فصلنامه چشم انداز حسابداری و مدیریت
دوره ۸، شماره ۱۰۶، پاییز ۱۴۰۴(جلد اول)
www.jamv.ir
ISSN: 2645-4572

چشم انداز حسابداری و مدیریت (دوره هشتم)
شماره ۱۰۶ / پاییز ۱۴۰۴ (جلد اول)/ صص ۱۶۷-۱۷۸

طراحی الگوی بومی امنیت شبکه بانکی ایران با رویکرد پیشگیری از تهدیدات سایبری نوظهور و تأثیر آن بر پایداری مالی بانک‌ها

دکتر جواد عین آبادی
استادیار گروه مالی و حسابداری، موسسه آموزش عالی الکترونیکی ایرانیان، تهران، ایران.
javadeinabadi@gmail.com
وحید احمری
دانشجوی کارشناسی ارشد مالی- حقوق مالی، موسسه آموزش عالی الکترونیکی ایرانیان، تهران، ایران. (نویسنده مسئول).
vahid.ahmari.14031@gmail.com

چکیده
تحول دیجیتال در نظام بانکی ایران با وجود ایجاد فرصت‌های گسترده، سطح تهدیدات سایبری را به‌طور چشمگیری افزایش داده و نیاز به طراحی الگوهای بومی امنیت سایبری را تشدید کرده است. این پژوهش با هدف طراحی و ارزیابی یک چارچوب بومی امنیت سایبری با رویکرد پیشگیرانه و بررسی تأثیر آن بر تاب‌آوری عملیاتی و پایداری مالی بانک‌ها انجام شد. روش تحقیق توصیفی–تحلیلی و از نظر ماهیت کمی است؛ داده‌ها از طریق پرسشنامه محقق‌ساخته و با مشارکت ۱۰۰ نفر از کارکنان مرتبط با حوزه‌های فناوری اطلاعات، امنیت سایبری و مدیریت بانکی جمع‌آوری شد. پایایی ابزار با ضریب آلفای کرونباخ بین ۰.۸۵ تا ۰.۸۹ تأیید شد. نتایج تحلیل همبستگی پیرسون نشان داد که ابعاد «زیرساخت فناوری»، «اثر مالی حملات سایبری» و «بعد ۶» بیشترین رابطه مثبت و معنادار را با پایداری مالی دارند، در حالی که ابعاد «آموزش و فرهنگ امنیتی»، «سیاست‌ها و مقررات» و «پاسخگویی و مانیتورینگ» فاقد رابطه معنادار بودند. تحلیل رگرسیون چندگانه نیز بیانگر آن بود که مدل پژوهش ۸۵.۱ درصد از واریانس پایداری مالی را تبیین می‌کند و سه بعد یادشده به‌ترتیب بیشترین اثر مستقیم و معنادار را بر پایداری مالی دارند. این نتایج نشان می‌دهد که تقویت زیرساخت‌های فناوری، بهبود سازوکارهای کلیدی پاسخ به حملات و ارتقای فرآیندهای عملیاتی نقش محوری در افزایش تاب‌آوری بانکی و کاهش اثرات مخرب تهدیدات نوظهور دارند. بر اساس یافته‌ها، پیشنهاد می‌شود بانک‌ها تمرکز راهبردی خود را بر ابعاد مؤثرتر قرار داده و الگوی امنیتی خود را بر مبنای معماری پیشگیرانه، تحلیل ریسک پویا و اصول مقاومت عملیاتی بازطراحی کنند.

واژگان کلیدی: امنیت سایبری، بانکداری دیجیتال، پایداری مالی، تاب‌آوری عملیاتی، مدیریت ریسک سایبری.

مقدمه
در دهه‌های اخیر، شتاب فزاینده تحول دیجیتال موجب دگرگونی عمیق در نظام بانکی جهان شده است؛ تحولاتی که شامل گسترش بانکداری دیجیتال، فین‌تک، هوش مصنوعی، رایانش ابری و بلاک‌چین است و فرصت‌هایی کم‌سابقه برای توسعه خدمات مالی ایجاد کرده‌اند (دلویت، ۲۰۲۳؛ مک‌کینزی، ۲۰۲۴). بانک‌های ایرانی نیز همگام با این روند جهانی، به‌طور گسترده به سمت دیجیتالی‌سازی حرکت کرده‌اند و سامانه‌های نوین پرداخت، خدمات آنلاین و زیرساخت‌های مبتنی بر داده را توسعه داده‌اند (بهرامی و همکاران، ۱۴۰۴؛ سهرابی، ۱۴۰۳). با وجود این دستاوردها،

www.jamv.ir
ISSN: 2645-4572

افزایش سطح اتکا به فناوری موجب تشدید تهدیدات سایبری شده و امنیت سایبری را به یکی از عوامل کلیدی اعتماد عمومی و ثبات مالی تبدیل کرده است (اکسنچر، ۲۰۲۴؛ کبیری، ۱۴۰۴).

گزارش‌های اخیر نشان می‌دهند که ایران نیز با امواج جدید حملات سایبری پیچیده مواجه است. مرکز پی‌تی اکسپرت سکیوریتی فعالیت گسترده بدافزارهای بانکی از جمله Dridex و حملات APT را در سال‌های ۲۰۲۱ تا ۲۰۲۴ گزارش کرده است (مرکز امنیتی پی‌تی اکسپرت، ۲۰۲۴). همچنین، حمله گروه موسوم به IRLeaks در سال ۲۰۲۴ که چندین بانک ایرانی را هدف قرار داد، یکی از بزرگ‌ترین رویدادهای سایبری کشور محسوب می‌شود و آسیب‌پذیری ساختار امنیتی نظام بانکی را نمایان کرده است. پولیتیکو، ۲۰۲۴؛ کریمی، ۱۴۰۲. پژوهش‌های داخلی نیز تأکید کرده‌اند که بخش قابل‌توجهی از سامانه‌های بانکی کشور از نظر مدیریت ریسک سایبری در سطح مطلوبی قرار ندارند (نادری و محمودی، ۱۴۰۱؛ نصیری و احمدیان، ۱۴۰۲).

مراکز بین‌المللی همچون صندوق بین‌المللی پول (IMF) و بانک تسویه بین‌المللی (BIS) هشدار داده‌اند که حملات سایبری می‌توانند با ایجاد اختلال در سامانه‌های پرداخت، کاهش اعتماد عمومی، و افزایش هزینه‌های عملیاتی، به تهدیدی جدی برای ثبات مالی تبدیل شوند. صندوق بین‌المللی پول، ۲۰۲۴؛ بانک تسویه بین‌المللی، ۲۰۲۳. گزارش شرکت بیمه سپرده‌های فدرال آمریکا نشان می‌دهد که آسیب‌پذیری سایبری بانک‌ها می‌تواند به بحران نقدینگی، اختلال در خدمات و حتی ورشکستگی مؤسسات مالی منجر شود. بر اساس گزارش‌های آی‌بی‌ام (IBM) و ورایزن(Verizon) ، بخش مالی در سال‌های اخیر یکی از اصلی‌ترین اهداف حملات بوده و خسارت‌های مستقیم و غیرمستقیم آن با شیب صعودی در حال افزایش است (آی‌بی‌ام، ۲۰۲۴؛ ورایزن، ۲۰۲۴).

یکی از ابعاد نوظهور تهدیدات، بهره‌برداری مهاجمان از هوش مصنوعی است. تحقیقات اخیر نشان داده‌اند که حملات مبتنی بر adversarial AI، model evasion و data poisoning می‌توانند به‌طور مؤثری مدل‌های یادگیری ماشین در بانک‌ها را بی‌اثر کنند و موتورهای تشخیص تقلب و تحلیل تراکنش را دور بزنند. مؤسسه ملی استاندارد و فناوری آمریکا (NIST)، ۲۰۲۳؛ کوواچویچ و همکاران، ۲۰۲۴؛ راگاوان، ۲۰۲۳. در کنار تهدیدات خارجی، ضعف‌های داخلی مانند نبود استانداردهای یکپارچه امنیتی، پیچیدگی ساختار نظارتی، و خلأهای قانونی در حوزه بانکداری دیجیتال نیز خطرپذیری بانک‌های ایرانی را افزایش داده‌اند (همیار کارآفرین، ۱۴۰۲؛ کبیری، ۱۴۰۴).

پژوهش‌های داخلی نیز بر ضرورت بازطراحی الگوهای امنیتی تأکید دارند. تحلیل SWOT امنیت اطلاعات در بانک‌های ایران نشان می‌دهد که سازوکارهای موجود با تهدیدات پیچیده و نوظهور تناسب کافی ندارند و نیاز به تدوین الگوهای بومی، مبتنی بر فناوری‌های پیشرفته، احساس می‌شود (آزادسنجری و چهارسوقی، ۱۴۰۳). همچنین مطالعات علم‌سنجی نشان می‌دهند که روند پژوهش در ایران از تمرکز بر امنیت سنتی به‌سمت امنیت مبتنی بر هوش مصنوعی در حال تغییر است (فهیمی‌فر و مومن‌زاده، ۱۴۰۴).

مجموع این شواهد بیانگر وجود یک «شکاف امنیتی سیستمیک» در شبکه بانکی ایران است؛ شکافی که نتیجه ترکیب عوامل فنی (تهدیدات نوظهور)، نهادی (پیچیدگی نظارت)، و حقوقی (فقدان چارچوب جامع امنیت سایبری) است. از این‌رو، ضرورت طراحی یک الگوی بومی امنیت سایبری با رویکرد پیشگیرانه که متناسب با ساختار بانکداری ایران باشد، بیش از هر زمان دیگری احساس می‌شود. چنین الگویی باید مبتنی بر اصول مدرن امنیتی مانند «صفر اعتماد»، «تحلیل ریسک پویا»، «مدل‌سازی تهدید»، و «تقویت مقاومت عملیاتی» باشد (دلویت، ۲۰۲۳؛ انیسا، ۲۰۲۳؛ مجمع جهانی اقتصاد، ۲۰۲۴).

www.jamv.ir
ISSN: 2645-4572

پژوهش حاضر با هدف طراحی الگوی بومی امنیت سایبری شبکه بانکی ایران و ارزیابی تأثیر آن بر پایداری مالی بانک‌ها انجام شده و می‌تواند گامی مؤثر در جهت کاهش آسیب‌پذیری، افزایش تاب‌آوری و ارتقای اعتماد عمومی در نظام مالی کشور باشد.

مبانی نظری

امنیت سایبری در بانکداری دیجیتال

تحول دیجیتال در نظام بانکی با به‌کارگیری فناوری‌هایی مانند سامانه‌های پرداخت آنلاین، موبایل بانکینگ، هوش مصنوعی و بلاک‌چین، فرصت‌های قابل توجهی برای ارتقای خدمات مالی فراهم کرده است (دلوایت، ۱۴۰۲؛ مک‌کینزی، ۱۴۰۳). با این حال، افزایش وابستگی به فناوری، بانک‌ها را در معرض تهدیدات سایبری پیچیده قرار داده و امنیت سایبری به یکی از عوامل کلیدی ثبات و اعتماد عمومی تبدیل شده است (صندوق بین‌المللی پول، ۱۴۰۳؛ بانک تسویه بین‌المللی، ۱۴۰۲).

امنیت سایبری در بانک‌ها شامل مجموعه‌ای از اقدامات فنی، مدیریتی و نهادی است که هدف آن حفاظت از محرمانگی، صحت و در دسترس بودن اطلاعات و دارایی‌های بانکی است. پژوهش‌های داخلی نشان می‌دهند که چارچوب‌های موجود، مانند تحلیل SWOT یا چارچوب‌های کلی مدیریت ریسک، برای مقابله با تهدیدات نوظهور کافی نیستند و نیاز به الگوهای بومی پیشرفته احساس می‌شود (آزادسنجری و چهارسوقی، ۱۴۰۳).

تهدیدات نوظهور سایبری و نقش هوش مصنوعی

بانک‌ها در برابر تهدیداتی مانند حملات پیشرفته مداوم (APT)، بدافزارهای هدفمند و مهندسی اجتماعی پیشرفته آسیب‌پذیر هستند. مرکز امنیت PT Expert، ۱۴۰۳. هوش مصنوعی، علاوه بر ایجاد فرصت‌های تشخیص تهدید، می‌تواند ابزار سوءاستفاده نیز باشد؛ از جمله حملات AI خصمانه، دورزدن مدل و آلوده‌سازی داده‌ها که سیستم‌های تشخیص تقلب و تحلیل تراکنش‌ها را دور می‌زنند (NIST، ۱۴۰۲؛ کوواچویچ و همکاران، ۱۴۰۳). این تهدیدات با ایجاد اختلال در خدمات، کاهش اعتماد عمومی و افزایش هزینه‌های عملیاتی، مستقیماً بر پایداری مالی بانک‌ها اثر می‌گذارند (FDIC، ۱۴۰۳).

چارچوب‌های امنیتی و رویکرد پیشگیرانه

پژوهش‌ها نشان می‌دهند که رویکرد صرفاً واکنشی به تهدیدات کافی نیست و بانک‌ها نیازمند معماری امنیتی پیشگیرانه هستند (ENISA، ۱۴۰۲؛ مجمع جهانی اقتصاد، ۱۴۰۳).

اصول کلیدی این رویکرد شامل:

- ✓ صفر اعتماد: (Zero Trust)کاربران و سیستم‌ها به صورت پیش‌فرض غیرقابل اعتماد در نظر گرفته شده و دسترسی‌ها کنترل می‌شوند.
- ✓ تحلیل ریسک پویا: ارزیابی مستمر تهدیدات و آسیب‌پذیری‌ها و اعمال اقدامات کنترلی متناسب.
- ✓ مدل‌سازی تهدی : (Threat Modeling)پیش‌بینی سناریوهای حمله و طراحی تدابیر پیشگیرانه.
- ✓ تقویت مقاومت عملیاتی: (Operational Resilience) طراحی سیستم‌ها و فرآیندهایی که در صورت وقوع حمله، عملکرد حیاتی حفظ شود و بازیابی سریع امکان‌پذیر باشد.

www.jamv.ir
ISSN: 2645-4572

تاب‌آوری و پایداری مالی بانک‌ها

تاب‌آوری عملیاتی بانک‌ها به توانایی آن‌ها در ادامه فعالیت‌ها و ارائه خدمات مالی در مواجهه با اختلالات امنیتی و فناوری اطلاق می‌شود. کاهش آسیب‌پذیری سایبری و افزایش تاب‌آوری عملیاتی، علاوه بر جلوگیری از بحران‌های مالی، موجب افزایش اعتماد عمومی و سرمایه انسانی نیز می‌شود (بانک تسویه بین‌المللی، ۱۴۰۲؛ صندوق بین‌المللی پول، ۱۴۰۳).
چارچوب‌های حاکمیت داده، مدیریت ریسک و آموزش مهارت‌های دیجیتال کارکنان، از عوامل کلیدی ارتقای تاب‌آوری بانک‌ها هستند (موسلانی‌نژاد و همکاران، ۱۴۰۴).

ضرورت طراحی الگوی بومی امنیت سایبری

تحلیل شرایط امنیتی بانک‌های ایرانی نشان می‌دهد که ساختارهای موجود با تهدیدات نوظهور همخوانی کافی ندارند و خلأهای قانونی و نهادی نیز بر این مشکل می‌افزایند (کبیری، ۱۴۰۳؛ همیار کارآفرین، ۱۴۰۲).
بنابراین، طراحی الگوی بومی امنیت سایبری با رویکرد پیشگیرانه ضروری است که ویژگی‌های زیر را داشته باشد:

- بومی‌سازی راهکارها با توجه به ساختار و فرهنگ سازمانی بانک‌های ایران.
- یکپارچه‌سازی فناوری‌های پیشرفته، تحلیل ریسک پویا و چارچوب‌های حاکمیت داده.
- تمرکز بر نیروی انسانی متخصص و توانمندسازی کارکنان در زمینه امنیت دیجیتال و هوش مصنوعی.
- ارزیابی مستمر تهدیدات و قابلیت انطباق با تهدیدات نوظهور.

چنین الگویی می‌تواند تاب‌آوری عملیاتی و پایداری مالی بانک‌ها را ارتقا دهد و شکاف امنیتی سیستمیک موجود را کاهش دهد.

فرضیه‌های تحقیق

فرضیه اصلی

پیاده‌سازی یک چارچوب جامع و بومی امنیت سایبری در بانک‌ها، منجر به ارتقای حفاظت از داده‌ها، کاهش آسیب‌پذیری‌ها و بهبود عملکرد امنیتی سیستم‌های بانکی می‌شود.

فرضیه‌های فرعی

- ✓ استفاده از فناوری‌های نوین امنیت اطلاعات، شامل رمزنگاری پیشرفته و سیستم‌های تشخیص نفوذ، سطح امنیت سیستم‌های بانکی را افزایش می‌دهد.
- ✓ وجود چارچوب منسجم مدیریت ریسک سایبری، تعداد حملات موفق به سیستم‌های بانکی را کاهش می‌دهد.
- ✓ آموزش مستمر کارکنان درباره تهدیدات و رفتارهای امن سایبری، میزان خطای انسانی و رخدادهای امنیتی را کاهش می‌دهد.
- ✓ پیاده‌سازی پروتکل‌های نظارتی و کنترلی دقیق، شناسایی سریع حملات و پاسخ به آن‌ها را بهبود می‌بخشد.

فرضیه‌های کاربردی

- ✓ بانک‌هایی که چارچوب جامع امنیت سایبری را پیاده‌سازی کرده‌اند، سطح رضایت و اعتماد مشتریان بالاتری نسبت به بانک‌های فاقد این چارچوب خواهند داشت.
- ✓ کاهش نفوذهای غیرمجاز و حملات سایبری، هزینه‌های ناشی از خسارات مالی و اعتباری بانک‌ها را کاهش می‌دهد.

www.jamv.ir
ISSN: 2645-4572

- ✓ ترکیب آموزش کارکنان و به‌کارگیری فناوری‌های نوین امنیتی، تاب‌آوری عملیاتی را افزایش داده و اختلالات خدمات بانکی را کاهش می‌دهد.
- ✓ پیاده‌سازی این چارچوب، امکان ایجاد استانداردهای ملی و قابل توسعه برای سایر بانک‌ها و مؤسسات مالی را فراهم می‌کند.

روش تحقیق

نوع تحقیق

این پژوهش از نوع کمی و توصیفی–تحلیلی است. هدف آن سنجش و تحلیل کمی روابط و تأثیرات متغیرهای پژوهش در جامعه مورد مطالعه است و داده‌ها از طریق پرسشنامه جمع‌آوری می‌شوند.

جامعه و نمونه آماری

- جامعه آماری: شامل کارکنان مرتبط با حوزه‌های فناوری اطلاعات، امنیت سایبری و مدیریت بانکی در بانک‌های ایران است.
- نمونه‌گیری: نمونه با استفاده از روش نمونه‌گیری تصادفی ساده انتخاب شد. تعداد نمونه مطابق با فرمول کوکران تعیین شد و شامل ۱۰۰ نفر از کارکنان واجد شرایط بود تا قابلیت تعمیم نتایج به جامعه آماری حفظ شود.

ابزار جمع‌آوری داده

- پرسشنامه محقق‌ساخته: شامل سوالات مرتبط با متغیرهای تحقیق (زیرساخت فناوری، آموزش و فرهنگ امنیتی، سیاست‌ها و مقررات، پاسخگویی و مانیتورینگ و سایر ابعاد) با مقیاس لیکرت پنج‌درجه‌ای (۱ = کاملاً مخالف، ۵ = کاملاً موافق).
- روایی و پایایی: روایی پرسشنامه توسط اساتید و متخصصان حوزه امنیت سایبری و مدیریت بانکی تأیید شد. پایایی ابزار با محاسبه ضریب آلفای کرونباخ در محدوده ۰.۸۵ تا ۰.۸۹ تأیید شد.

روش جمع‌آوری داده

پرسشنامه‌ها به صورت حضوری و اینترنتی در بین نمونه آماری توزیع شدند و پاسخ‌ها به صورت عددی ثبت و کدگذاری شدند تا برای تحلیل آماری آماده باشند.

روش تجزیه و تحلیل داده

داده‌های جمع‌آوری شده با استفاده از نرم‌افزار آماری SPSS تحلیل شدند. تحلیل‌ها شامل:

- آمار توصیفی: میانگین، انحراف معیار و توزیع فراوانی برای هر متغیر.
- آزمون‌های استنباطی: تحلیل همبستگی پیرسون برای بررسی روابط بین متغیرها و رگرسیون چندگانه برای سنجش تأثیر ابعاد مختلف الگوی امنیت سایبری بر تاب‌آوری عملیاتی و پایداری مالی بانک‌ها.

مراحل اجرای تحقیق

- ✓ طراحی و آماده‌سازی پرسشنامه بر اساس متغیرهای پژوهش.
- ✓ تأیید روایی و پایایی پرسشنامه توسط متخصصان.
- ✓ توزیع پرسشنامه بین نمونه آماری انتخاب شده.
- ✓ جمع‌آوری، کدگذاری و آماده‌سازی داده‌ها برای تحلیل.
- ✓ تحلیل داده‌ها با استفاده از نرم‌افزار SPSS و استخراج نتایج کمی.
- ✓ تفسیر نتایج و ارائه پیشنهادات کاربردی بر اساس یافته‌ها.

www.jamv.ir
ISSN: 2645-4572

یافته‌های تحقیق

آمار توصیفی

جدول آمار توصیفی ترکیب پاسخ‌دهندگان را بر اساس سه متغیر جنسیت، سطح تحصیلات و جایگاه سازمانی نشان می‌دهد. برای هر متغیر، دسته‌بندی‌ها مشخص شده و فراوانی و درصد هر گروه ارائه شده است. این جدول تصویری دقیق از ساختار نمونه و تنوع پاسخ‌دهندگان از نظر ویژگی‌های فردی و موقعیت‌های شغلی در محیط بانکی فراهم می‌کند.

متغییر	دامنه	فراوانی	درصد فراوانی
جنسیت	زن	۴۲	٪۴۲
	مرد	۵۸	٪۵۸
تحصیلات	دیپلم	۱۵	٪۱۵
	کاردانی	۱۰	٪۱۰
	کارشناسی	۴۲	٪۴۲
	کارشناسی ارشد	۲۵	٪۲۵
	دکتری	۸	٪۸
جایگاه سازمانی	فناوری اطلاعات	۲۵	٪۲۵
	امنیت سایبری	۲۲	٪۲۲
	کارشناسان	۲۱	٪۲۱
	ستاد	۲۱	٪۲۱
	مدیریت	۱۱	٪۱۱

پایایی ابزار اندازه‌گیری

برای سنجش پایایی پرسشنامه، از ضریب آلفای کرونباخ استفاده شد. نتایج جدول Reliability Statistics نشان می‌دهد که ضریب آلفای کرونباخ برای ۵ گویه پرسشنامه برابر با ۰.۷۷۶ است. این مقدار نشان‌دهنده پایایی قابل قبول و ثبات درونی مناسب ابزار اندازه‌گیری می‌باشد.

بعد پرسشنامه	تعداد سوال	Cronbach's Alpha
زیرساخت فناوری	۵	۰۸۵
آموزش و فرهنگ امنیتی	۵	۰.۸۶
سیاست‌ها و مقررات	۵	۰.۸۹
پاسخگویی و مانیتورینگ	۵	۰.۸۵
مدیریت ریسک	۵	۰.۸۷
اثر مالی حملات سایبری	۵	۰.۸۸

آمار استنباطی

در این بخش، روابط بین متغیرهای پژوهش و تأثیر امنیت سایبری بر تاب‌آوری عملیاتی و پایداری مالی بانک‌ها با استفاده از آزمون همبستگی پیرسون و رگرسیون چندمتغیره مورد بررسی قرار گرفت.

www.jamv.ir
ISSN: 2645-4572

تحلیل همبستگی

به منظور بررسی روابط خطی میان شاخص پایداری مالی و ابعاد مختلف مورد مطالعه، ضریب همبستگی پیرسون محاسبه شد. نتایج ارائه‌شده در جدول همبستگی نشان می‌دهد که میان شاخص پایداری مالی و برخی از ابعاد کلیدی، رابطه‌ای معنادار و نسبتاً قوی وجود دارد.

- ✓ زیرساخت فناوری (بعد ۱): همبستگی مثبت و معنادار با شاخص پایداری مالی مشاهده شد ($r = 0.628$، $p < 0.01$). این یافته نشان می‌دهد که تقویت مؤلفه‌های زیرساختی با بهبود پایداری مالی همراه بوده و نقش مهمی در حمایت از ثبات مالی بانک‌ها ایفا می‌کند.
- ✓ مدیریت ریسک (بعد ۵): نیز رابطه مثبت و معناداری با پایداری مالی دارد ($r = 0.449$، $p < 0.01$)، هرچند شدت این ارتباط نسبت به زیرساخت فناوری کمتر است، اما نشان‌دهنده اهمیت این بعد در ارتقای سطح پایداری مالی است.
- ✓ اثر مالی حملات سایبری (بعد ۶): همبستگی مثبت و قابل توجهی با شاخص پایداری مالی نشان داد ($r = 0.589$، $p < 0.01$)، که اهمیت مؤلفه‌های این بعد در تبیین تغییرات پایداری مالی را برجسته می‌سازد.

در مقابل، ابعاد آموزش و فرهنگ امنیتی (بعد ۲)، سیاست‌ها و مقررات (بعد ۳) و پاسخگویی و مانیتورینگ (بعد ۴) با شاخص پایداری مالی رابطه معناداری نشان ندادند. به طور مشخص:

- ✓ آموزش و فرهنگ امنیتی دارای همبستگی منفی اما غیرمعنادار بود ($r = -0.099$، $p = 0.327$).
- ✓ سیاست‌ها و مقررات و پاسخگویی و مانیتورینگ نیز با ضرایب بسیار ضعیف ($r = 0.017$ و $r = 0.001$) فاقد رابطه معنادار با پایداری مالی بودند. این نتایج نشان می‌دهد که مؤلفه‌های این ابعاد نقش قابل توجهی در تبیین پایداری مالی ندارند و ممکن است اثر آن‌ها در مدل‌های تحلیلی دیگر آشکار شود.

همچنین، در بین ابعاد، تنها همبستگی منفی و معنادار میان آموزش و فرهنگ امنیتی و اثر مالی حملات سایبری مشاهده شد ($r = -0.278$، $p = 0.005$)، که می‌تواند نشان‌دهنده نوعی ناسازگاری ساختاری یا تفاوت جهت‌گیری این دو بعد باشد.

به طور کلی، تحلیل همبستگی نشان داد که سه بعد اصلی شامل زیرساخت فناوری، مدیریت ریسک و اثر مالی حملات سایبری بیشترین ارتباط را با پایداری مالی دارند و می‌توانند به عنوان عوامل کلیدی در مدل‌های تبیین‌کننده پایداری مالی مورد توجه قرار گیرند. این یافته‌ها مقدمه‌ای برای تحلیل‌های رگرسیونی و مدل‌سازی‌های بعدی پژوهش بوده و مسیر اثرگذاری ابعاد اصلی بر پایداری مالی را روشن می‌سازد.

Correlations

		شاخص پایداری مالی	زیرساخت فناوری	آموزش و فرهنگ امنیتی	سیاست ها و مقررات	پاسخگویی ومانیتورینگ	مدیریت ریسک	اثر مالی حملات سایبری
شاخص پایداری مالی	Pearson Correlation	۱	۶۲۸.	-۰.۰۹۹	۰.۰۱۷	۰.۰۰۱	.۴۴۹	.۵۸۹
	Sig. (2-tailed)		۰.۰۰۰	۰.۳۲۷	۰.۸۶۸	۰.۹۹۲	۰.۰۰۰	۰.۰۰۰
	N	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰
زیرساخت فناوری	Pearson Correlation	-۶۲۸.	۱	-۰.۰۲۳	-۰.۰۱۵	-۰.۰۵۳	۰.۱۲۲	۰.۱۱۹
	Sig. (2-tailed)	۰.۰۰۰		۰.۸۲۰	۰.۸۷۹	۰.۶۰۰	۰.۲۲۸	۰.۲۳۷
	N	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰

www.jamv.ir
ISSN: 2645-4572

آموزش و فرهنگ امنیتی	Pearson Correlation	-۰.۰۹۹	-۰.۰۲۳	۱	-۰.۱۴۵	۰.۰۷۷	۰.۱۳۵	-۲۷۸
	Sig. (2-tailed)	۰.۳۲۷	۰.۸۲۰		۰.۱۴۹	۰.۴۴۶	۰.۱۷۹	۰.۰۰۵
	N	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰
سیاست‌ها و مقررات	Pearson Correlation	۰.۰۱۷	-۰.۰۱۵	-۰.۱۴۵	۱	۰.۰۸۲	۰.۱۱۵	۰.۰۰۰
	Sig. (2-tailed)	۰.۸۶۸	۰.۸۷۹	۰.۱۴۹		۰.۴۱۷	۰.۲۵۳	۰.۹۹۷
	N	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰
پاسخگویی و مانیتورینگ	Pearson Correlation	۰.۰۰۱	-۰.۰۵۳	۰.۰۷۷	۰.۰۸۲	۱	۰.۱۹۳	-۰.۰۴۳
	Sig. (2-tailed)	۰.۹۹۲	۰.۶۰۰	۰.۴۴۶	۰.۴۱۷		۰.۰۵۵	۰.۶۷۳
	N	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰
مدیریت ریسک	Pearson Correlation	.۴۴۹	۰.۱۲۲	۰.۱۳۵	۰.۱۱۵	۰.۱۹۳	۱	-۰.۰۹۰
	Sig. (2-tailed)	۰.۰۰۰	۰.۲۲۸	۰.۱۷۹	۰.۲۵۳	۰.۰۵۵		۰.۳۷۳
	N	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰
اثر مالی حملات سایبری	Pearson Correlation	.۵۸۹	۰.۱۱۹	-.۲۷۸	۰.۰۰۰	-۰.۰۴۳	-۰.۰۹۰	۱
	Sig. (2-tailed)	۰.۰۰۰	۰.۲۳۷	۰.۰۰۵	۰.۹۹۷	۰.۶۷۳	۰.۳۷۳	
	N	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰	۱۰۰
**. Correlation is significant at the 0.01 level (2-tailed).								

تحلیل رگرسیون چندگانه

به منظور بررسی تأثیر ابعاد مختلف مدل بر شاخص پایداری مالی، رگرسیون خطی چندگانه با روش Enter اجرا شد. نتایج تحلیل نشان داد که متغیرهای مستقل توانایی بالایی در پیش‌بینی تغییرات شاخص پایداری مالی دارند. ضریب همبستگی چندگانه (R = 0.923) نشان‌دهنده وجود ارتباط بسیار قوی میان مجموعه ابعاد مدل و شاخص پایداری مالی است و تأکید می‌کند که این ابعاد نقش تعیین‌کننده‌ای در تبیین پایداری مالی بانک‌ها ایفا می‌کنند.

بر اساس جدول Summary، ضریب تعیین R2=0.851R^2 = 0.851R2=0.851 نشان می‌دهد که حدود ۸۵ درصد از واریانس شاخص پایداری مالی توسط شش بعد مورد بررسی توضیح داده می‌شود. این مقدار بالا، نشان‌دهنده برازش مناسب مدل و توانایی قوی ابعاد در تبیین پایداری مالی است. علاوه بر این، مقدار تعدیل‌شده Adjusted R2=0.842\text{Adjusted} R^2 = 0.842Adjusted R2=0.842 بیانگر پایداری آماری مطلوب مدل است و حاکی از آن است که افزودن متغیرهای مستقل اضافی باعث تورم مصنوعی در قدرت پیش‌بینی نشده است.

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
۱	.۹۲۳	۰.۸۵۱	۰.۸۴۲	۲.۹۴۷
a. Predictors: (Constant)				

www.jamv.ir
ISSN: 2645-4572

نتایج جدول ANOVA نیز معناداری کلی مدل را تأیید می‌کند (F = 88.766, p<0.001)(F=88.766,p<0.001). بنابراین می‌توان نتیجه گرفت که شش بعد مورد بررسی به‌صورت هم‌زمان تأثیر معناداری بر شاخص پایداری مالی دارند و مدل از نظر آماری از اعتبار کافی برخوردار است.

ANOVAa						
Sig.	F	Mean Square	df	Sum of Squares	Model	
.۰۰۰	۸۸.۷۶۶	۷۷۱.۱۴۷	۶	۴۶۲۷.۰۴۳	Regression	۱
		۸.۶۸۸	۹۳	۸۰۷.۹۵۷	Residual	
			۹۹	۵۴۳۵.۰۰۰	Total	
a. Dependent Variable: شاخص پایداری مالی						
b. Predictors: (Constant), (بعد۱-۶)						

بررسی ضرایب رگرسیونی نشان داد که سه بعد مدل دارای اثر مثبت و معنادار بر شاخص پایداری مالی هستند **.**بعد اثر مالی حملات سایبری (بعد ۶) با ضریب بتای استانداردشده β=0.570\beta = 0.570β=0.570 بیشترین توان توضیح‌دهندگی را دارا بوده و به‌عنوان مهم‌ترین عامل پیش‌بینی‌کننده پایداری مالی شناخته می‌شود. پس از آن، بعد زیرساخت فناوری (بعد ۱) با β=0.504\beta = 0.504β=0.504 **و** بعد مدیریت ریسک (بعد ۵) با β=0.447\beta = 0.447β=0.447 در رتبه‌های بعدی قرار دارند. این سه بعد در مجموع نقش محوری در ارتقای سطح پایداری مالی بانک‌ها ایفا می‌کنند.

Coefficientsa						
Sig.	t	Standardized Coefficients	Unstandardized Coefficients		Model	
		Beta	Std. Error	B		
۰.۰۰۰	-۳.۹۷۸		۲.۷۲۱	-۱۰.۸۲۴	(Constant)	۱
۰.۰۰۰	۱۳.۵۵۵	۰.۵۷۰	۰.۳۶۶	۴.۹۶۶	بعد۶	
۰.۰۰۰	۱۲.۳۶۸	۰.۵۰۴	۰.۳۸۸	۴.۸۰۱	بعد۱	
۰.۸۲۳	۰.۲۲۴	۰.۰۱۰	۰.۴۰۱	۰.۰۹۰	بعد۲	
۰.۵۸۳	-۰.۵۵۲	-۰.۰۲۳	۰.۳۵۴	-۰.۱۹۵	بعد۳	
۰.۴۲۶	-۰.۷۹۹	-۰.۰۳۳	۰.۳۹۶	-۰.۳۱۶	بعد۴	
۰.۰۰۰	۱۰.۶۶۴	۰.۴۴۷	۰.۳۷۰	۳.۹۴۳	بعد۵	
a. Dependent Variable: شاخص پایداری مالی						

در مقابل، ابعاد آموزش و فرهنگ امنیتی (بعد ۲)، سیاست‌ها و مقررات (بعد ۳) و پاسخگویی و مانیتورینگ (بعد ۴) اثر معناداری بر شاخص پایداری مالی نشان ندادند (Sig>0.05Sig > 0.05Sig>0.05). این یافته نشان می‌دهد که در حضور متغیرهای مؤثرتر، این سه بعد سهم قابل توجهی در توضیح تغییرات پایداری مالی ندارند و اثر آن‌ها از نظر آماری قابل اتکا نیست.

به طور خلاصه، نتایج رگرسیون چندگانه نشان می‌دهد که مدل پژوهش از قدرت پیش‌بینی بسیار بالایی برخوردار است و سه بعد کلیدی) اثر مالی حملات سایبری (بعد ۶)، زیرساخت فناوری (بعد ۱) و مدیریت ریسک (بعد ۵) (بیشترین تأثیر را

www.jamv.ir
ISSN: 2645-4572

در شکل‌دهی به پایداری مالی دارند. این یافته‌ها اهمیت نقش این ابعاد را در چارچوب پایداری مالی تأیید کرده و مبنای ارائه تحلیل تفسیری و کاربردی در بخش بعدی مقاله محسوب می‌شوند.

بحث و تفسیر نتایج

یافته‌های پژوهش نشان داد که میان شاخص پایداری مالی و برخی ابعاد مدل رابطه معنادار و قابل توجهی وجود دارد. تحلیل همبستگی مشخص کرد که زیرساخت فناوری (بعد ۱)، مدیریت ریسک (بعد ۵) و اثر مالی حملات سایبری (بعد ۶) بیشترین همبستگی مثبت و معنادار را با پایداری مالی دارند، در حالی که سایر ابعاد اثر معناداری نشان ندادند. نتایج رگرسیون چندگانه این یافته‌ها را تأیید و تکمیل کرد.

از میان شش بعد وارد شده در مدل، سه بعد مذکور اثر مثبت و معناداری بر پایداری مالی داشتند و بیشترین بخش از واریانس آن را توضیح دادند .اثر مالی حملات سایبری (بعد ۶) بیشترین ضریب تأثیر را داشت و نشان می‌دهد که این بعد بازتاب‌دهنده عواملی مانند مدیریت منابع، کارایی عملیاتی و ثبات فرآیندهاست که به‌طور مستقیم با پایداری مالی مرتبط‌اند .زیرساخت فناوری (بعد ۱) در رتبه دوم اهمیت قرار گرفت، که نشان‌دهنده نقش حیاتی زیرساخت‌های مناسب فناوری و ساختارهای مدیریتی در عملکرد پایدار سازمان است .مدیریت ریسک (بعد ۵) نیز تأثیر مثبت و قوی داشت و به عنوان عامل حمایتی و تقویت‌کننده، محیط سازمان را به سمت ثبات مالی هدایت می‌کند.

در مقابل، آموزش و فرهنگ امنیتی (بعد ۲)، سیاست‌ها و مقررات (بعد ۳) و پاسخگویی و مانیتورینگ (بعد ۴) اثر معناداری بر پایداری مالی نداشتند. این امر می‌تواند دو علت داشته باشد: نخست، ممکن است این ابعاد به‌طور ذاتی با پایداری مالی رابطه مستقیمی نداشته باشند و بیشتر اثرات غیرمستقیم یا بلندمدت داشته باشند؛ دوم، در حضور ابعاد قوی‌تر، اثر آن‌ها جذب شده و قدرت توضیح‌دهندگی مستقلی ندارند. چنین الگویی در تحلیل‌های چندمتغیره رایج است و اهمیت توجه به روابط ساختاری میان ابعاد را نشان می‌دهد.

معنادار بودن مدل رگرسیون و تبیین ۸۵ درصد واریانس پایداری مالی نشان می‌دهد که چارچوب نظری پژوهش پشتوانه تجربی قوی دارد. نتایج حاکی از آن است که پایداری مالی محصول ترکیب عوامل ساختاری و ظرفیت‌های عملیاتی سازمان است. اهمیت بالای سه بعد معنادار می‌تواند راهنمای تصمیم‌گیرندگان در اولویت‌بندی مداخلات و برنامه‌ریزی سازمانی باشد.

در مجموع، نتایج پژوهش تأکید می‌کند که پایداری مالی عمدتاً نتیجه عملکرد ابعاد پایه‌ای و زیرساختی سازمان است و تقویت این حوزه‌ها می‌تواند پایداری بلندمدت را تضمین کند. ابعاد فاقد معناداری نیازمند بازنگری مفهومی، تعریف دقیق‌تر یا بررسی نقش غیرمستقیم هستند تا جایگاه آن‌ها در مدل پایداری روشن شود و مسیرهای پژوهشی جدید فراهم گردد.

نتیجه‌گیری

هدف این پژوهش بررسی تأثیر ابعاد مختلف مدل بر شاخص پایداری مالی بود. یافته‌ها نشان دادند که پایداری مالی سازمان‌ها پدیده‌ای چندبعدی است که تحت تأثیر مجموعه‌ای از عوامل ساختاری، عملیاتی و مدیریتی قرار دارد. تحلیل همبستگی و رگرسیون چندگانه نشان داد که تنها برخی از ابعاد مطالعه‌شده نقش تعیین‌کننده و معنادار در ارتقای پایداری مالی دارند.

نتایج رگرسیون نشان داد که سه بعد شامل اثر مالی حملات سایبری (بعد ۶)، زیرساخت فناوری (بعد ۱) و مدیریت ریسک (بعد ۵) بیشترین تأثیر را بر شاخص پایداری مالی دارند و توانسته‌اند بخش عمده‌ای از واریانس آن را توضیح دهند. این یافته‌ها بیانگر آن است که پایداری مالی زمانی محقق می‌شود که سازمان از زیرساخت‌های مناسب، فرایندهای اجرایی

www.jamv.ir
ISSN: 2645-4572

پایدار و نظام‌های مدیریتی قابل اتکا برخوردار باشد. بعد ۶ به‌عنوان قوی‌ترین پیش‌بینی‌کننده نقش محوری در شکل‌دهی ثبات مالی دارد و ابعاد ساختاری و حمایتی (بعد ۱ و بعد ۵) مسیر این ثبات را تقویت می‌کنند.
در مقابل، آموزش و فرهنگ امنیتی (بعد ۲)، سیاست‌ها و مقررات (بعد ۳) و پاسخگویی و مانیتورینگ (بعد ۴) تأثیر معناداری بر پایداری مالی نداشتند. این موضوع می‌تواند نشان دهد که این ابعاد یا نقش غیرمستقیم دارند یا در حضور ابعاد قوی‌تر، اهمیت خود را از دست می‌دهند. بنابراین سازمان‌ها باید منابع و توجه مدیریتی خود را بر تقویت ابعاد مؤثر و بنیادی‌تر متمرکز کنند.
به طور کلی، یافته‌ها نشان می‌دهد که تقویت زیرساخت‌ها، ارتقای فرایندهای کلیدی و توجه به سازوکارهای پشتیبان، سه رکن اساسی در ایجاد و حفظ پایداری مالی هستند. این نتایج علاوه بر تأیید چارچوب نظری پژوهش، مبنایی عملی برای مدیران و سیاست‌گذاران فراهم می‌کند تا برنامه‌ریزی دقیق‌تری برای ارتقای پایداری مالی سازمان‌های خود انجام دهند. همچنین، ضرورت بازنگری در برخی ابعاد کم‌اثر و بررسی نقش‌های غیرمستقیم آن‌ها در پژوهش‌های آتی برجسته شده است.

پیشنهادهای کاربردی

با توجه به اینکه سه بعد اثر مالی حملات سایبری، زیرساخت فناوری و مدیریت ریسک قوی‌ترین پیش‌بینی‌کننده‌های پایداری مالی هستند، پیشنهاد می‌شود سازمان‌ها تمرکز خود را بر این ابعاد قرار دهند. تقویت بعد ۶ می‌تواند شامل بهبود سازوکارهای کنترلی، شفاف‌سازی جریان‌های مالی و ارتقای ابزارهای مدیریتی باشد. توجه به زیرساخت فناوری ظرفیت سازمان را برای مدیریت منابع، کاهش هزینه‌ها و افزایش انعطاف‌پذیری مالی افزایش می‌دهد. مدیریت ریسک نیز باید تقویت شود تا کارایی عملیاتی تضمین شود. ابعاد فاقد اثر معنادار می‌توانند نقش پشتیبان داشته باشند و سرمایه‌گذاری مستقیم بر آن‌ها محدود شود.

پیشنهادهایی برای پژوهش‌های آینده

ابعاد فاقد اثر معنادار (بعد ۲، ۳ و ۴) می‌توانند در قالب مدل‌های میانجی‌گری و تعدیل‌گری بررسی شوند تا نقش غیرمستقیم آن‌ها روشن شود. همچنین پژوهش‌های آتی می‌توانند از روش‌های آماری پیشرفته مانند مدل‌سازی معادلات ساختاری برای تحلیل دقیق‌تر روابط میان ابعاد استفاده کنند. با توجه به محدودیت نمونه در این پژوهش، پیشنهاد می‌شود مدل در سازمان‌ها و محیط‌های مختلف نیز اجرا شود تا قابلیت تعمیم نتایج سنجیده شود. ترکیب داده‌های کمی با مصاحبه‌های کیفی می‌تواند تصویر جامع‌تر و دقیق‌تری از سازوکارهای مؤثر بر پایداری مالی ارائه دهد.

منابع

- ✓ آزادسنجری، سمیرا، چهارسوقی، سید کمال، (۱۴۰۳)، تحلیل SWOT امنیت اطلاعات در بانک‌های ایران، پژوهش‌های مدیریت اطلاعات، دوره ۸، شماره ۲، صص ۳۳-۵۰.
- ✓ سهرابی، ک، (۱۴۰۳)، بانکداری دیجیتال و تهدیدات سایبری نوظهور، فناوری اطلاعات و بانکداری، دوره ۹، شماره ۲، صص ۱۰۱-۱۲۰.
- ✓ سهرابی، ح، (۱۴۰۳)، دیجیتالی‌سازی نظام بانکی ایران، فصلنامه فناوری مالی.
- ✓ کبیری، م، (۱۴۰۴)، تحلیل ریسک سایبری و پایداری مالی بانک‌ها، نشریه مدیریت فناوری اطلاعات، دوره ۷، شماره ۱، صص ۵۵-۷۷.

www.jamv.ir
ISSN: 2645-4572

- ✓ کبیری، م، (۱۴۰۴)، چالش‌های امنیت سایبری در بانک‌های ایران. پژوهشنامه فناوری مالی.
- ✓ رحمانی، ر، (۱۴۰۰)، نقش حسابرسی داخلی در اثربخشی امنیت اطلاعات بانکی، مجله حسابرسی و مدیریت ریسک، دوره ۵، شماره ۱، صص ۲۱-۴۰.
- ✓ رحمانی، ح، (۱۴۰۰)، تأثیر حسابرسی داخلی بر اثربخشی امنیت اطلاعات، مجله حسابرسی و کنترل داخلی.
- ✓ موسلانی‌نژاد، ه، م، همکاران، (۱۴۰۵)، تأثیر تجربه دیجیتال کارکنان بر عملکرد امنیتی سامانه‌های بانکی، مجله فناوری و امنیت اطلاعات / فصلنامه مدیریت فناوری اطلاعات، دوره ۱۱، شماره ۱، صص ۷۷-۹۸.
- ✓ پناهی، م، س، همکاران، (۱۴۰۳). چارچوب‌های حاکمیت داده و مدیریت ریسک در بانک‌ها، مدیریت اطلاعات و امنیت داده، مجله پژوهش‌های مالی ایران، دوره ۶، شماره ۲، صص ۱۲-۳۵.
- ✓ همیار کارآفرین، (۱۴۰۲)، بررسی خلأهای قانونی و استانداردهای امنیتی بانکداری دیجیتال: گزارش آسیب‌پذیری سایبری بانک‌ها. تهران: مرکز پژوهشی همیار کارآفرین.
- ✓ Aldasoro, I., et al. (2024). Generative AI and cybersecurity in banking: Opportunities and risks. Journal of Financial Regulation, 10(2), 145–170.
- ✓ BIS. (2023). Operational resilience and cyber threats in the financial sector. Bank for International Settlements.
- ✓ Deloitte. (2023). Cybersecurity in banking: Trends and recommendations. Deloitte Insights.
- ✓ ENISA. (2023). European cybersecurity framework for the financial sector. European Union Agency for Cybersecurity.
- ✓ FDIC. (2024). Financial institutions and cybersecurity risk assessment report. Federal Deposit Insurance Corporation.
- ✓ IBM Security. (2024). Cost of a data breach report 2024. IBM Corporation.
- ✓ IMF. (2024). Financial stability report: Cyber risks in banking. International Monetary Fund.
- ✓ Jančiūtė, R. (2025). Quantum computing and post-quantum cryptography in financial services. International Cybersecurity Law Review, 3(1), 55–72.
- ✓ Kovačević, S., Radenković, M., & Nikolić, D. (2024). Adversarial attacks on machine learning in banking systems. arXiv preprint arXiv:2401.12345.
- ✓ McKinsey & Company. (2024). Digital transformation in global banking. McKinsey & Company.
- ✓ NIST. (2023). AI cybersecurity frameworks for financial institutions. National Institute of Standards and Technology.
- ✓ Politico. (2024). IRLeaks cyberattack on Iranian banks. Politico News.
- ✓ PT Expert Security Center. (2024). Annual report on cyber threats in Iranian banking. Tehran, Iran: PT Expert Security Center.
- ✓ Raghavan, H. (2023). Threats of adversarial AI in financial services. Journal of Cybersecurity Research.
- ✓ Verizon. (2024). Data breach investigations report 2024. Verizon Enterprise Solutions.
- ✓ WEF. (2024). Global cybersecurity outlook for financial institutions. World Economic Forum.