessment of the safety of the enterprise information system information based on entropy, Computer Science, 37(5): 45-48. (2010).
27- Gerić, S., & Hutinski, Ž. Information system security threats classifications. Journal of Information and Organizational Sciences, 31(1): 51-61. (2007).
28- Chorppath, A., Kumar, A. & Alpcan, T. risk management for it security: When theory meets practice: New Technologies, Mobility and Security (NTMS), 5th International Conference on. IEEE. (2012).
29- Reed, A. H., & Angolia, M. G. Risk management usage and impact on information systems project success. In Start-Ups and SMEs: Concepts, Methodologies, Tools, and Applications (1065-1084). IGI Global. (2020).
30- Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M. Deterrence and prevention-based model to mitigate information security insider threats in organisations. Future Generation Computer Systems, 97, 587-597. (2019).
31- Sinha, P., kumar Rai, A., & Bhushan, B. Information Security threats and attacks with conceivable counteraction. In 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT). IEEE. (2019).
32- Gao, W., Hong, B., Swaney, D. P., Howarth, R. W., & Guo, H. A system dynamics model for managing regional N inputs from human activities. Ecological Modelling, 322: 82-91. (2016).
33- Yuan, H. & Wang, J. A system dynamics model for determining the waste disposal charging fee in construction. European Journal of Operational Research, 237(3): 988-996. (2014).
34- Şenaras, A. E., & Sezen, H. K. System Dynamics Modelling for Policy Design: A Case Study in Turkey. In Corporate Governance Models and Applications in Developing Economies (256-274). IGI Global. (2020)
35- Samara, E., Georgiadis, P. & Bakouros, I. The impact of innovation policies on the performance of national innovation systems: A system dynamics analysis. Technovation, 32(11): 624-638. (2012).
36- Nikabadi, M. S., & Hakaki, A. A dynamic model of effective factors on open innovation in manufacturing small and medium sized companies. Int. J. of System Dynamics Applications, 7(1), 1-26. (2018).
37- Shepherd, S. P. A review of system dynamics models applied in transportation. Transportmetrica B: Transport Dynamics, 2(2): 83-105. (2014).
38- Lee, C. F. & Chung, C. P. An inventory model for deteriorating items in a supply chain with system dynamics analysis. Procedia-Social and Behavioral Sciences, 40: 41 – 51. (2012).
39- Forrester J.W. & Senge, P.M. Test for building confidence in system dynamics models. Georgia institute of technology. (1980).