Journal of Information and Communication Technology

Volume 17, Issue 66-67, Autumn and Winter 2025, pp. 54-68

Security Evaluation of Information Systems with Systems Dynamics Approach (Study Case: Agriculture Bank)

Amirhossein Abdolalipour[1*], Mohsen Shafiee[2]

[1] Assistant Prof, Department of Industrial Managemen, Khoy Branch, Islamic Azad University, Khoy. Iran

[2] MSc. in Information Technology Management, Faculty of Management, Electronic Branch, Islamic Azad University, Tehran, Iran.

Received: 20 October 2024, Revised: 10 June 2025, Accepted: 25 August 2025
Paper type: Research

Abstract

The main goal of the current research is to identify and analyze the interactions between various factors affecting information security and risks in the information systems of the Agriculture Bank using the systems dynamics approach. The simulation results show that the scenarios of increasing the security budget and improving the awareness of employees will bring the greatest risk reduction in the 36-month time horizon for the bank's information system. In the time horizon of 3 years, the risk level of the bank's information system will reach below 0.01. While with the implementation of the security budget increase scenario, this amount will be less than 0.001. In the mentioned time horizon, by increasing the budget from 1000 units to 1500 units in the 10th month, the information security level of the Agriculture Bank will increase to about 95%. To achieve this goal, the optimal allocation of resources should include new technologies and continuous training of employees. Also, it is essential to develop and update security protocols and regularly assess the weaknesses of financial institutions. Finally, it is suggested to establish a continuous monitoring and evaluation system of the bank's information systems security and to use the advice of information security experts to optimize security strategies and approaches.

Keywords: Security of Information Systems, Agriculture Bank, System Dynamics, Simulation

[*] Corresponding Author's email: amirhpour@iau.ir

دوفصلنامه
فناوری اطلاعات و ارتباطات ایران

سال هفدهم، شماره‌های ۶۶ و ۶۷، پاییز و زمستان ۱۴۰۴، صفحه ۵۴ الی ۶۸

ارزیابی امنیت سیستم‌های اطلاعاتی با رویکرد پویایی‌شناسی سیستم‌ها (مورد مطالعه: بانک کشاورزی)

امیرحسین عبدالعلی پور [۱*]، محسن شفیعی [۲]

[۱] استادیار، گروه مدیریت صنعتی، دانشکده علوم انسانی، واحد خوی، دانشگاه آزاد اسلامی، خوی، ایران.

[۲] دانش‌آموخته کارشناسی ارشد، گروه مدیریت فناوری اطلاعات، دانشکده مدیریت، واحد الکترونیکی، دانشگاه آزاد اسلامی، تهران، ایران.

تاریخ دریافت: ۱۴۰۳/۰۷/۲۹ تاریخ بازبینی: ۱۴۰۴/۰۳/۲۰ تاریخ پذیرش: ۱۴۰۴/۰۶/۰۳

نوع مقاله: پژوهشی

چکیده

هدف اصلی پژوهش حاضر، شناسایی و تحلیل تعاملات میان عوامل مختلف مؤثر بر امنیت اطلاعات و ریسک‌های سیستم‌های اطلاعاتی بانک کشاورزی با استفاده از رهیافت پویایی‌شناسی سیستم‌ها است. شبیه‌سازی‌های پژوهش نشان می‌دهد که سناریوهای سناریوی افزایش بودجه امنیتی و ارتقاء آگاهی کارکنان به ترتیب بیشترین کاهش ریسک را در افق زمانی ۳۶ ماهه برای سیستم اطلاعاتی بانک به همراه خواهند داشت. در افق زمانی ۳ ساله، سطح ریسک سیستم اطلاعاتی بانک به پایین‌تر از ۰/۰۱ خواهد رسید. درحالی‌که با اجرای سناریوی افزایش بودجه امنیتی، این میزان کمتر از ۰/۰۰۱ خواهد بود. در افق زمانی مذکور، با افزایش بودجه از ۱۰۰۰ واحد به ۱۵۰۰ واحد در ماه دهم، سطح ایمنی اطلاعاتی بانک کشاورزی تا حدود ۹۵ درصد افزایش می‌یابد. برای تحقق این هدف، تخصیص بهینه منابع باید شامل فناوری‌های نوین و آموزش مستمر کارکنان باشد. همچنین، توسعه و به‌روزرسانی پروتکل‌های امنیتی و ارزیابی منظم نقاط ضعف مؤسسات مالی ضروری است. درنهایت، پیشنهاد می‌شود که نظام پایش و ارزیابی مستمر وضعیت امنیت سیستم‌های اطلاعاتی بانک برقرار شود و از مشاوره کارشناسان امنیت اطلاعات بهره‌برداری گردد تا استراتژی‌ها و رویکردهای امنیتی بهینه‌سازی شوند.

کلیدواژگان: امنیت سیستم‌های اطلاعاتی، بانک کشاورزی، پویایی‌شناسی سیستم، شبیه‌سازی.

* رایانامهٔ نویسنده مسؤول: amirhpour@iau.ir

۱- مقدمه

ارزیابی امنیت سیستم‌های اطلاعاتی بانکی به‌عنوان یکی از پیش‌نیازهای اساسی در حفظ اعتبار و اعتماد عمومی به نظام مالی کشورها، حائز اهمیت بسزایی است. با توجه به رشد روزافزون تهدیدات سایبری و پیچیدگی محیط فناوری اطلاعات، ارزیابی و ارتقاء امنیت اطلاعات در بانک‌ها به یک ضرورت استراتژیک برای پایداری و تاب‌آوری مؤسسات مالی تبدیل شده است. این ارزیابی نه‌تنها شامل شناسایی آسیب‌پذیری‌های موجود در زیرساخت‌های فناوری اطلاعات می‌شود، بلکه نیازمند تعیین و مدیریت ریسک‌های مرتبط با تهدیدات سایبری، نشت اطلاعات و سوءاستفاده‌های مالی است. جوانب مختلف این ارزیابی، ازجمله سیاست‌گذاری‌های امنیتی، پیاده‌سازی استانداردهای بین‌المللی و برگزاری آزمون‌های نفوذ، نشان‌دهنده پیچیدگی و ضرورت رویکردهای جامع در این زمینه است. به‌علاوه، با توجه به اینکه سیستم‌های اطلاعاتی بانکی به‌عنوان مراکز حساسی برای ذخیره و پردازش اطلاعات مالی مورداستفاده قرار می‌گیرند، اطمینان از یکپارچگی، محرمانگی و در دسترس بودن اطلاعات بدون شک به استمرار و پایداری فعالیت‌های اقتصادی و مالی مؤسسات و همچنین امنیت ملی کمک شایانی خواهد کرد. در این میان، بانک کشاورزی به‌عنوان یک نهاد مالی مهم و تأثیرگذار در اقتصاد کشور، نیازمند توجه ویژه به این مقوله است.

نخستین پیامد نقص امنیت سیستم‌های اطلاعاتی، از دست رفتن داده‌های هزینه‌های ناشی از عدم وجود امنیت مناسب شامل جریمه‌های قانونی، هزینه‌های مربوط به بازسازی سیستم‌ها و نیز هزینه‌های مربوط به جبران خسارت به مشتریان و کارکنان است [۱]. بسیاری از سازمان‌ها فاقد سیاست‌های مناسب برای مدیریت حوادث امنیتی هستند که این موضوع باعث افزایش خطرات می‌شود[۲]. این مسأله نشان‌دهنده اهمیت سرمایه‌گذاری در امنیت سایبری و ارتقاء استانداردهای حفاظتی در سازمان‌ها است، چراکه هرگونه ضعف در این زمینه می‌تواند به زیان‌های جبران‌ناپذیری منجر شود.

سیستم‌های امنیت اطلاعات به دلیل ویژگی‌های ذاتی خود، به‌عنوان سیستم‌های پیچیده و پویا شناخته می‌شوند. این پیچیدگی و پویایی نه‌تنها ناشی از تنوع تهدیدات سایبری است، بلکه به تغییرات سریع در فناوری و نیازهای سازمان‌ها نیز مربوط می‌شود. ارزیابی و ارتقاء سطح امنیت سیستم‌های اطلاعاتی در بانک کشاورزی نه‌تنها به‌عنوان یک عامل بازدارنده در مقابل تهدیدات سایبری عمل می‌کند، بلکه موجب افزایش اعتماد عمومی به خدمات بانکی و همچنین بهبود عملکرد کلی این مؤسسه مالی می‌گردد. هدف اصلی پژوهش حاضر، ارائه تصویری جامع از وضعیت امنیت اطلاعات در سازمان موردمطالعه و شناسایی روندهای بحرانی و نقاط حساس است که می‌تواند مبنای اتخاذ تصمیمات مدیریتی و بهبود اقدامات امنیتی در آینده باشد در این راستا، رویکرد پویایی سیستم‌ها به‌عنوان یک ابزار کارآمد برای تحلیل دینامیک‌های موجود در این سیستم‌ها و شناسایی نقاط ضعف و قوت آن‌ها، موردتوجه قرار می‌گیرد. این رویکرد امکان مدل‌سازی رفتار سیستم و شبیه‌سازی سناریوهای مختلف را فراهم می‌آورد که می‌تواند به تصمیم‌سازان در این بانک در اتخاذ تصمیمات راهبردی و بهبود تدابیر امنیتی یاری رساند.

پژوهش حاضر با بهره‌گیری از رویکرد پویایی‌شناسی سیستم‌ها، به‌صورت جامع و نظام‌مند به تحلیل و شبیه‌سازی ابعاد مختلف امنیت سیستم‌های اطلاعاتی بانک کشاورزی می‌پردازد و با مدل‌سازی علی و شناسایی چرخه‌های بازخوردی، امکان تبیین روابط پیچیده میان متغیرهای کلیدی مؤثر بر امنیت اطلاعات را فراهم می‌آورد. با توجه به جایگاه راهبردی بانک کشاورزی در نظام مالی کشور و افزایش تهدیدات سایبری، ارزیابی و ارتقاء مستمر امنیت اطلاعات، نه‌تنها برای حفظ محرمانگی، یکپارچگی و دسترس‌پذیری داده‌های مالی ضروری است، بلکه نقشی بنیادین در پایداری عملیات بانکی، اعتماد عمومی و کاهش ریسک‌های عملیاتی ایفا می‌کند. یافته‌های این پژوهش، ضمن شناسایی نقاط ضعف و روندهای بحرانی، مبنایی علمی برای تصمیم‌سازی مدیران در زمینه تخصیص بهینه منابع، توسعه فناوری‌های نوین، طراحی سیاست‌های آموزشی هدفمند و به‌روزرسانی پروتکل‌های امنیتی فراهم می‌سازد و از این طریق، تاب‌آوری و امنیت بانک را در برابر تهدیدات نوظهور به‌طور معناداری افزایش می‌دهد.

۲- مروری بر مبانی نظری و پیشینه پژوهش

۲-۱- مبانی نظری

امنیت اطلاعات به‌عنوان یکی از ارکان اساسی در حفاظت از داده‌ها، شامل سه اصل محوری یعنی محرمانگی، یکپارچگی و قابلیت دسترسی است [۳]. امنیت سیستم‌های اطلاعاتی بانکی، به‌عنوان یکی از ارکان اساسی در حفظ اعتماد مشتریان و تضمین سلامت اقتصادی یک کشور، تحت تأثیر مجموعه‌ای از عوامل متنوع و پیچیده قرار دارد. این عوامل شامل خطاهای انسانی، تهدیدات سایبری، نقص‌های فناوری و همچنین سیاست‌ها و رویه‌های امنیتی داخلی بانک‌ها است.

۲-۱-۱- عوامل انسانی مؤثر بر امنیت سیستم‌های اطلاعاتی

خطاهای انسانی، به‌عنوان یکی از عوامل اصلی تهدیدکننده، می‌تواند به بروز نقص‌های جدی در سیستم‌های امنیتی منجر شود، چراکه نادیده گرفتن پروتکل‌های امنیتی یا ارتکاب اشتباهات در برنامه‌نویسی و استفاده نادرست از سیستم می‌تواند دروازه‌ای برای نفوذ هکرها به سیستم‌های اطلاعاتی باشد [۴]. آسیب عمدی کاربران معمولاً ناشی از نیت‌های مخرب است، درحالی‌که آسیب غیرعمدی ناشی از بی‌توجهی یا عدم آگاهی کارکنان است. هر دو نوع آسیب می‌توانند عواقب جدی برای امنیت سیستم‌های اطلاعاتی داشته باشند[۵]. انگیزه‌های حمله به سیستم‌های اطلاعاتی می‌تواند از نارضایتی شغلی، انتقام‌جویی، یا حتی سود مالی ناشی شود [۶]. علاوه بر این، تهدیدات سایبری به‌طور روزافزونی در حال افزایش است و گروه‌های مجرمانه از تکنیک‌های پیشرفته‌تر برای نفوذ به این سیستم‌ها استفاده می‌کنند که این امر نیازمند به‌روزرسانی مداوم پروتکل‌های امنیتی و استفاده از فناوری‌های جدید مانند هوش مصنوعی و بلاک‌چین است [۷].

توانایی پیشگیری از حملات به‌شدت به آموزش و آگاهی کارکنان و مشتریان بستگی دارد. عدم آموزش مناسب می‌تواند منجر به نادیده گرفتن پروتکل‌های امنیتی و درنتیجه افزایش خطرات شود [۷].

استفاده از نرم‌افزارها و خدمات غیرضروری می‌تواند سطح آسیب‌پذیری را افزایش دهد. این نرم‌افزارها ممکن است شامل برنامه‌های قدیمی یا غیر موردنیاز باشند که به‌راحتی می‌توانند مورد سوءاستفاده قرار گیرند [۸].

دسترسی حداقلی به اطلاعات و سیستم‌ها یکی از روش‌های مؤثر در کاهش خطرات امنیتی است. با محدود کردن دسترسی کاربران به اطلاعات حساس، می‌توان احتمال وقوع حملات داخلی را کاهش داد. این رویکرد به‌ویژه در سازمان‌های بزرگ بسیار حیاتی است [۹].

۲-۱-۲- اثر عملکرد شبکه بر امنیت سیستم‌های اطلاعاتی

امنیت سیستم‌های اطلاعاتی بانکی به‌شدت تحت تأثیر شبکه و آسیب‌پذیری‌های موجود در آن است. این آسیب‌پذیری‌ها می‌توانند شامل نقاط ضعف در پایگاه داده، بدافزارها، به‌روزرسانی نرم‌افزارها و پروتکل‌های ارتباطی مانند پروتکل کنترل انتقال **(TCP)** باشند. بدافزارها می‌توانند به سیستم‌های بانکی نفوذ کرده و داده‌ها را سرقت کنند یا آسیب‌هایی به زیرساخت‌ها وارد کنند. یک مطالعه نشان می‌دهد که حملات بدافزاری به‌ویژه در کانال‌های بانکی می‌تواند خسارات مالی قابل‌توجهی به بار آورد [۱۰].

ریسک امنیت شبکه به ضعف‌های موجود در زیرساخت‌های فناوری اطلاعات مربوط می‌شود. امکان‌پذیری حمله به سیستم‌های اطلاعاتی بستگی به وجود نقاط ضعف در زیرساخت‌ها دارد. این نقاط ضعف می‌توانند ناشی از طراحی ضعیف، عدم به‌روزرسانی نرم‌افزارها یا عدم رعایت استانداردهای امنیتی باشند [۱۱]. سیستم‌هایی که از پروتکل‌های امنیتی قدیمی استفاده می‌کنند یا به‌روزرسانی نمی‌شوند، بیشتر در معرض خطر قرار دارند [۱۲]. نرم‌افزارهای قدیمی یا ناپایدار ممکن است نقاط ضعف زیادی داشته باشند که هکرها از آن‌ها بهره‌برداری کنند. استفاده از استانداردهای معتبر مانند **PTES** و **OWASP** در ارزیابی آسیب‌پذیری‌ها می‌تواند به شناسایی نقاط ضعف کمک کند [۱۳]. همچنین، استفاده از فناوری‌های نوین مانند هوش مصنوعی می‌تواند به کاهش ریسک‌ها کمک کند [۱۴].

۲-۱-۳- ریسک‌های فنی در سیستم‌های بانکی

نقص‌های فناوری، شامل آسیب‌پذیری‌های نرم‌افزاری و زیرساخت‌های سخت‌افزاری، نیز به‌عنوان عوامل بحرانی در این زمینه مطرح هستند که ممکن است به‌روزرسانی‌های ناکافی یا عدم توجه به معایب امنیتی سیستم‌ها منجر شود [۱۵]. عدم انجام به‌روزرسانی‌های لازم می‌تواند منجر به بروز آسیب‌پذیری‌هایی شود که هکرها می‌توانند از آن‌ها سوءاستفاده کنند[۱۲].

استفاده از پروتکل‌های ناامن برای انتقال داده‌ها می‌تواند منجر به سرقت اطلاعات حساس شود؛ بنابراین، انتخاب و پیاده‌سازی پروتکل‌های امن مانند **TLS** ضروری است [۱۶].

حملات **MITM** می‌توانند با استفاده از تکنیک‌هایی مانند **ARP spoofing**، ارتباطات امن را تضعیف کنند و اطلاعات حساس را در معرض خطر قرار دهند [۱۷].

۲-۱-۴- اثر نوع داده‌ها بر امنیت سیستم‌های اطلاعاتی

حذف یا تغییر داده‌ها می‌تواند به‌طور مستقیم بر یکپارچگی و صحت اطلاعات تأثیر بگذارد [۱۸]. هرچه حجم داده‌ها بیشتر باشد، جذابیت برای هکرها نیز افزایش می‌یابد [۱۹]. در سیستم‌های بانکی، هرگونه تغییر غیرمجاز در داده‌ها می‌تواند منجر به خسارات مالی و از دست رفتن اعتماد مشتریان شود. همچنین، در صورت حذف ناخواسته داده‌ها، بازیابی اطلاعات ممکن است زمان‌بر و پرهزینه باشد [۱۸].

ریسک‌های مرتبط با داده‌ها شامل خطرات ناشی از نشت اطلاعات، دسترسی غیرمجاز و عدم تطابق با مقررات هستند. این ریسک‌ها می‌توانند منجر به خسارات مالی و قانونی برای مؤسسات مالی

شوند. ارزیابی دقیق ریسک و پیاده‌سازی استراتژی‌های مؤثر برای مدیریت آن ضروری است [۲۰].

محیط انتقال داده‌ها نقش حیاتی در امنیت اطلاعات دارد. وجود تهدیدات سایبری مانند حملات منع سرویس **(DDoS)** و نفوذ به شبکه می‌تواند به امنیت اطلاعات آسیب بزند. پروتکل **TCP** به‌خودی‌خود امنیت داده‌ها را تضمین نمی‌کند. استفاده از پروتکل‌هایی مانند **SSL** برای رمزگذاری داده‌ها در ارتباطات بانکی بسیار مهم است، اما این پروتکل‌ها نیز ممکن است تحت حملات خاصی قرار [۱۶]. استفاده از تکنیک‌های رمزنگاری مانند **Visual Cryptography** می‌تواند به تأمین امنیت اطلاعات در حین انتقال کمک کند [۲۱].

۲-۱-۵- اثر عوامل فیزیکی بر امنیت سیستم‌های اطلاعاتی

به‌طور خاص، زیرساخت‌های فیزیکی ازجمله امنیت مراکز داده، طراحی فیزیکی ساختمان‌ها و شرایط محیطی محیط کار مانند دما و رطوبت می‌توانند به‌طور مستقیم بر عملکرد و امنیت این سیستم‌ها تأثیر بگذارند [۲۲]. همچنین، نوسانات انرژی می‌توانند تأثیرات قابل‌توجهی بر عملکرد سیستم‌های اطلاعات بانکی داشته باشند. تغییرات ناگهانی در تأمین انرژی ممکن است منجر به خاموشی‌های ناخواسته یا کاهش کیفیت خدمات شود [۲۳]. این موضوع به‌ویژه در بانک‌ها که به پایداری و دسترسی مداوم به داده‌ها وابسته‌اند، اهمیت دارد. آسیب‌های سخت‌افزاری می‌توانند ناشی از عوامل طبیعی مانند زلزله یا طوفان یا عوامل محیطی مانند آتش‌سوزی نیز باشد [۲۴]. همچنین، نقص در تجهیزات می‌تواند به دلیل فرسودگی یا عدم نگهداری مناسب رخ دهد. این آسیب‌ها ممکن است منجر به از دست رفتن داده‌ها یا اختلال در خدمات بانکی شوند [۲۵].

از طرف دیگر، ریسک‌های فیزیکی مانند تهدیدات ناشی از سرقت، خرابکاری و حملات فیزیکی به زیرساخت‌ها، می‌توانند منجر به آسیب جدی به سیستم‌های اطلاعات بانکی شوند و نیازمند تدابیر امنیتی قوی برای حفاظت از دارایی‌ها هستند [۲۶].

اندازه سیستم اطلاعاتی نیز عاملی کلیدی است .سیستم‌های بزرگ‌تر معمولاً پیچیدگی بیشتری دارند و این پیچیدگی می‌تواند منجر به ضعف‌های امنیتی بیشتری شود. همچنین، مدیریت و نظارت بر سیستم‌های بزرگ‌تر دشوارتر است و این موضوع می‌تواند ریسک حملات را افزایش دهد [۲۷].

قابلیت کشف تهدیدات سایبری یکی از مهم‌ترین عوامل در پیشگیری از حملات است. استفاده از ابزارهای پیشرفته برای شناسایی تهدیدات و تجزیه‌وتحلیل رفتار شبکه می‌تواند به شناسایی زودهنگام حملات کمک کند. تحقیقات نشان داده‌اند که سازمان‌هایی که قابلیت کشف بالایی دارند، کمتر در معرض حملات موفق قرار دارند [۲۸]. علاوه بر این، سابقه حملات سایبری در یک نهاد مالی خاص نیز می‌تواند بر احتمال وقوع حملات آینده تأثیر بگذارد [۲۹]. رویدادهای ناخوشایند مانند حملات سایبری موفق می‌توانند تأثیر منفی بر سطح امنیت ادراک‌شده مشتریان بانک داشته باشند. [۳۰].

با استفاده از فناوری‌های پیشرفته، بانک‌ها قادر به شناسایی و پاسخ سریع‌تر به تهدیدات هستند که این امر می‌تواند خسارات مالی و اعتباری را به حداقل برساند[۳۱]. وجود رویه‌های بازرسی منظم و دقیق می‌تواند به شناسایی نقاط ضعف کمک کند. با انجام بازرسی‌های دوره‌ای، سازمان‌ها می‌توانند نقاط ضعف خود را شناسایی و برطرف کنند [۳۲]. این رویه‌ها باید شامل ارزیابی مستمر خطرات و آسیب‌پذیری‌ها باشند.

۲-۱-۶- اثر توسعه سیاست‌های پیشگیرانه و استانداردهای امنیتی بر امنیت سیستم‌های اطلاعاتی

تدوین سیاست‌های پیشگیرانه و استانداردهای امنیتی مشخص می‌تواند به کاهش احتمال وقوع حملات کمک کند [۳۳]. تخصیص بودجه آگاهی بخشی و تخصیص منابع مالی برای توسعه سیاست‌های امنیتی و زیرساخت‌ها، نقش مهمی در تقویت امنیت سیستم‌های اطلاعاتی ایفا می‌کند [۳۴ و ۳۵].

بااین‌حال، تحقیق [۳] با رویکردی انتقادی تأکید می‌کند که صرف افزایش بودجه یا پیروی از استانداردهای مرسوم، بدون توجه به زمینه سازمانی و رفتار کاربران، نمی‌تواند تضمین‌کننده امنیت پایدار باشد. همچنین، تعهد مدیریت ارشد در پیاده‌سازی سیاست‌های امنیتی و تخصیص منابع مالی مناسب برای این امر از اهمیت ویژه‌ای برخوردار است[۳۶]. جدول ۱ خلاصه‌ای از دسته‌بندی شاخص‌های امنیتی سیستم‌های اطلاعاتی بانک کشاورزی را ارائه می‌دهد.

با توجه به اهداف و چارچوب نظری پژوهش حاضر، سؤالات اصلی زیر مطرح می‌شود:

۱. چه عواملی بیشترین تأثیر را بر سطح امنیت سیستم‌های اطلاعاتی بانک کشاورزی دارند؟
۲. افزایش بودجه امنیتی و ارتقاء آگاهی کارکنان چه تأثیری بر کاهش ریسک اطلاعاتی بانک کشاورزی دارد؟
۳. کدام‌یک از سناریوهای پیشنهادی (افزایش بودجه، آموزش کارکنان، به‌روزرسانی فناوری) بیشترین اثربخشی را در بهبود امنیت اطلاعاتی بانک کشاورزی دارد؟

جدول ۱. دسته‌بندی شاخص‌های امنیتی سیستم‌های اطلاعاتی بانک

دسته	شاخص‌های کلیدی	توضیح
عوامل انسانی	آگاهی و آموزش کارکنان، مدیریت دسترسی، سیاست‌ها و رویه‌های امنیتی	تأثیر رفتار و دانش کارکنان بر امنیت
شبکه و زیرساخت	امنیت شبکه (فایروال، **IDS/IPS**)، امنیت پایگاه داده، امنیت فیزیکی	حفاظت از زیرساخت‌های **IT**بانک.
داده‌ها	حفاظت از یکپارچگی داده‌ها، حفاظت از محرمانگی داده‌ها، قابلیت دسترسی به داده‌ها	مدیریت و حفاظت از اطلاعات حساس بانک
ریسک‌های فنی	آسیب‌پذیری‌های نرم‌افزاری، پروتکل‌های امنیتی، مدیریت حوادث امنیتی	مقابله با تهدیدات فنی و آسیب‌پذیری‌ها.
سیاست‌ها و استانداردها	تطابق با استانداردها و مقررات، تعهد مدیریت، بودجه امنیتی	اهمیت سیاست‌ها، استانداردها و حمایت مدیریت از امنیت

۲-۲- پیشینه پژوهش

در پژوهش [۳۷] شاخص‌های تأثیرگذار بر امنیت سیستم‌های اطلاعاتی. بررسی شد. نتایج شبیه‌سازی در مدت ۱۲ ماه نشان می‌دهد که در بین ریسک‌های شناسایی‌شده بیشترین اهمیت مربوط به ریسک فنی است؛ ریسک داده، انسان و فیزیکی در رتبه‌های بعدی قرار می‌گیرند؛ کم‌اهمیت‌ترین ریسک مربوط به محیط است. درنهایت، 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.

نتیجه مطالعه [۲۹] نشان داد که بانک‌هایی که سابقه حملات بیشتری دارند، معمولاً با نرخ بالاتری از حملات جدید مواجه می‌شوند. این امر می‌تواند ناشی از عدم توانایی در اصلاح نقاط ضعف امنیتی یا عدم اجرای پروتکل‌های امنیتی مؤثر باشد.

نتیجه مطالعه [۲۸] در مورد ریسک‌های سایبری در خدمات مالی نشان داد که بسیاری از بانک‌ها به دلیل ضعف در دفاع امنیتی و عدم آگاهی کافی از تهدیدات، هدف حملات سایبری قرار می‌گیرند.

در یک مطالعه موردی در یک بانک بزرگ، مشخص شد که مشکلات اساسی در حاکمیت و فرهنگ امنیت وجود دارد که می‌تواند منجر به افزایش ریسک حملات سایبری شود [۳۸].

مطالعه [۳۹] به بررسی امنیت دستگاه‌های خودپرداز **(ATM)** در نیجریه پرداخته است و نشان می‌دهد که اجرای فعلی امنیت در این سیستم‌ها به‌اندازه کافی مؤثر نیست. این تحقیق با توزیع ۴۰۰ پرسشنامه بین کارآفرینان، کارمندان دولتی و دانشجویان انجام شد. نتایج نشان داد که هیچ تفاوت معناداری در ادراک این گروه‌ها نسبت به تأثیر مثبت دستگاه‌های خودپرداز بر خدمات بانکی وجود ندارد. همچنین، چالش‌های امنیتی مربوط به خدمات خودپرداز برای این گروه‌ها یکسان بود.

مطالعه [۴۰] به ارزیابی اثربخشی امنیت شبکه و فایروال در سیستم‌های بانکی نیجریه پرداخته است. نتایج مطالعه مذکور نشان می‌دهد که بانک‌های نیجریه‌ای به‌ندرت با حملات مخرب مواجه می‌شوند و استراتژی‌های امنیت شبکه‌ای که اتخاذ کرده‌اند، مؤثر بوده است. همچنین، یک برنامه کاربردی برای تقویت امنیت سیستم‌های بانکی توسعه‌یافته است.

مطالعه [۴۱] به بررسی پیاده‌سازی استاندارد **ISO 27001** در صنعت بانکداری می‌پردازد. این استاندارد به‌عنوان یک چارچوب جامع برای حفاظت از داده‌های حساس شناخته می‌شود. نتایج پژوهش مذکور نشان می‌دهد که پیاده‌سازی **ISO 27001** به بهبود مدیریت ریسک، قابلیت پاسخگویی به حوادث و افزایش تاب‌آوری کنترل‌های امنیت اطلاعات کمک کرده است. همچنین، این مطالعه به بررسی چالش‌ها و ملاحظات خاص صنعت بانکداری پرداخته و تأثیرات مثبت آن بر فرهنگ آگاهی امنیتی میان کارکنان بانک‌ها را موردبررسی قرار داده است.

مطالعه [۴۲] به بررسی تأثیر جنگ اوکراین بر امنیت اطلاعات صنعت بانکداری در کشورهای مجارستان و اسلواکی می‌پردازد. با استفاده از روش‌های کیفی، محققان داده‌های موجود و مصاحبه‌هایی با کارشناسان امنیت اطلاعات انجام دادند. نتایج نشان می‌دهد که بانک‌ها در اتحادیه اروپا با سطح بالایی از ریسک‌های سایبری مواجه هستند.

مطالعه [۴۳] در مورد تهدیدات امنیتی سیستم‌های حسابداری کامپیوتری در بانک‌های اردن انجام‌شده است. نتایج این تحقیق نشان می‌دهد که بسیاری از تهدیدات امنیتی ناشی از اشتباهات غیرعمدی کارکنان مانند ورود داده‌های نادرست یا اشتراک‌گذاری رمزهای عبور است.

تحقیق [۴۴] به ارزیابی نرم‌افزارها و سیستم‌های امنیتی در بانک‌های چین پرداخته است. این مطالعه به شناسایی آسیب‌پذیری‌های موجود در نرم‌افزارهای بانکی و نحوه مدیریت آن‌ها پرداخته است. محققان به این نتیجه رسیدند که به‌کارگیری رویکردهایی نظیر ارزیابی مستمر ریسک و آزمایش‌های نفوذ می‌تواند به شناسایی و کاهش تهدیدات امنیتی کمک کند.

به‌علاوه، در تحقیق [۴۵] که در مورد ارزیابی ریسک‌های امنیتی در بانک‌ها در اسپانیا انجام شد، به بررسی تأثیر مهاجرت به سیستم‌های ابری بر امنیت اطلاعات پرداخته‌شده است. نتایج این

تحقیق نشان داد که درحالی‌که خدمات ابری می‌توانند بهره‌وری را افزایش دهند، اما به نیاز به ارزیابی دقیق‌تری از ریسک‌های موجود در نگهداری داده‌ها می‌افزایند. آن‌ها پیشنهاد کردند که بانک‌ها باید تدابیر امنیتی مضاعف را در رویکردهای خود لحاظ کنند.

نهایتاً، مطالعه [۴۶] در مورد رابطهٔ آگاهی از امنیت اطلاعات با قصد نقض امنیت اطلاعات با نقش میانجی هنجارهای فردی و خودکنترلی عنوان مکرر: قصد نقض امنیت اطلاعات، با مطالعه از ۱۸۴ نفر از کارمندان بانک کشاورزی اصفهان نشان داد آگاهی از امنیت اطلاعات با کاهش ۵۳ درصدی قصد نقض امنیت مرتبط است. این پژوهش تأکید می‌کند که آموزش کارکنان توسط متخصصان امنیت، از طریق تقویت هنجارهای فردی (۰/۶۷) و خودکنترلی (۰/۷۱) نقشی کلیدی در کاهش رفتارهای مخرب سایبری دارد.

مطالعه [۴۷] با رویکردی انتقادی خاطرنشان می‌کند که بسیاری از رویکردهای امنیتی فعلی، به دلیل اتکای بیش‌ازحد بر کنترل‌های فنی و بی‌توجهی به تهدیدات نوظهور و ابعاد رفتاری کاربران، پاسخگوی کامل نیازهای امنیتی بانک‌های چین نیستند. این پژوهش توصیه می‌کند که مدل‌های ارزیابی امنیت باید به‌صورت مستمر به‌روزرسانی شوند و تحلیل ریسک جامع‌تری را شامل شوند. همچنین، تقویت آموزش و فرهنگ‌سازی امنیتی در میان کارکنان و مشتریان به‌عنوان یک ضرورت کلیدی مطرح‌شده است. افزون بر این، مطالعه مذکور بر اهمیت بهره‌گیری از فناوری‌های نوین همچون هوش مصنوعی و یادگیری ماشین برای شناسایی تهدیدات پیشرفته و تحلیل رفتار کاربران تأکید دارد تا بتوان از رویکردهای سنتی فراتر رفت و به سطح بالاتری از امنیت اطلاعاتی در بانکداری آنلاین دست یافت.

۳- روش پژوهش

پژوهش حاضر از لحاظ رویکردی از نوع استقرایی، به لحاظ هدف از نوع کاربردی و ازلحاظ گردآوری داده‌ها، توصیفی- تحلیلی است. در پژوهش حاضر بنا بر فلسفه عمل‌گرایی، به‌منظور ارزیابی امنیت سیستم‌های اطلاعاتی بانک کشاورزی از مدل‌های تأییدشده، بهره گرفته‌شده است. همچنین در راستای طراحی مدل و اعتبارسنجی آن از نظر خبرگان استفاده‌شده است.

ابتدا، مقالات علمی، گزارش‌های صنعتی و استانداردهای امنیتی مرتبط با امنیت سیستم‌های اطلاعاتی در صنعت بانکداری (مانند استانداردهای**ISO 27001** ، **NIST** و غیره) بررسی شدند تا یک لیست اولیه از متغیرهای بالقوه مطابق جدول ۲ شناسایی شود. متغیرها بر اساس معیارهای زیر انتخاب شدند:

۱. ارتباط مستقیم با امنیت سیستم‌های اطلاعاتی بانک کشاورزی :متغیرها باید به‌طور مستقیم بر سطح امنیت سیستم‌های اطلاعاتی بانک تأثیرگذار باشند.
۲. قابلیت اندازه‌گیری و کمی‌سازی :متغیرها باید قابل‌اندازه‌گیری و کمی‌سازی باشند تا بتوان آن‌ها را در مدل پویایی‌شناسی سیستم‌ها استفاده کرد.
۳. تأثیرگذاری بر سایر متغیرها در سیستم :متغیرها باید بر سایر متغیرهای سیستم تأثیرگذار باشند و روابط علی و معلولی قابل‌توجهی داشته باشند.

سپس، مصاحبه‌های نیمه ساختاریافته با ۵ نفر از کارشناسان امنیت اطلاعات بانک کشاورزی انجام شد. این کارشناسان دارای حداقل ۵ سال تجربه در زمینه امنیت اطلاعات بانکی بودند و در بخش‌های مختلفی مانند مدیریت ریسک امنیت اطلاعات، امنیت شبکه و امنیت پایگاه داده فعالیت می‌کردند. هدف از این مصاحبه‌ها، اعتبارسنجی لیست اولیه متغیرها، شناسایی متغیرهای خاص بانک کشاورزی و جمع‌آوری اطلاعات کیفی در مورد روابط بین متغیرها بود.

درنهایت، اسناد و مدارک داخلی بانک کشاورزی، مانند گزارش‌های ارزیابی ریسک، سیاست‌های امنیتی، رویه‌های عملیاتی، گزارش‌های ممیزی امنیتی و گزارش‌های حوادث امنیتی، مورد تجزیه‌وتحلیل قرار گرفتند تا داده‌های لازم برای کمی‌سازی متغیرها جمع‌آوری شود. این اسناد به شناسایی دقیق‌تر نقاط ضعف و قوت امنیتی بانک و همچنین تعیین مقادیر اولیه متغیرها کمک کردند.

به‌منظور ارزیابی اثرات عوامل مختلف بر امنیت سیستم‌های اطلاعاتی بانک کشاورزی، از مدل پویایی‌شناسی سیستم‌ها برای شبیه‌سازی رفتار سیستم در طول زمان استفاده شد.

شبیه‌سازی‌ها با استفاده از نرم‌افزار **Vensim PLE** انجام یافتند. این نرم‌افزار به دلیل قابلیت‌های قدرتمند در مدل‌سازی سیستم‌های پیچیده و پویا، انتخاب شد. مدل با استفاده از داده‌های تاریخی بانک کشاورزی و نظرات کارشناسان امنیت اطلاعات کالیبره شد.

شبیه‌سازی‌ها برای یک بازه زمانی ۳۶ ماهه انجام شدند تا اثرات بلندمدت سناریوها بر امنیت سیستم‌های اطلاعاتی ارزیابی شود. این بازه زمانی با توجه به چرخه عمر سیستم‌های اطلاعاتی و اهداف استراتژیک بانک انتخاب شده است. نهایتاً، به‌منظور سنجش اعتبار مدل‌های پویایی‌شناسی سیستم، از روش‌های اعتبار ساختاری و رفتاری استفاده‌شده است.

جدول ۲. متغیرهای اولیه اثرگذار بر سطح امنیت سیستم‌های اطلاعاتی بانک

متغیر	تعریف عملیاتی	واحد	نقش در مدل
سطح امنیت اطلاعات	میزان حفاظت از اطلاعات بر اساس شاخص‌های رخدادهای امنیتی، رعایت سیاست‌ها و آزمون‌های نفوذ	درصد	نشان‌دهنده وضعیت کلی امنیت و تحت تأثیر سرمایه‌گذاری و تهدیدات است
سرمایه‌گذاری در امنیت	میزان منابع مالی و انسانی اختصاص‌یافته به امنیت	واحد پول (ریال)	جریان ورودی به سطح امنیت اطلاعات و عامل افزایش آن.
تعداد کارکنان آموزش‌دیده	تعداد کارکنان دارای آموزش رسمی امنیت اطلاعات	نفر	نشان‌دهنده آگاهی کارکنان و عامل کاهش خطاهای انسانی
تعداد رخدادهای امنیتی	تعداد حملات سایبری موفق و نشت اطلاعات در دوره زمانی مشخص	تعداد	جریان خروجی از سطح امنیت اطلاعات و عامل کاهش آن
آگاهی کارکنان از تهدیدات امنیتی	میانگین نمره کارکنان در آزمون دانش امنیت اطلاعات	درصد	مؤثر بر میزان رعایت سیاست‌های امنیتی و کاهش خطاهای انسانی
آسیب‌پذیری‌های فنی	تعداد نقاط ضعف شناسایی‌شده در سیستم‌ها بر اساس استاندارد **CVSS**	تعداد	نشان‌دهنده نقاط ضعف سیستم‌ها و عامل افزایش احتمال رخدادهای امنیتی.
به‌روزرسانی نرم‌افزارها و سیستم‌عامل‌ها	درصد سیستم‌های دارای آخرین نسخه نرم‌افزار و سیستم‌عامل.	درصد	جریان ورودی به آسیب‌پذیری‌های فنی و عامل کاهش آن
رعایت سیاست‌های امنیتی	درصد کارکنان پایبند به سیاست‌ها و رویه‌های امنیتی.	درصد	مؤثر بر کاهش رخدادهای امنیتی و خطاهای انسانی
تعداد حملات سایبری	تعداد تلاش‌های نفوذ به سیستم‌ها شناسایی‌شده توسط **IDS و SIEM**	تعداد	جریان خروجی از سطح امنیت اطلاعات و عامل کاهش آن.
حجم داده‌های حساس	میزان داده‌های محرمانه ذخیره‌شده در سیستم‌ها.	گیگابایت	نشان‌دهنده خسارت احتمالی ناشی از نشت اطلاعات و عامل افزایش جذابیت برای مهاجمان
سرعت شناسایی تهدیدات	میانگین زمان شناسایی تهدید در سیستم‌ها با استفاده از **IDS و SIEM**	ساعت	مؤثر بر کاهش خسارات ناشی از رخدادهای امنیتی
اثربخشی پاسخ به رخدادها	درصد رخدادهای امنیتی مهار و رفع شده توسط **CSIRT**	درصد	مؤثر بر کاهش خسارات ناشی از رخدادهای امنیتی
بودجه امنیتی	میزان بودجه اختصاص‌یافته به امنیت سیستم‌ها.	واحد پول (ریال)	مؤثر بر افزایش سرمایه‌گذاری در امنیت و تعداد کارکنان آموزش‌دیده

۴- یافته‌های پژوهش

۴-۱- نمودار علت و معلولی آسیب‌پذیری از سوی خطاهای انسانی

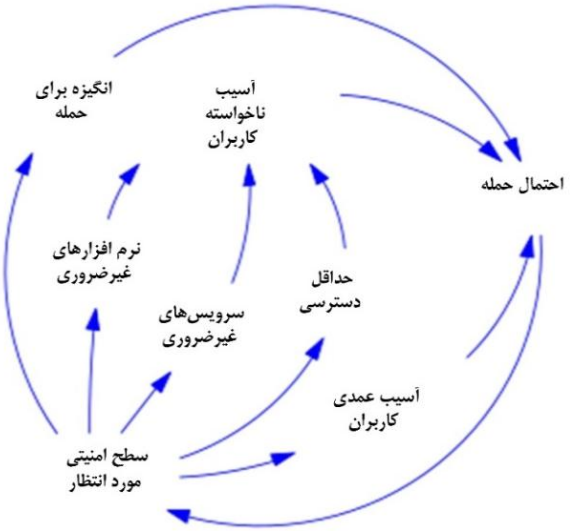
قابلیت پیشگیری یکی از متغیرهای اساسی سیستم است که افزایش آن، انگیزه حملات هکرها به سیستم بانک را کاهش می‌دهد. با کاهش انگیزه هکرها، احتمال حمله از سوی آن‌ها کاهش پیدا می‌کند که افزایش قابلیت پیشگیری را به دنبال خواهد داشت. از سوی دیگر، افزایش قابلیت پیشگیری موجب می‌شود که کاربران به دنبال استفاده از نرم‌افزارها و خدمات غیرضروری نباشند و دسترسی آن‌ها به سطح کاربری تعریف‌شده برایشان محدود گردد. این مسائل موجب کاهش خسارات و صدمات ناخواسته‌ای است که استفاده بدون محدودیت از اینترنت می‌تواند به دنبال داشته باشد. سازوکارهای ذکرشده در شکل ۱ قابل‌بررسی می‌باشند.

۴-۲- نمودار علت و معلولی سطح امنیت

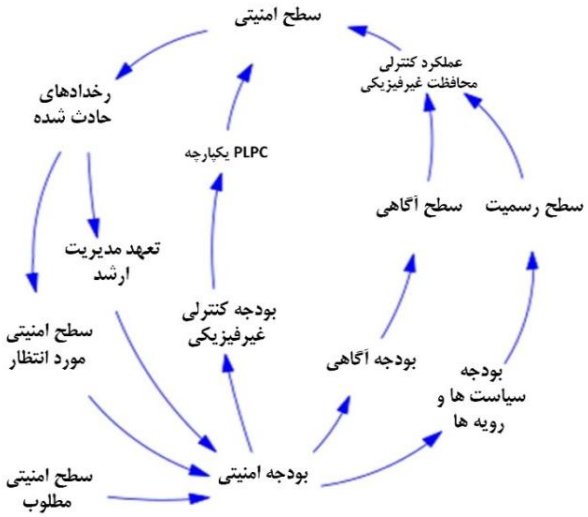
شکل ۲، حلقه‌های علی و معلولی مرتبط با سطح امنیت را نشان می‌دهد. سطح امنیت سیستم اطلاعاتی یکی از مهم‌ترین متغیرهای موجود در سیستم است که سطح پایین آن موجب افزایش حوادث امنیتی می‌شود. این مسئله موجب تقویت تعهد مدیریت ارشد به مسائل حفاظتی و تخصیص بودجه بیشتر به این بخش می‌گردد. شکاف امنیتی که حاصل تفاضل وضع مطلوب و وضع موجود امنیت سیستم اطلاعاتی است هم در بودجه‌بندی ایمنی از سوی مدیریت ارشد تأثیرگذار است. با افزایش بودجه امنیتی، بودجه مربوط به این حوزه به‌خصوص بودجه خط‌مشی‌ها و رویه‌های ایمنی، بودجه آگاه‌سازی کارکنان از خطرات و ریسک‌های سیستم‌های اطلاعاتی و بودجه کنترل حفاظت منطقی صرف بهبود عملکرد سیستم و افزایش سطح امنیتی آن خواهد شد.

۴-۳- نمودار علت و معلولی قابلیت کشف اختلال

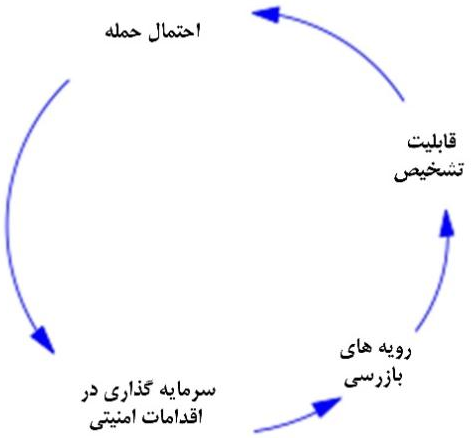
افزایش سرمایه‌گذاری بر روی شاخص‌های امنیتی موجب بهبود رویه‌های کشف اختلال در سیستم اطلاعاتی می‌شود. با بهبود این رویه‌ها، قابلیت‌های سازمان در کشف اختلال افزایش می‌یابد. انتظار می‌رود که این افزایش منجر به کاهش احتمال حمله از سوی هکرها گردد. این روابط از طریق سازوکار ذکرشده در شکل ۳ نمایش داده‌شده است.



شکل ۱. حلقه‌های علی و معلولی آسیب‌های نیروی انسانی



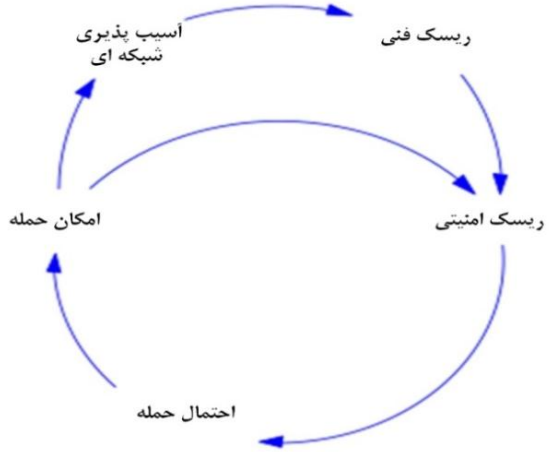
شکل ۲. حلقه‌های علت و معلولی سطح امنیت



شکل ۳. حلقه‌های علت و معلولی قابلیت کشف اختلال

۴-۴- نمودار علت و معلولی حمله سایبری

افزایش امکان حمله سایبری از سوی هکرها، امکان حمله را افزایش می‌دهد و این مساله، آسیب‌پذیری بیشتر شبکه را به دنبال دارد که خود منجر به افزایش ریسک فنی می‌گردد. با افزایش ریسک فنی، ریسک امنیتی سیستم افزایش پیدا می‌کند که افزایش احتمال حمله سایبری را به دنبال دارد. بعلاوه، افزایش امکان حمله سایبری از سوی هکرها، امکان حمله را افزایش می‌دهد که ریسک امنیتی سیستم را بالا برده و مجدداً موجب افزایش امکان حمله سایبری از سوی هکرها می‌شود. فرضیه پویای ارائه شده در قالب شکل ۴ نمایش داده‌شده است.



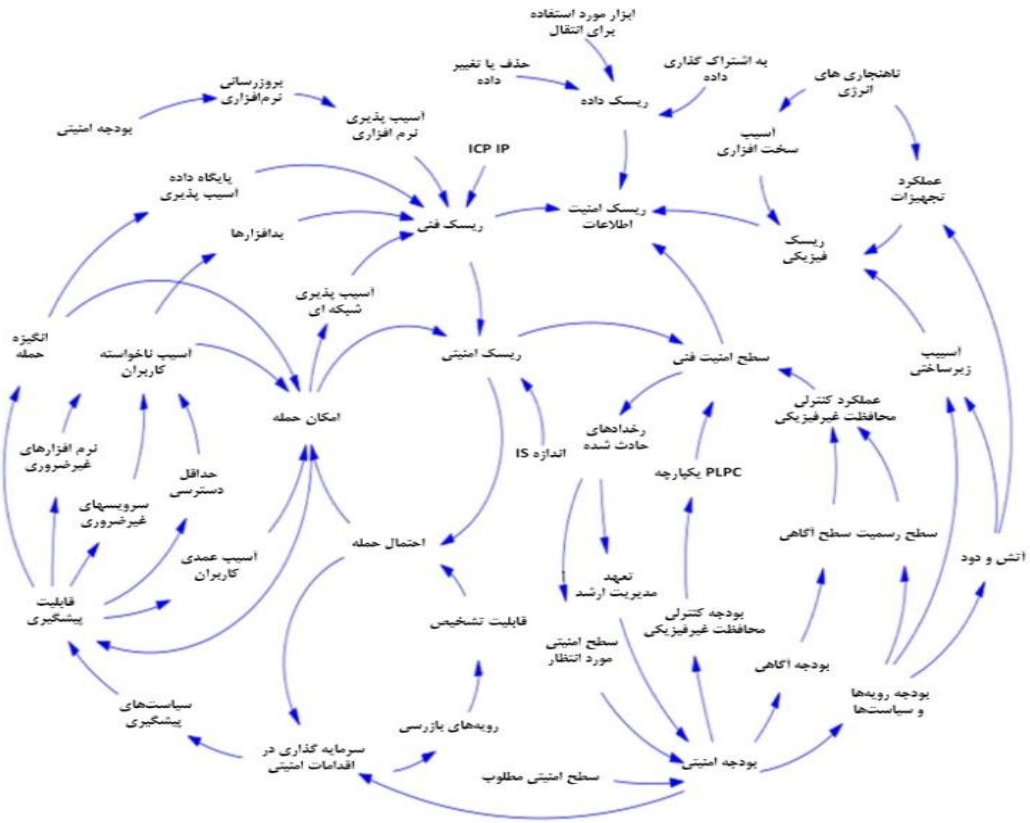
شکل ۴. نمودار علت و معلولی کارایی حمله سایبری

۴-۵- نمودار علت و معلولی امنیت سیستم اطلاعاتی

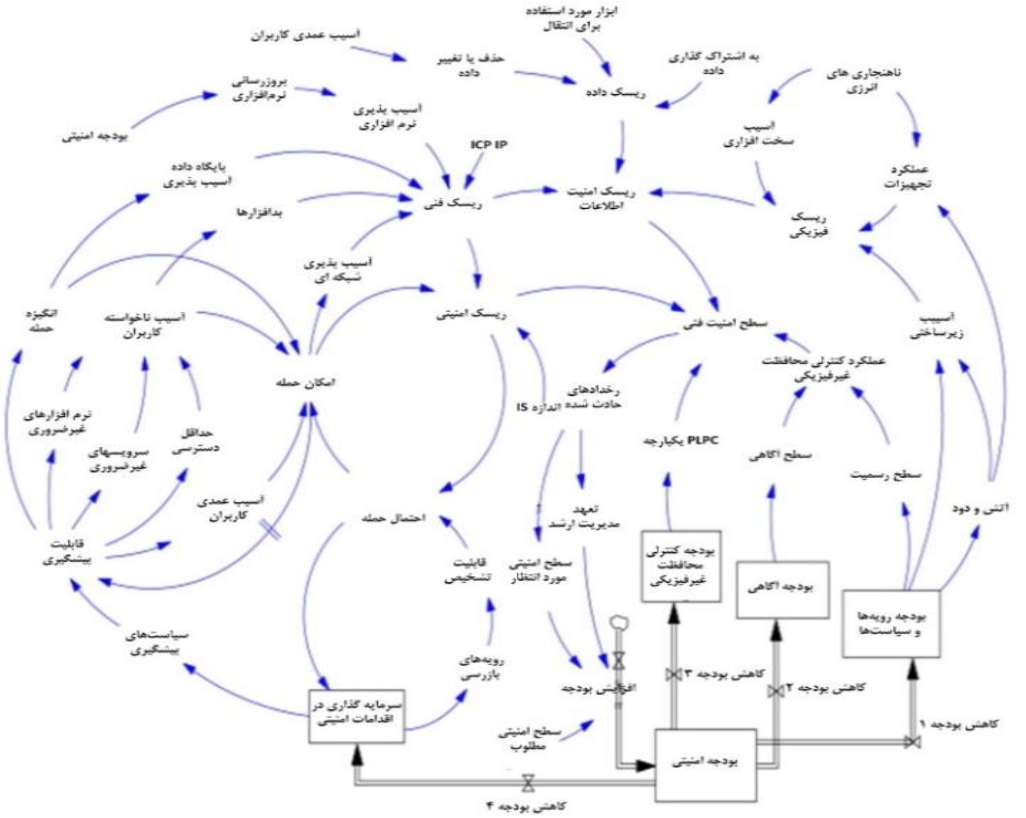
با توجه به نمودارهای علت و معلولی نمایش داده‌شده در بخش‌های قبل، نمودار علت و معلولی پژوهش تشکیل می‌شود که در شکل ۵ نشان داده‌شده است.

۴-۶- نمودار جریان و موجودی

به‌منظور ترسیم نمودار جریان- موجودی ضرورت دارد تا متغیرهای بکار رفته در شکل ۵ در قالب متغیرهای نرخ، موجودی، کمکی و مقادیر ثابت، تقسیم‌بندی شوند. پس از بررسی متغیرهای مدل علت و معلولی و مشورت با خبرگان موضوع، متغیرهای مدل به‌صورت ذکرشده در جدول ۳ دسته‌بندی گردیدند. بر این اساس، مدل نهایی پژوهش دارای ۴ متغیر موجودی، ۵ متغیر نرخ و ۳۹ متغیر کمکی (شامل متغیرهای واسطه و توابع جدولی) و ۴ ثابت است که در شکل ۶ نمایش داده‌شده است.



شکل ۵. نمودار علت و معلولی پژوهش



شکل ۶. مدل موجودی- جریان امنیت اطلاعات

جدول ۳. متغیرهای مدل تحقیق

تغیر	ماهیت	متغیر	ماهیت
انگیزه حمله	کمکی	احتمال حمله	کمکی
توانایی پیشگیری	کمکی	ریسک امنیت شبکه	کمکی
نرم‌افزارهای غیرضروری	کمکی	اندازه سیستم اطلاعاتی	ثابت
خدمات غیرضروری	کمکی	قابلیت کشف	کمکی
حداقل دسترسی	کمکی	رویه بازرسی	کمکی
آسیب عمدی کاربران	کمکی	سرمایه‌گذاری بر روی معیارهای امنیت	کمکی
آسیب غیرعمدی کاربران	کمکی	سیاست‌های پیشگیرانه	کمکی
امکان‌پذیری حمله	کمکی	سطح امنیت	کمکی
آسیب‌پذیری پایگاه داده	کمکی	عملکرد کنترل حفاظت منطقی	کمکی
بدافزارها	کمکی	سطح رسمیت	کمکی
به‌روزرسانی نرم‌افزار	کمکی	سطح آگاهی	کمکی
آسیب‌پذیری نرم‌افزار	کمکی	عملکرد کنترل حفاظت یکپارچه	کمکی
پروتکل کنترل انتقال	کمکی	رویدادهای ناخوشایند	کمکی
آسیب‌پذیری شبکه	کمکی	تعهد مدیریت ارشد	کمکی
ریسک فنی	کمکی	سطح امنیت ادراک‌شده	کمکی
حذف یا تغییر داده‌ها	کمکی	بودجه کنترل حفاظت منطقی	موجودی
محیط انتقال	**ثابت**	بودجه آگاهی	موجودی
به اشتراک‌گذاری داده‌ها	**ثابت**	بودجه سیاست‌ها و رویه‌ها	موجودی
ریسک داده‌ها	کمکی	سطح امنیت مطلوب	کمکی
نوسانات انرژی	کمکی	افزایش بودجه	جریان
آسیب سخت‌افزاری	کمکی	سطح امنیت مطلوب	ثابت
عملکرد تجهیزات	کمکی	بودجه امنیتی	موجودی
ریسک فیزیکی	کمکی	کاهش بودجه ۱	جریان
آسیب زیرساخت‌ها	کمکی	کاهش بودجه ۲	جریان
سیگار و آتش	کمکی	کاهش بودجه ۳	جریان
ریسک امنیت اطلاعات	کمکی	کاهش بودجه ۴	جریان

۴-۷- آزمون‌های اعتبار ساختاری مدل

در این آزمون‌ها اعتبار مدل از جهت تناظر ساختار، اجزا و عناصر آن با سیستم واقعی مورد آزمون قرار می‌گیرد. در این تحقیق با توجه به عدم امکان افشای داده‌های دقیق در مورد سیستم امنیت بانک، از دو روش اعتبارسنجی ساختار مدل با استفاده از نظرات خبرگان و آزمون ساختاری شرایط حدی استفاده‌شده است.

۴-۷-۱- آزمون کفایت مرزهای مدل

آزمون کفایت مرزها، تناسب مرزهای مدل را بر اساس هدف طراحی آن مورد آزمون قرار می‌دهد. به‌عبارت‌دیگر حدود مدل باید با هدف طراحی آن هماهنگ باشد و همه عوامل و بخش‌های مؤثر بر رفتار متغیر موردبررسی را در برگیرد و تعریف متغیرهای درون‌زا و برون‌زا متناسب با اهداف مدل باشد. این جنبه از اعتبارسنجی مدل، کیفی است و از طریق مطالعه دیاگرام‌ها و نمودارهای جریان توسط صاحب‌نظران و خبرگان میسر می‌گردد. بدین منظور نمودار حالت-جریان برای مشارکت‌کنندگان پژوهش شرح داده شد و با تعدیلاتی مدل نهایی مورد تأیید قرار گرفت.

۴-۷-۲- آزمون سازگاری ابعاد

برای آزمون ساختاری مدل، صحت ابعاد لحاظ شده برای متغیرهای مختلف در نمودارهای جریان که از طریق روابط ریاضی به‌صورت زنجیروار به همدیگر وابسته‌اند، توسط نرم‌افزار **Vensim** مورد ارزیابی قرار گرفت و صحت روابط تعریف‌شده در مدل موجودی- جریان تائید گردید.

۴-۸- آزمون‌های اعتبار رفتاری مدل

۴-۸-۱- آزمون خطای انتگرال‌گیری

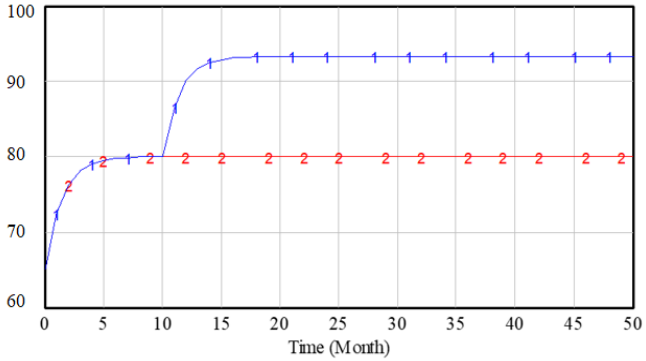
آزمون خطای انتگرال‌گیری منظور تأیید تناسب گام زمانی مدل برقرار می‌شود. بر این اساس علاوه بر شبیه‌سازی اولیه که با ۳ گام زمانی سالیانه صورت گرفت، شبیه‌سازی دیگری با گام‌های شش‌ماهه اجرا و نتایج برای چند متغیر اصلی مورد مقایسه قرار گرفت. بر اساس نتایج مدل، در هر دو مورد رفتار متغیرهای اصلی مشابه هستند و خطای انتگرال‌گیری قابل‌چشم‌پوشی است. جهت انجام اعتبارسنجی اول، از نظرات دو خبره که سابقه فعالیت به‌عنوان مدیر فناوری بانک کشاورزی را داشته‌اند، استفاده‌شده است که ساختار علی و معلولی مدل و توابع مورداستفاده در مدل و همچنین رفتار شبیه‌سازی مورد تأیید آن‌ها قرار گرفت.

۴-۸-۲- آزمون بازتولید رفتار

در این آزمون رفتار حاصل‌شده از شبیه‌سازی متغیرهای اصلی با رفتار مرجع آن‌ها مقایسه شده و در صورت اندک بودن درصد خطا می‌توان ادعا کرد که مدل از اعتبار رفتاری برخوردار است. بدین منظور نتایج حاصل از شبیه‌سازی برخی متغیرها را با مقادیر پیش‌بینی‌شده به روش سری زمانی استخراج‌شده از داده‌ها، مقایسه نمودیم. شاخص **RMSPE** یکی از روش‌های آماری تأیید رفتار مدل است که اختلاف داده‌های واقعی **(At)** و داده‌های شبیه‌سازی‌شده **(St)** را نشان می‌دهد. برای تأیید رفتار سیستم این شاخص باید کمتر از ۰/۱ باشد. با توجه به محاسبات انجام‌شده مقدار شاخص **RMSPE** در این شبیه‌سازی ۰/۰۴ به دست آمد که مقداری کمتر از ۰/۱ دارد و اعتبار رفتاری مدل را تأیید می‌کند.

۴-۹- آزمون تحلیل حساسیت مدل

برای ارزیابی تحلیل حساسیت در نرم‌افزار ونسیم در نمودارهای جریان، چند شبیه‌سازی با تغییرات ناگهانی و شدید در برخی پارامترهای مدل صورت پذیرفت تا صحت واکنش مدل نسبت به این تغییرات مورد بررسی قرار گیرد. به‌عنوان نمونه اگر در حالت مدل پایه، بودجه ایمنی افزایش پیدا کند، سرمایه‌گذاری در بخش‌های سیاست‌ها و رویه‌های امنیت، آگاه‌سازی کارکنان از اصول امنیتی و تبعات عدم رعایت آن‌ها، مسائل حفاظتی و افزایش می‌یابد که این مساله تأثیر فراوانی بر روی سطح امنیت دارد. چنانچه در ماه دهم، بودجه ایمنی از ۱۰۰۰ واحد به ۱۵۰۰ واحد افزایش یابد، سطح ایمنی به حدوداً ۹۵ درصد افزایش خواهد یافت. الگوی این تغییر در شکل ۷ نشان داده‌شده است. الگوی پایه با رنگ قرمز نشان داده‌شده است.



شکل ۷. تحلیل حساسیت متغیر سطح امنیت

۴-۱۰- ارزیابی امنیت سیستم‌های اطلاعاتی

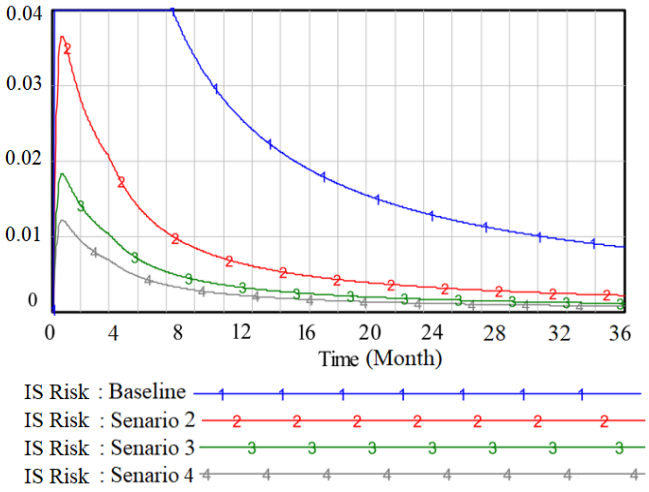
با پشت سر گذاشتن موفقیت‌آمیز آزمون‌های سازگاری ابعاد و ساختار مدل در نرم‌افزار **Vensim** می‌توان شبیه‌سازی اولیه مدل را انجام داد. در این بخش، نمودار تغییرات متغیر ریسک سیستم اطلاعاتی به‌عنوان مهم‌ترین متغیر سیستم در شرایط تغییر متغیرهای مختلف مدل، ارائه می‌شوند.

۱. سناریوی پایه: شبیه‌سازی وضعیت جاری سیستم بدون دست‌کاری در متغیرهای مدل.

۲. سناریوی افزایش بودجه سیاست‌ها و رویه‌ها: در این سناریو، بودجه تخصیص‌یافته به توسعه و به‌روزرسانی سیاست‌ها و رویه‌های امنیتی بانک به میزان ۵ درصد افزایش می‌یابد. هدف اصلی از این سناریو، بررسی تأثیر افزایش بودجه در بهبود امنیت سیستم‌های اطلاعاتی از طریق تقویت سیاست‌ها و پروتکل‌های امنیتی است. با افزایش بودجه، بانک قادر خواهد بود سیاست‌ها و رویه‌های امنیتی موجود را بازنگری کرده و پروتکل‌های جدیدی را برای مقابله با تهدیدات نوظهور تدوین کند. این شامل به‌روزرسانی قوانین مربوط به دسترسی کاربران، مدیریت داده‌ها و نحوه برخورد با رخدادهای امنیتی است.

۳. سناریوی ارتقاء آگاهی کارکنان: در این سناریو، با افزایش بودجه آگاه‌سازی به میزان ۱۰ درصد، تمرکز بر افزایش آموزش‌ها و برنامه‌های آگاهی‌بخشی امنیتی برای کارکنان و کاربران سیستم اطلاعاتی بانک است. هدف بررسی تأثیر افزایش آگاهی و دانش امنیتی بر کاهش ریسک‌های انسانی، خطاهای کاربری و نقض امنیتی است.

۴. سناریوی افزایش بودجه امنیتی: در این سناریو، بودجه تخصیص‌یافته به امنیت اطلاعات به میزان ۵ درصد افزایش می‌یابد. این افزایش می‌تواند بر عواملی نظیر به‌روزرسانی نرم‌افزارها، آموزش کارکنان و اجرای پروتکل‌های امنیتی تأثیر بگذارد. هدف این سناریو بررسی تأثیرات مستقیم و غیرمستقیم افزایش بودجه بر ریسک سیستم اطلاعاتی بانک است. شکل ۸ نتایج اجرای هر یک از این سناریوها را نشان می‌دهد.



شکل ۸. بررسی اثر پیاده‌سازی سناریوها بر ریسک سیستم اطلاعاتی

بر اساس نتایج حاصل از شبیه‌سازی در شکل ۸، سناریوهای چهارم، سوم و دوم به ترتیب بیشترین کاهش ریسک را در افق زمانی ۳۶ ماهه برای سیستم اطلاعاتی بانک به همراه خواهند داشت و اولویت‌بندی اثربخشی سناریوهای مطرح‌شده را مشخص می‌کنند.

در سناریوی پایه، سطح ریسک امنیت اطلاعات در طول زمان کاهش می‌یابد و به حدود ۸۰ درصد در پایان دوره ۳۶ ماهه می‌رسد.

با اجرای سناریوی ۴ (افزایش بودجه توسعه رویه‌های امنیتی بانک

به میزان ۵ درصد)، انتظار می‌رود سطح ریسک سیستم اطلاعاتی بانک در افق زمانی ۳۶ ماهه به پایین‌تر از ۰/۰۰۱ کاهش یابد. درحالی‌که با اجرای سناریوی ۳ (ارتقای بودجه آموزش و آگاه‌سازی کارکنان و کاربران سیستم به میزان ۱۰ درصد)، انتظار می‌رود سطح ریسک سیستم اطلاعاتی در افق ۳۶ ماهه به پایین‌تر از ۰/۰۱ کاهش یابد. در این سناریو، سطح امنیت اطلاعات افزایش می‌یابد، اما این افزایش کمتر از سناریوی افزایش بودجه امنیتی است. این نشان می‌دهد که ارتقاء آگاهی کارکنان یک عامل مهم در بهبود امنیت است، اما به‌تنهایی کافی نیست و باید با سایر اقدامات امنیتی همراه باشد. این یافته با نتایج مطالعات اخیر هم‌راستا است که تأکید دارند که افزایش هدفمند بودجه امنیتی و ارتقای مستمر آگاهی کارکنان، بیشترین نقش را در کاهش ریسک امنیت اطلاعاتی و افزایش تاب‌آوری بانک‌ها در برابر تهدیدات سایبری و عملیاتی ایفا می‌کند [۱۶ و ۲۴].

۵- نتیجه‌گیری و پیشنهادها

این پژوهش با هدف ارزیابی و تحلیل اثربخشی سناریوهای مختلف بهبود امنیت سیستم‌های اطلاعاتی بانک کشاورزی با استفاده از رویکرد پویایی‌شناسی سیستم‌ها انجام گردید. نتایج نشان داد که تخصیص بهینه منابع با اولویت‌دهی به توسعه رویه‌های امنیتی و زیرساخت‌های فنی (سناریو ۴)، بیشترین تأثیر را در کاهش ریسک در بازه زمانی ۳۶ ماهه دارد و سطح ریسک را به کمتر از ۰/۰۰۱ می‌رساند. درعین‌حال، ارتقاء آگاهی و آموزش کارکنان (سناریو ۳) نیز نقش مهمی در بهبود امنیت ایفا می‌کند اما تأثیر آن به‌تنهایی کمتر از سرمایه‌گذاری در زیرساخت‌های امنیتی است و سطح ریسک را به کمتر از ۰/۰۱ می‌رساند. در سناریوی پایه (وضعیت فعلی)، سطح ریسک در پایان دوره ۳۶ ماهه به حدود ۸۰٪ کاهش می‌یابد. این یافته‌ها بر اهمیت تلفیق سرمایه‌گذاری در فناوری‌های نوین و نیروی انسانی آگاه در راستای دستیابی به امنیت پایدار تأکید دارد.

بر اساس نتایج پژوهش، پیشنهاد می‌شود بانک کشاورزی به‌جای افزایش کلی بودجه امنیتی، بخش عمده‌ای از منابع خود را به تقویت زیرساخت‌های حیاتی مانند مراکز داده و سرورهای اصلی، استقرار تجهیزات برق اضطراری و توسعه سامانه‌های پشتیبان اختصاص دهد تا تاب‌آوری بانک در برابر نوسانات انرژی و بلایای طبیعی به شکل هدفمند ارتقا یابد. همچنین، لازم است دوره‌های آموزشی امنیت اطلاعات به‌طور تخصصی برای کارکنان فناوری اطلاعات، مدیران شعب و کارکنان بخش‌های حساس برگزار شود و در این آموزش‌ها سناریوهای واقعی تهدیدات نظیر فیشینگ و مهندسی اجتماعی شبیه‌سازی گردد تا سطح آمادگی عملیاتی افزایش یابد. به‌کارگیری سامانه‌های هوشمند مدیریت رویداد و اطلاعات امنیتی **(SIEM)** و ابزارهای مبتنی بر هوش مصنوعی برای پایش لحظه‌ای ترافیک شبکه و شناسایی رفتارهای غیرعادی، امکان کشف سریع تهدیدات و واکنش مؤثر به رخدادهای امنیتی را فراهم می‌کند. همچنین، تدوین و اجرای برنامه منظم برای به‌روزرسانی سیستم‌عامل‌ها، نرم‌افزارهای کاربردی و پروتکل‌های ارتباطی (مانند جایگزینی پروتکل‌های ناامن با **TLS**) و انجام تست نفوذ حداقل هر شش ماه یک‌بار، ضروری است. در حوزه امنیت فیزیکی، استفاده از سامانه‌های کنترل دسترسی بیومتریک، دوربین‌های مداربسته با قابلیت تحلیل تصویر و سامانه‌های هشداردهنده هوشمند جهت حفاظت از زیرساخت‌های حیاتی بانک توصیه می‌شود. علاوه بر این، برگزاری مانورهای دوره‌ای برای شبیه‌سازی رخدادهای امنیتی مانند قطع برق، حمله سایبری یا نفوذ فیزیکی، به ارزیابی آمادگی تیم‌های عملیاتی و بهبود فرآیندهای واکنش اضطراری کمک می‌کند. درنهایت، ایجاد کانال ارتباطی مستقیم با مراکز هشداردهی تهدیدات سایبری و دریافت هشدارهای به‌روز، بانک را در مقابله سریع و مؤثر با تهدیدات نوظهور یاری خواهد کرد.

یکی از محدودیت‌های اساسی شبیه‌سازی در این پژوهش، وجود عدم قطعیت نسبت به مقادیر دقیق پارامترهای مدل بوده است. به‌منظور کاهش این عدم قطعیت و افزایش اعتبار مدل، داده‌های تاریخی بانک و نظرات کارشناسان برای کالیبراسیون پارامترها مورداستفاده قرارگرفته است. بااین‌حال، تحلیل حساسیت صرفاً بر متغیرهای اصلی مدل متمرکزشده و سایر عوامل تأثیرگذار، ازجمله اثربخشی تجهیزات پشتیبان، نرخ به‌روزرسانی نرم‌افزارها و سیاست‌های دسترسی کاربران، در این تحلیل لحاظ نشده‌اند. بر این اساس، پیشنهاد می‌شود پژوهش‌های آتی با گسترش دامنه تحلیل حساسیت، متغیرهای بیشتری را به‌صورت منفرد و ترکیبی موردبررسی قرار دهند و از روش‌های پیشرفته‌تری مانند تحلیل حساسیت جهانی یا سناریوهای چندمتغیره بهره ببرند. همچنین، مدل‌سازی و ارزیابی اثر شوک‌های محیطی نظیر قطع برق یا حملات فیزیکی می‌تواند به ارائه تصویری جامع‌تر از رفتار سیستم در شرایط بحرانی منجر شود و اعتبار نتایج را افزایش دهد.

مراجع

[1] Moore, A., & Warkentin, M. “Cybersecurity: Principles and Practices”. Pearson.2019.

[2] Osmanbegović, E., Piric, N., & Suljic, M. “Information Security Controls As Determinant Of Continuity Of Information System Work”. Vol. XV, Issue 2, 35-42, 2017.

[3] Böhme, R., & Moore, T. (2023). The Economics of Cybersecurity: Principles and Policy Options. Annual Review of Economics, 15, 567-592.

[4] Bock, S. “Human Error and Cybersecurity in the Banking Sector”. Journal of Banking Technology, 15(2), 123-135.2021.

[5] Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2023). A Human-Centric Risk-Based Investment Model for Information Security: Empirical Evidence from the Financial Sector. Computers & Security, 128, 103234.

[6] Lubua, E.W., Semlambo, A.A., & Mkude, C.G. “Factors Affecting the Security of Information Systems in Africa: A Literature Review”. University of Dar es Salaam Library Journal, 17(2), 94-114.2022.

[7] Alizadeh, A., Chehrehpak, M., Nasr, A.K., & Zamanifard, S. “An empirical study on effective factors on adoption of cloud computing in electronic banking: a case study of Iran banking sector”. Int. J. Bus. Inf. Syst., 33, 408-428.2020.

[8] Khan, H. U., Malik, M. Z., Nazir, S. , and Khan,F., "Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis," in IEEE Access, vol. 11, pp. 80181-80198.2023.

[9] Rapina, R., Carolina, Y., Setiawan, S., Gania, A., Sandra, L.M., Darmasetiawan, J.B., & Fuentes, R.O. “Empirical Study on Banking in Indonesia: Factors Affecting Information Systems Quality”. Proceedings of the 2020 12th International Conference on Information Management and Engineering. 2020.

[10] Alsalamah, A. “Security Risk Management in Online System”. 5th Intl Conf on Applied Computing and Information Technology/4th Intl Conf on Computational Science/Intelligence and Applied Informatics/2nd Intl Conf on Big Data, Cloud Computing, Data Science (ACIT-CSII-BCD), 119-124.2017.

[11] Lestari, D., Tama, A., Karlina, S., Sultan, A., & Tarwoto, T. “Factors Affecting Security Information Systems: Information Security, Threats and Cyber Attack, Physical Security, and Information Technology”. International Journal of Informatics and Information Systems, 7(1), 16-21.2024.

[12] Noubissi, A.C., Iguchi-Cartigny, J., & Lanet, J. “Hot updates for Java based smart cards”. IEEE 27th International Conference on Data Engineering Workshops, 168-173.2011.

[13] Putra Utama, F., & Hilmi Nurhadi, R.M. “Uncovering the Risk of Academic Information System Vulnerability through PTES and OWASP Method”, COMMIT (Communication and Information Technology) Journal. 18(1), 39-51.2024.

[14] Smith, J. (2023). The Role of Artificial Intelligence in Banking Risk Management. Journal of Banking and Finance, 134, 1-10.

[15] Rajendran, S. R., N. F., Dipu, Tarek, S., H. M., Kamali, Farahmandi F. and Tehranipoor, M., "Exploring the Abyss? Unveiling Systems-on-Chip Hardware Vulnerabilities Beneath Software," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 3914-3926, 2024.

[16] ENISA (European Union Agency for Cybersecurity). (2022). Threat Landscape for Information Integrity in Financial Services.

[17] Duddu, S., Rishita sai, A., Sowjanya, C.L., Rao, G.R., & Siddabattula, K. (2020). Secure Socket Layer Stripping Attack Using Address Resolution Protocol Spoofing. 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 973-978.

[18] Gai, K., Qiu, M., & Qiu, L. (2022). Security and Privacy Issues: A Survey on FinTech in Banking Systems. Future Generation Computer Systems, *135*, 386-399.

[19] Brown, L., & Green, T. (2022). The Impact of Data Types on Cyber Threats in Financial Institutions. International Journal of Cyber Studies, 9(2), 123-139.

[20] Li, Z., Xu, W., Shi, H., Zhang, Y., & Yan, Y. “Security and Privacy Risk Assessment of Energy Big Data in Cloud Environment”. Computational intelligence and neuroscience, 2398460. 2021. https://doi.org/10.1155/2021/2398460 (Retraction published Comput Intell Neurosci. 2023 Oct 18; 2023:9896475. doi: 10.1155/2023/9896475).

[21] Blesswin, J., Mary, S.J., Suryawanshi, S., Kshirsagar, V.G., Pabalkar, S.Y., Venkatesan, M., & Karunya, C.E. “Secure transmission of grayscale images with triggered error visual sharing”. Journal of Autonomous Intelligence. 2023.

[۲۲] اکبرنژاد، ابوالقاسم و چشک، کریم، "اولویت‌بندی مؤلفه‌های اثرگذار بر سیاست دفاعی- امنیتی جمهوری اسلامی ایران". ۱۳۹۹

[۲۳] جلالی، محمد و افشاری، مریم و مزینانیان، زینب،"تأثیر ابعاد زیست‌محیطی تغییرات اقلیمی بر امنیت ملی". ۱۳۹۹.

[24] Alsmadi, I., & Zarour, M. (2023). Cybersecurity in Banking: Risks, Challenges, and Solutions. Journal of Banking and Financial Technology, 7(1), 21-34.

[۲۵] خون جوش, ف.خ. و عاشوری, م. "بررسی تأثیر تنظیمات پارامترهای سخت‌افزاری بر انرژی مصرفی در الگوریتم ضرب برداری ماتریس‌های تنک بر روی پردازنده‌های گرافیکی" فصلنامه فناوری اطلاعات و ارتباطات ایران، (۹)۳۱، ۷۸-۶۷. ۱۳۹۸.

[26] Lee, S. Y. (2022). Physical Security Threats to Banking Information Systems. Journal of Financial Risk Management, 11(3), 1-12.

[27] Hassan, R., Bandi, C., Tsai, M., Golchin, S., P D, S.M., Rafatirad, S., & Salehi, S. (2023). Automated Supervised Topic Modeling Framework for Hardware Weaknesses. 2023 24th International Symposium on Quality Electronic Design (ISQED), 1-8.

[28] Shehab, R., s.alismail, A., Amin Almaiah, D.M., Alkhdour, D.T., AlWadi, D.B., & Alrawad, D.M. “Assessment of Cybersecurity Risks and threats on Banking and Financial Services. Journal of Internet Services and Information Security” 14(3), 167-190.2024.

[29] White, R., & Black, S. “Historical Cyber Attacks and Their Future Implications for Banks. Cybersecurity Review”, 15(1), 88-102.2023.

[30] Shams, S., & Soltanifar, M. (2023). The Impact of Cyberattacks on Customer Trust in the Banking Sector: Evidence from Emerging Markets. Journal of Financial Crime, 30(2), 545-562.

[31] Lavanya, M., & Mangayarkarasi, D.S. “A Review on Detection of Cybersecurity Threats in Banking Sectors Using AI Based Risk Assessment”. Journal of Electrical Systems. Vol. 20 No. 6s, 1359-1365.2024.

[32] Dawodu, S.O., Omotosho, A., Akindote, O.J., Adegbite, A.O., & Ewuga, S.K. “CYBERSECURITY RISK ASSESSMENT IN BANKING: METHODOLOGIES AND BEST PRACTICES”. Computer Science & IT Research Journal, 4(3), 220-243. 2023.

[۳۳] عزیزی سرخانی, محمدجواد و کردلوئی, حمیدرضا. "بررسی ابزارهای امنیتی بانکداری الکترونیک در بخش بانکداری دولتی بانک‌های هند با مروری بر جهانی شدن". دانش سرمایه‌گذاری، (۱۸) ۵، ۲۶۲-۲۵۳، ۱۳۹۵.

[۳۴] فرزام نیا، نیما، عبدی, بهنام و رضائیان، علی. "ارائه الگوی حکمرانی خوب امنیت فضای سایبری در سازمان‌های دفاعی"، فصلنامه مدیریت نظامی، (۷۷)۲۰، ۸۱-۱۲۰. ۱۳۹۹.

[35] Dhanya, C., & Ramya, K. “Impact of System-Level Indicators of Chatbots on Perceived Usefulness and Intention to use for Banking

Services". The Review of Finance and Banking, 16(1), 43-55.2024.

[36] Fatoki, J.O. "The influence of cyber security on financial fraud in the Nigerian banking industry". International Journal of Science and Research Archive, 9(02), 503–515.2023.

[۳۷] شفیعی نیک‌آبادی، محسن، حکاکی، امیر و غلامشاهی، سارا. "مدلی پویا جهت ارزیابی امنیت سیستم‌های اطلاعاتی با استفاده از رویکرد پویایی‌شناسی سیستم‌ها" ، فصلنامه رشد فناوری، (۱۶)۶۴، ۶۱-۵۲. ۱۳۹۹.

[38] Damenu, T.K., & Beaumont, C. "Analysing information security in a bank using soft systems methodology". Inf. Comput. Secur., 25, 240-258.2017.

[39] Cheng, L., Liu, F., Yao, D., & Wang, X. (2022). ATM Security: Threats, Vulnerabilities, and Countermeasures in the Era of Digital Banking. Computers & Security, 119, 102765.

[40] Sarumi, J.A., Longe, O.B., & Adelodun, F.O. "An Empirical Evaluation of the Effectiveness of the Computer-Based Network Security and Firewall in Banking Systems". Advances in Multidisciplinary and scientific Research Journal Publication, 10(1), 21-33. 2022.

[41] Ewuga, S.K., Egieya, Z.E., Omotosho, A., & Adegbite, A.O. "ISO 27001 IN BANKING: AN EVALUATION OF ITS IMPLEMENTATION AND EFFECTIVENESS IN ENHANCING INFORMATION SECURITY". Finance & Accounting Research Journal, 5(12), 405-426.2024.

[42] Somogyi, T., & Nagy, R. "The Impact of the War in Ukraine on the Information Security of the European Union's Banking Industry – A Case Study of Hungary And Slovakia". CONTEMPORARY MILITARY CHALLENGES, 25, 23 - 32. 2023.

[43] Al-Hadhrami, A., Alghamdi, A., & Alfarraj, O. (2022). Perceived Security Threats and Their Impact on the Adoption of Accounting Information Systems in the Banking Sector. Journal of Information Security and Applications, 68, 103236.

[44] Zhou, Y., Li, X., & Wang, J. (2023). Security Assessment and Vulnerability Analysis of Online Banking Systems: Recent Advances and Challenges. Computers & Security, 126, 103140.

[45] Pérez, J., et al. "Risk Assessment of Cloud Migration in Banking Sector." Journal of Financial Services Technology.2020.

[۴۶] پیکری، حمیدرضا و بنازاده، بابک. "رابطهٔ آگاهی از امنیت اطلاعات با قصد نقض امنیت اطلاعات با نقش میانجی هنجارهای فردی و خودکنترلی عنوان مکرر: قصد نقض امنیت اطلاعات". پژوهش‌های راهبردی مسائل اجتماعی، (۴)۷، ۴۱-۵۸، ۱۳۹۷.

[47] Zhou, Y., Li, X., & Wang, J. (2023). Security Assessment and Vulnerability Analysis of Online Banking Systems: Recent Advances and Challenges. Computers & Security, 126, 103140.