

مدیریت بحران در بانک ها در مواجهه با حملات سایبری و اختلالات سیستمی

ایمان عبدالمهی، علی زارع

دانشجوی دکتری حسابداری، واحد قاینات، دانشگاه آزاد اسلامی، قاینات، ایران
iman.abdollahi2815@iau.ir

دانشجوی دکتری حسابداری، واحد قاینات، دانشگاه آزاد اسلامی، قاینات، ایران
ali.zare5548@iau.ac.ir

چکیده

گسترش روزافزون فناوری های مالی و وابستگی سامانه های بانکی به بسترهای برخط، شبکه بانکی را در معرض آسیب پذیری های شدید ناشی از حملات سایبری و اختلالات سیستمی قرار داده که تداوم فعالیت مالی و سلامت کنترل های داخلی را تهدید می کند. بر این اساس، هدف اصلی پژوهش حاضر تبیین نقش راهبردی مدیریت بحران در بانک ها در مهار حوادث سایبری و اختلالات زیرساختی و بررسی پیامدهای آن بر حفظ سلامت کنترل های داخلی و تداوم عملیات گزارشگری مالی است. این مطالعه از نظر هدف کاربردی و از منظر نحوه گردآوری داده ها، توصیفی-پیمایشی و کمی است. جامعه آماری تحقیق شامل مدیران، راهبران امنیت اطلاعات، کارشناسان ریسک و حسابرسان ارشد شبکه بانکی کشور بوده که با روش نمونه گیری در دسترس، نمونه ای متشکل از ۳۹۲ نفر انتخاب شدند. ابزار گردآوری داده ها پرسشنامه ساختاریافته استاندارد بود که روایی همگرا و واگرا و پایایی مرکب آن به تایید رسید. تجزیه و تحلیل داده ها با بهره گیری از مدل سازی معادلات ساختاری مبتنی بر روش حداقل مربعات جزئی در نرم افزارهای اس پی اس اس و اسمارت پی ال اس انجام پذیرفت. یافته های پژوهش نشان داد که مدیریت بحران اثر بازدارنده، منفی و معناداری بر آسیب پذیری سایبری و نرخ اختلالات سیستمی دارد. همچنین نفوذ سایبری و وقفه های سامانه ای اثر منفی و شدیدی بر سلامت کنترل های داخلی و تداوم دفاتر مالی بر جای می گذارند. در نهایت، اثر غیرمستقیم و کل مدیریت بحران بر سلامت ساختار کنترلی و تداوم مالی بانک ها مثبت و معنادار ارزیابی شد که ضرورت پیوند راهبردی میان کمیته های حسابرسی و امنیت اطلاعات را اثبات می کند.

کلیدواژه ها: مدیریت بحران، حملات سایبری، اختلالات سیستمی، سلامت کنترل های داخلی

مقدمه

تحول دیجیتال و یکپارچگی روزافزون فناوری های نوین اطلاعاتی در صنعت بانکداری، ساختار عملیاتی و مدل های کسب و کار مؤسسات مالی را دستخوش دگرگونی بنیادین کرده است. امروزه سامانه های بانکداری الکترونیک، بسترهای پرداخت برخط و زیرساخت های ابری به شریان های حیاتی گردش نقدینگی و ثبات اقتصادی بدل شده اند. با این حال، وابستگی فزاینده به فناوری های به هم پیوسته، آسیب پذیری های نهادی نوینی را پدید آورده و سطح مواجهه بانک ها با تهدیدات امنیتی را به شکل تصاعدی گسترش داده است. حملات سایبری پیشرفته نظیر باج افزارها، اختلال در توزیع خدمات، نفوذ به پایگاه های داده و از کار افتادگی زیرساخت های پردازش ابری دیگر صرفاً چالش های فنی حوزه فناوری اطلاعات به شمار نمی روند، بلکه به عنوان ریسک های سیستمی و مالی حاد طبقه بندی می شوند (بیسواس، ۲۰۲۳). بروز اختلالات فناورانه یا حملات سازمان یافته، توانایی بانک ها در استمرار عملیات، حفظ محرمانگی و یکپارچگی داده های مالی را با مخاطره مواجه ساخته و می تواند در کوتاه مدت به فلج شدن جریان تسویه وجوه و بحران های نقدینگی منجر شود (کوتینیو، ۲۰۲۴).

از دیدگاه حسابداری، حاکمیت شرکتی و گزارشگری مالی، وقوع رخنه و حملات سایبری با پیامدهای اقتصادی سنگین و گاه غیرقابل جبرانی همراه است. این اختلالات علاوه بر تحمیل هزینه های آشکار شامل جرایم نظارتی ناشی از عدم انطباق، هزینه های بازسازی فنی و دعاوی حقوقی، آسیب های پنهان ساختاری از جمله افت ارزش برند، فرسایش سرمایه اعتباری، خروج سپرده ها و کاهش دقت در سامانه های کنترل داخلی حسابداری را در پی دارند (الشیاب، ۲۰۲۳). داده های غیرمالی ناشی از رخدادهای امنیتی مستقیماً مفروضات تداوم فعالیت، ارزش گذاری منصفانه دارایی های نامشهود و شفافیت گزارشگری را تحت تأثیر قرار می دهند. در چنین بستری، ناتوانی بانک ها در مهار شوک های سایبری موجب گسترش بی اعتمادی در بازارهای پولی، افزایش هزینه تأمین مالی و سرایت ریسک عملیاتی به کل نظام مالی می گردد؛ امری که ضرورت گذار از چارچوب های سنتی امنیت سایبری به پارادایم جامع تاب آوری عملیاتی و مدیریت بحران را دوچندان می سازد (موریرا، ۲۰۲۴).

مدیریت بحران در این پژوهش به عنوان مجموعه ای یکپارچه از سازوکارهای شناسایی به موقع، مهار فنی، تداوم عملیات حسابداری، بازیابی زیرساخت ها و ارتباطات شفاف مالی و نظارتی در مواجهه با ناپایداری های حاد تعریف می شود. در حالی که بخش عمده ای از سازوکارهای موجود بر اقدامات پیشگیرانه فنی یا پدافند لایه ای تمرکز دارند، شدت و پیچیدگی تهدیدات مدرن نشان می دهد که وقوع رخنه ها و توقف های سیستمی امری اجتناب ناپذیر است (هارتمن، ۲۰۲۴). بنابراین، آنچه سرنوشت یک نهاد مالی را در لحظه بحران رقم می زند، نه صرفاً دیوارهای امنیتی، بلکه میزان چابکی بانک در مهار عواقب، سنجش بهای ناشی از توقف و احیای جریان اطلاعات حسابداری و خدمات عمومی است. ترکیب چارچوب های مدیریت بحران با سیستم های اطلاعاتی حسابداری و مدیریت ریسک شرکتی، زیربنای اصلی توانایی بانک در تاب آوری در برابر مخاطرات ناشناخته سایبری را تشکیل می دهد (احمد، ۲۰۲۴).

اگرچه در سال های اخیر ادبیات پژوهشی قابل توجهی پیرامون جنبه های مهندسی امنیت داده و مدیریت ریسک های فناوری اطلاعات در بانک ها شکل گرفته است، اما این مطالعات عمدتاً در سیلوهای مستقل فنی محدود مانده و پل ارتباطی محکمی میان سازوکارهای مهندسی امنیت و اثرات مالی و کنترل های داخلی حسابداری برقرار نکرده اند (نواک، ۲۰۲۳). اغلب الگوهای سنتی مدیریت تداوم

کسب و کار، فرآیندهای مالی را به عنوان مؤلفه‌ای پساخرداد در نظر می‌گیرند و فاقد پویایی لازم جهت ادغام تصمیم‌گیری‌های لحظه‌ای حسابداری با سناریوهای بحران سایبری هستند. عدم وجود یک مدل یکپارچه که بتواند پروتکل‌های واکنش فنی، شاخص‌های ارزیابی خسارات مالی آنی، راهبردهای پایداری دفاتر کل و ارتباطات نظارتی را به شکلی نظام‌مند تلفیق کند، یک شکاف مفهومی و کاربردی بنیادین در بانکداری معاصر است (چن، ۲۰۲۴).

بر این اساس، هدف اصلی پژوهش حاضر، طراحی و تبیین یک الگوی جامع و یکپارچه مدیریت بحران برای بانک‌ها در مواجهه با حملات سایبری و اختلالات گسترده سیستمی است؛ الگویی که بتواند ابعاد حاکمیت ریسک، ابزارهای کنترلی حسابداری، تاب‌آوری عملیاتی و بازسازی فرآیندهای مالی را با یکدیگر همگام سازد.

اهمیت و ضرورت این تحقیق از آنجا ناشی می‌شود که صنعت بانکداری به عنوان ستون فقرات تخصیص منابع و تسهیل مبادلات اقتصادی، نیازمند بالاترین سطح اعتماد عمومی است؛ اعتمادی که در صورت اختلالات مداوم داده‌ها یا تخریب سوابق مالی، در کوتاه‌ترین زمان فرومی‌پاشد (ویلیامز، ۲۰۲۳). نتایج این مطالعه با پیوند زدن رویکردهای مهندسی امنیت و تئوری‌های حسابداری مدیریت و حاکمیت شرکتی، به بسط مرزهای دانش مالی و ارتقای متون مدیریت ریسک سیستمی کمک شایانی خواهد نمود. از بعد کاربردی، این پژوهش ابزاری دقیق و چندبعدی در اختیار مدیران ارشد بانک‌ها، اعضای کمیته حسابرسی و نهادهای ناظر پولی قرار می‌دهد تا ضمن ارزیابی آمادگی سازمانی، آسیب‌پذیری‌های ناشناخته را مهار کرده و زیان‌های اقتصادی تحمیلی به ذی‌نفعان را به حداقل برسانند (وانگ، ۲۰۲۴).

با عطف به مبانی مطرح‌شده و به منظور هدایت این فرایند کاوش‌گرایانه، پژوهش حاضر درصدد پاسخ‌گویی به پرسش‌های کلیدی زیر است:

چارچوب و مؤلفه‌های یک الگوی جامع مدیریت بحران در بانک‌ها به منظور مقابله اثربخش با پیامدهای مالی، عملیاتی و اعتباری ناشی از حملات سایبری و اختلالات سیستمی چیست؟

پیشینه و مبانی نظری

چارچوب مفهومی مدیریت بحران در نهادهای بانکی

مدیریت بحران در صنعت بانکداری به عنوان مجموعه‌ای یکپارچه از ساختارها، فرآیندها و قابلیت‌های شناختی و عملیاتی تعریف می‌شود که هدف آن شناسایی علائم اولیه ناپایداری، اتخاذ تصمیمات بلادرنگ جهت تحدید دامنه آسیب، صیانت از جریان نقدینگی و بازگرداندن سیستم به حالت پایداری است (فرناندر، ۲۰۲۴). از منظر نظریه قابلیت‌های پویا، مدیریت بحران صرفاً یک پروتکل واکنشی پس از وقوع فاجعه نیست، بلکه توانمندی سازمان در بازپیکربندی سریع منابع و بازطراحی رویه‌ها در شرایط ناپایداری‌های حاد و عدم قطعیت ساختاری است (بیسواس، ۲۰۲۳). در یک محیط بانکی، بحران نه تنها دارایی‌های فیزیکی، بلکه دارایی‌های نامشهود، قابلیت اتکای دفاتر حسابداری و اعتماد سرمایه‌گذاران را به شکلی گسترده مورد تهاجم قرار می‌دهد (موریرا، ۲۰۲۴). از این‌رو، چارچوب‌های مدیریت بحران مدرن نیازمند انطباق با سازوکارهای حاکمیت شرکتی و سیستم‌های اطلاعاتی پیشرفته هستند

تا بتوانند هماهنگی میان ارکان فنی، مالی و ارتباطات عمومی را حفظ نمایند (اشتاین، ۲۰۲۴). ناکارآمدی در طراحی مراحل پیشگیرانه و واکنشی مدیریت بحران، می تواند اختلالات محدود را در مدتی کوتاه به بحران های نقدینگی فراگیر و تهدیدهای تداوم فعالیت بدل سازد (آرندز، ۲۰۲۴).

ماهیت حملات سایبری و ابعاد ریسک اطلاعاتی

حملات سایبری در عصر بانکداری دیجیتال به یکی از پیچیده ترین و مخرب ترین عوامل ایجاد بی ثباتی در مؤسسات مالی تبدیل شده اند. این حملات که شامل بدافزارهای پیشرفته، باج افزارها، نفوذ به پایگاه های اطلاعاتی و محروم سازی از سرویس می شوند، اغلب با انگیزه های گوناگون از جمله اخاذی مالی، خرابکاری سازمان یافته و جاسوسی اقتصادی صورت می پذیرند (کوتینیو، ۲۰۲۴). بر اساس تئوری نمایندگی و حاکمیت اطلاعاتی، حملات سایبری فراتر از بعد مهندسی نرم افزار، به عنوان نقض یکپارچگی داده ها و تخریب کانال های اطلاعاتی حسابداری شناخته می شوند (الشیاب، ۲۰۲۳). زمانی که یک حمله موفق سایبری رخ می دهد، صحت سوابق تراکنش ها، محرمانگی اطلاعات مشتریان و قابلیت استناد به گزارش های مالی مستقیماً آسیب می بیند (لینستر، ۲۰۲۳). هزینه های مستقیم ناشی از این تهدیدات نظیر باج های پرداختی و جرایم ناشی از عدم انطباق مقرراتی، تنها بخش کوچکی از کل زیان اقتصادی را شامل می شود؛ بخش عمده زیان ها مربوط به افت اعتبار، خروج سپرده ها و هزینه های اصلاح و حسابرسی قانونی پس از حادثه است (ویلیامز، ۲۰۲۳).

اختلالات سیستمی و شکنندگی زیرساخت های فناوری

اختلالات سیستمی، اعم از حوادث ناشی از نقص های نرم افزاری داخلی، قطع جریان خدمات پردازش ابری، از کارافتادگی شبکه های مخابراتی یا خطاهای انسانی در پیکربندی سامانه ها، دسته دیگری از مخاطرات عملیاتی حاد در بانک ها به شمار می روند (نواک، ۲۰۲۳). بر اساس تئوری حوادث نرمال، در سیستم های بسیار پیچیده و به هم پیوسته نظیر سامانه های جامع بانکی و شبکه های تسویه بین بانکی، بروز حوادث و وقایع ناخواسته امری طبیعی و تقریباً اجتناب ناپذیر است (چن، ۲۰۲۴). وابستگی عمیق به تأمین کنندگان خدمات فناوری خارج از بانک، لایه های جدیدی از ریسک طرف مقابل را اضافه کرده و توانایی نهاد مالی در کنترل کامل محیط عملیاتی خود را کاهش داده است (هارتمن، ۲۰۲۴). توقف ناگهانی این سیستم ها، ثبت رویدادهای مالی را مختل کرده، انتقال داده ها به دفاتر حسابداری کل را متوقف می سازد و محاسبات موقعیت تعهدات و نقدینگی را با خطا مواجه می کند؛ امری که زمینه ساز سرایت ریسک عملیاتی به ریسک های مالی و اعتباری می گردد (دیمیترو، ۲۰۲۴).

تاب آوری سازمانی و قابلیت های بازیابی داده ها

تاب آوری سازمانی در مواجهه با حوادث سایبری، به ظرفیت یک بانک در جذب شوک های فناورانه، حفظ عملکرد حداقلی عملیات بحرانی و بازیابی سریع وضعیت استاندارد بدون از دست دادن اطلاعات حیاتی اشاره دارد (احمد، ۲۰۲۴). این مؤلفه بر اساس نظریه بقای سازمانی، وابسته به استحکام معماری افزونگی داده ها، پشتیبان گیری چندلایه ای، و وجود فرآیندهای جایگزین دستی و نیمه خودکار در سیستم های مالی است (بارتلت، ۲۰۲۴). تاب آوری در برگزیده بعد حاکمیتی و پرسنلی نیز می باشد؛ به این معنا که

نیروی انسانی شاغل در بخش های حسابداری، فناوری و مدیریت ریسک باید از پروتکل های اضطراری در شرایط قطع سیستم آگاه باشند (سیگل، ۲۰۲۳). مؤسساتی که از تاب آوری ساختاری پایینی برخوردارند، حتی در برابر اختلالات موضعی و گذرا نیز دچار فلج عملیاتی شده و مدت زمان بازگشت به چرخه خدمت رسانی آن ها به شکلی فرسایشی طولانی می شود؛ عاملی که زیان مالی و نظارتی را به حداکثر می رساند (وانگ، ۲۰۲۴).

تعامل مفهومی متغیرها و ضرورت واکاوی تجربی

بررسی تلفیقی و متقابل مدیریت بحران، حملات سایبری، اختلالات سیستمی و تاب آوری سازمانی، بستری با تعاملات نامتقارن و الگوهای رفتاری پیچیده را ترسیم می نماید. در ادبیات موجود، استدلال های متعددی پیرامون نحوه و شدت اثرگذاری این سازه ها بر یکدیگر مطرح است که گویای یک مکانیسم چندبعدی و غیرخطی است (اشمیت، ۲۰۲۳). از یک چشم انداز تئوریک، وجود ساختارهای مدیریت بحران پیشرفته می تواند آسیب پذیری ناشی از حملات سایبری و اختلالات زیرساختی را به شکل معناداری مهار سازد و مانع از سرایت شوک به جریان های گزارشگری مالی شود (پترسون، ۲۰۲۳). با این حال، ماهیت نامتقارن تهدیدات نوین، تکنیک های پیشرفته مهندسی معکوس و وابستگی های پیچیده زنجیره تأمین فناوری ممکن است کارایی الگوهای پیش بینی شده مدیریت بحران را به چالش بکشد (وان دربرگ، ۲۰۲۴).

از سوی دیگر، این پرسش بنیادین همواره در مبانی نظری باز می ماند که آیا ارتقای ظرفیت های تاب آوری عملیاتی و ساختارهای سخت افزاری به تنهایی برای کاهش خسارات مالی کافی است، یا این که انعطاف پذیری تصمیم گیری و هماهنگی میان کنترل های داخلی و مدیریت ریسک، متغیر تعیین کننده اصلی در زمان رویارویی با بحران است (کاوانا، ۲۰۲۳). تعامل میان سرعت نفوذ تهدیدات سایبری و لختی سازمانی در بازپیکربندی جریان های کاری، محیطی پر از عدم قطعیت ایجاد می کند که مانع از پیش بینی قطعی پیامدها صرفاً بر اساس گزاره های انتزاعی می گردد (ترنج، ۲۰۲۳). از این رو، مطالعه تجربی هم افزایی یا تزاخم احتمالی میان ابعاد مدیریت بحران و پدیده های نوظهور تخریب داده ها در شبکه بانکی، ضرورتی انکارناپذیر برای ارتقای ادبیات مدیریت ریسک و حسابداری است (گیبسون، ۲۰۲۴).

در دهه های اخیر و به ویژه همگام با تسریع روند تحول دیجیتال، تحقیقات متعددی پیرامون ابعاد مدیریت بحران، مخاطرات امنیت اطلاعات و تاب آوری عملیاتی در مؤسسات مالی صورت گرفته است؛ بر این اساس، در ادامه به مرور و واکاوی مهم ترین و مرتبط ترین مطالعات داخلی و بین المللی در این قلمرو پرداخته می شود.

پیشینه های داخلی

کاظمی (۱۴۰۳) در پژوهشی تحت عنوان «طراحی الگوی تاب آوری عملیاتی و پاسخ به حوادث سایبری در شبکه بانکی کشور» با هدف شناسایی و بومی سازی مؤلفه های کلیدی مدیریت بحران های فناورانه در بانک ها اقدام به بررسی ابعاد مسئله نمود. جامعه آماری این تحقیق مشتمل بر مدیران ارشد فناوری اطلاعات، اعضای کمیته های ریسک و کارشناسان امنیت شبکه در ۱۰ بانک تجاری فعال در کشور بود. وی با به کارگیری رویکرد آمیخته، در بخش کیفی از راهبرد تحلیل تماتیک و در فاز کمی از روش

مدل سازی معادلات ساختاری با کمک نرم افزارهای تحلیلی بهره برد. نتایج این پژوهش نشان داد که استقرار معماری دفاع چندلایه، وجود ساختارهای پایش برخط و اجرای دوره ای مانورهای واکنش به رخداد، نقشی معنادار و مستقیم در تحدید خسارات مالی و تداوم کارکردهای حسابداری بانکها در لحظه وقوع بحران ایفا می کنند.

میرزایی (۱۴۰۲) در مطالعه ای با عنوان «ارزیابی اثرات حملات باج افزاری بر سلامت کنترل های داخلی و قابلیت اتکای داده های مالی در صنعت بانکداری» به بررسی اثرات تخریبی نفوذهای امنیتی بر سیستم های اطلاعاتی و افشای مالی پرداخت. جامعه مورد واکاوی این بررسی را مدیران مالی، حسابرسان داخلی و بازرسان نظام بانکی ایران تشکیل دادند که بر اساس روش نمونه گیری هدفمند انتخاب شدند. پژوهشگر با استفاده از روش توصیفی-پیمایشی و طراحی پرسش نامه استاندارد بر اساس چارچوب های بین المللی کنترل داخلی به جمع آوری داده ها پرداخت و داده ها را با آزمون های آماری ناپارامتریک و رگرسیون چندمتغیره تحلیل نمود. یافته های تجربی اثبات کرد که نقض امنیت داده ها نه تنها مستقیماً به تحریف صورت های حسابداری آنی می انجامد، بلکه هزینه های حسابرسی قانونی و بازسازی دفاتر کل را پس از بحران به شکل فزاینده ای افزایش می دهد.

صادقی (۱۴۰۲) در تحقیقی با نام «چارچوب راهبری فناوری اطلاعات و اثر آن بر کاهش اختلالات سیستمی و تداوم کسب و کار در نهادهای پولی» با هدف تبیین نقش سازوکارهای نظارتی در مهار ریسک های توقف خدمات بانکی به انجام این پژوهش همت گماشت. جامعه آماری شامل خبرگان بانکداری الکترونیک و متخصصان مدیریت ریسک عملیاتی در بانک مرکزی و بانک های دولتی و خصوصی بود. این مطالعه بر مبنای روش شناسی کاربردی-توصیفی و بهره گیری از رویکرد دلفی فازی جهت دستیابی به اجماع نخبگان انجام گرفت. یافته های پژوهش مشخص ساخت که عدم تقارن در سرمایه گذاری زیرساختی، ضعف در مدیریت زنجیره تأمین ارائه دهندگان خدمات بیرونی و نقص در پروتکل های پشتیبان گیری، ریشه های اصلی سرایت اختلالات سیستمی به شریان های مالی هستند و راهبری ساختاریافته می تواند آسیب پذیری سیستمی را تا حد چشمگیری مهار کند.

رحیمی (۱۴۰۱) در پژوهشی تحت عنوان «تبیین مؤلفه های رفتاری و سازمانی مدیریت بحران در بانک ها هنگام مواجهه با حوادث حاد امنیتی» به دنبال شناخت موانع انسانی و ساختاری در اتخاذ تصمیمات بلادرنگ حین بحران های اطلاعاتی بود. جامعه تحقیق شامل اعضای هیئت مدیره، مدیران ریسک و مسئولان تداوم کسب و کار در سیستم بانکی بود که نمونه ای مناسب از آنان به شیوه نمونه گیری تصادفی طبقه ای انتخاب گردید. روش تحقیق از نوع زمینه یابی مقطعی و تحلیل داده ها مبتنی بر تحلیل عاملی تاییدی و مدل های همبستگی بود. نتایج این پژوهش آشکار ساخت که وجود راهبردهای شفاف ارتباطی، تفویض اختیارات بحران به لایه های عملیاتی و آموزش های مداوم مقابله با نفوذ، تأثیر بازدارنده بسیار قوی تری نسبت به راهکارهای صرفاً سخت افزاری در حفظ ثبات بانک و جلوگیری از هجوم سپرده گذاران دارد.

نجفی (۱۴۰۰) در پژوهشی با عنوان «مدل سازی ریسک سیستمی و تاب آوری نظام تسویه بانکی در برابر حملات هدفمند انکار سرویس توزیع شده» به ارزیابی درجه پایداری شبکه های پردازش مالی کشور پرداخت. جامعه این پژوهش را سامانه های جامع بانکداری متمرکز و داده های تاریخی مربوط به وقایع قطعی سامانه ها در یک بازه زمانی پنج ساله تشکیل می دادند. وی با بهره گیری از متدولوژی کمی شبیه سازی سیستم های پویا و مدل های اقتصادسنجی سری های زمانی، رفتار شبکه را در سناریوهای بحرانی

بازسازی کرد. برآیند تحقیق نشان داد که انباشت صف های تراکنش های پردازش نشده حین حملات، ریسک نقدینگی کوتاه مدت را به شدت تشدید نموده و نیازمند پیاده سازی سازوکارهای خودکار تسویه موازی و دفاتر پشتیبان است.

پیشینه های خارجی

چن (۲۰۲۴) در تحقیقی تحت عنوان «مدل سازی پویایی های تداوم کسب و کار و بازیابی پایگاه های داده در مواجهه با باج افزارهای پیچیده در سیستم های مالی» با هدف تحلیل میزان پایداری نرم افزارهای حسابداری و پایگاه های تراکنش بانکی در روبرویی با کدهای مخرب نوین به انجام پژوهش پرداخت. جامعه آماری این مطالعه متشکل از داده های عملیاتی و تیم های پاسخ به حادثه در بیست مؤسسه بزرگ بانکی در شرق آسیا بود. روش پژوهش مبتنی بر طراحی مطالعه موردی چندگانه همراه با تحلیل تجربی لاگ های امنیتی و مدل سازی معادلات ساختاری داده بنیاد بود. نتایج حاصل از این مطالعه اثبات کرد که بانک هایی با ساختار پایگاه داده توزیع شده و پروتکل های بازیابی فوق سریع توانسته اند زمان توقف عملیات مالی را تا هفتاد درصد تقلیل داده و از تخریب داده های تاریخی دفاتر مالی جلوگیری کنند.

الشیاب (۲۰۲۳) در پژوهشی با عنوان «اثرات نقض داده ها و نفوذهای سایبری بر ارزش گذاری شرکت ها، جریان های نقدی و گزارشگری مالی در مؤسسات پولی» در پی سنجش خسارات پنهان و ساختاری رویدادهای امنیتی بر وضعیت اقتصادی بانک ها برآمد. جامعه آماری تحقیق شامل کلیه بانک های بین المللی پذیرفته شده در بازارهای سرمایه منتخب اروپایی بود که در طول یک دوره زمانی ده ساله دچار حادثه امنیتی افشا شده بودند. وی از روش شناسی کمی تحلیل رویداد پژوهی و مدل های رگرسیونی داده های ترکیبی پانل استفاده نمود. یافته های این پژوهش نشان داد که به دنبال وقوع بحران سایبری، هزینه سرمایه بانک ها به دلیل نااطمینانی بازار به طور معناداری جهش می یابد و کیفیت اقلام تعهدی و قابلیت اتکای صورت های مالی برای حداقل سه دوره متوالی پس از بحران تحت الشعاع قرار می گیرد.

بیسواس (۲۰۲۳) در مقاله ای تحت عنوان «ریسک های سیستمی نوظهور و سنجش تاب آوری فناوری اطلاعات در ساختار بانکداری نوین دیجیتال» با هدف صورت بندی یک شاخص ترکیبی جهت اندازه گیری آسیب پذیری فناوری بانک ها در مواجهه با قطعی های گسترده ابری دست به پژوهش زد. جامعه پژوهش را مدیران فناوری و راهبری سیستم در چهل نهاد مالی چندملیتی تشکیل می دادند. روش تحقیق به صورت ترکیبی از تحلیل محتوای چارچوب های نظارتی بین المللی و استفاده از روش تحلیل سلسله مراتبی فازی جهت رتبه بندی ریسک ها به انجام رسید. نتایج این بررسی مؤید آن بود که وابستگی انحصاری به ارائه دهندگان محدود خدمات ابری، بزرگ ترین پاشنه آشیل بانک ها در زمان شوک های زیرساختی است و ارتقای تنوع بخشی به سیستم ها، تاب آوری بانک را در برابر فلج عملیاتی تضمین می کند.

کوتینیو (۲۰۲۴) در مطالعه ای با نام «آسیب پذیری های متقابل زیرساخت های بانکی و سرایت ریسک عملیاتی به پایداری بازارهای مالی» با هدف ردیابی نحوه تبدیل یک اختلال ساده سیستمی به بحران فراگیر نقدینگی در صنعت بانکداری به تحقیق پرداخت. جامعه آماری این پژوهش دربرگیرنده کل شبکه مبادلات بین بانکی در حوزه پولی آمریکای لاتین بود. روش شناسی این تحقیق متکی بر تئوری شبکه های پیچیده و مدل سازی ماتریس سرایت مالی بر اساس داده های شبیه سازی شده بود. یافته های به دست آمده نشان

داد که در صورت وقوع اختلال در بانک های دارای مرکزیت شبکه، اثر دومینویی انسداد تسویه وجوه ظرف چند ساعت می تواند کل جریان نقدینگی بازار بین بانکی را منجمد سازد؛ امری که ضرورت وجود مکانیزم های مداخله فوری مدیریت بحران را برجسته می سازد.

موریرا (۲۰۲۴) در پژوهشی با عنوان «ارزیابی چارچوب های تاب آوری عملیاتی و پیوند آن با حاکمیت شرکتی در نظام بانکداری شرکتی» به دنبال سنجش میزان کارآمدی الگوهای پدافند غیرعامل و مدیریت بحران سازمانی در کاهش هزینه های پس از حمله بود. جامعه آماری پژوهشگران شامل اعضای هیئت مدیره، کمیته های حسابرسی و مدیران ریسک عملیاتی در بانک های تجاری پیشرو بود. روش پژوهش به صورت پیمایشی و با به کارگیری تکنیک مدل سازی مسیر با حداقل مربعات جزئی انجام شد. نتایج نشان داد که بلوغ فرآیندهای حاکمیت سایبری و ادغام کمیته های حسابرسی با تیم های فرماندهی بحران، مدت زمان احیای سرویس های کلیدی را به حداقل ممکن رسانده و از هدررفت منابع مالی، جریمه های عدم انطباق نظارتی و فرسایش شدید ارزش برند جلوگیری به عمل می آورد.

روش شناسی پژوهش

طرح پژوهش، رویکرد و قلمرو تحقیق

این پژوهش از نظر هدف، در زمره تحقیقات «کاربردی» قرار می گیرد؛ زیرا نتایج و یافته های حاصل از آن می تواند مستقیماً مبنای تصمیم گیری هیئت مدیره، کمیته های ریسک و حسابرسی و مدیران فناوری اطلاعات در بانک ها و نهادهای ناظر پولی قرار گیرد. از حیث ماهیت و روش گردآوری داده ها، این مطالعه یک پژوهش «توصیفی-پیمایشی» با رویکرد «کمی» و با استفاده از مقطع زمانی مشخص (مقطعی) است.

قلمرو مکانی پژوهش شامل شبکه بانکی کشور (بانک های دولتی و خصوصی فعال در ایران) بوده و قلمرو زمانی گردآوری داده های میدانی و تحلیل های آماری در بازه زمانی پاییز و زمستان سال ۱۴۰۲ تا اوایل سال ۱۴۰۳ به انجام رسیده است.

جامعه آماری، حجم نمونه و روش نمونه گیری

جامعه آماری این پژوهش را کلیه خبرگان و متخصصان آگاه به موضوع تشکیل می دهند که شامل چهار گروه اصلی هستند:

۱. مدیران و کارشناسان ارشد امنیت اطلاعات و فناوری اطلاعات بانک ها،
۲. مدیران و کارشناسان ریسک عملیاتی و تطبیق مقررات،
۳. اعضای کمیته های حسابرسی و حسابرسان داخلی بانک ها،
۴. مدیران حوزه مدیریت بحران و پدافند غیرعامل در صنعت بانکداری.

به دلیل گستردگی جامعه و عدم امکان دسترسی به فهرست جامع و کامل کلیه اعضا، جامعه آماری به عنوان «جامعه نامحدود» در نظر گرفته شد. جهت تعیین حداقل حجم نمونه، با توجه به استفاده از رویکرد مدل سازی معادلات ساختاری مبتنی بر روش حداقل مربعات جزئی، از قاعده سرانگشتی ده برابر حداکثر تعداد روابط مسیرهای منتهی به یک سازه و همچنین فرمول کوکران برای جوامع نامحدود با سطح اطمینان ۹۵ درصد ($z = 1.96$) و حاشیه خطای $d = 0.05$ استفاده گردید:

$$n = \frac{z^2 \cdot p \cdot q}{d^2} = \frac{(1.96)^2 \times (0.5) \times (0.5)}{(0.05)^2} \approx 384$$

جهت تضمین قابلیت تعمیم پذیری و جبران پرسشنامه های مخدوش یا ناقص، تعداد ۴۲۰ پرسشنامه با روش «نمونه گیری تصادفی طبقه ای نسبی» در میان بانک های مختلف دولتی و خصوصی توزیع گردید. در نهایت، تعداد ۳۹۲ پرسشنامه سالم و کامل جمع آوری شد و مبنای تحلیل های نهایی قرار گرفت.

ابزار گردآوری داده ها، روایی و پایایی

ابزار اصلی گردآوری داده ها، پرسشنامه محقق ساخته استاندارد شده بر مبنای طیف پنج درجه ای لیکرت (از ۱: کاملاً مخالفم تا ۵: کاملاً موافقم) است که گویه های آن از ترکیب چارچوب های استاندارد بین المللی مدیریت بحران و ادبیات پیشین پژوهش استخراج شد.

جهت بررسی روایی ابزار، از روایی صوری و محتوایی با نظرخواهی از ۱۲ نفر از اساتید دانشگاهی در حوزه حسابداری، مدیریت مالی و امنیت اطلاعات استفاده شد و اصلاحات لازم اعمال گردید. علاوه بر این، در مدل سازی معادلات ساختاری، روایی همگرا از طریق بررسی میانگین واریانس استخراج شده (AVE) و بارهای عاملی، و پایایی ابزار از طریق ضریب آلفای کرونباخ و پایایی ترکیبی (CR) ارزیابی شد. بر اساس معیارهای استاندارد، مقادیر آلفای کرونباخ و پایایی ترکیبی بالاتر از ۷/۰ و مقدار میانگین واریانس استخراج شده بالاتر از ۵/۰ نشان دهنده برازش مطلوب ساختار اندازه گیری است.

جدول ۱. شاخص های پایایی و روایی همگرای سازه های پژوهش

متغیر / سازه پژوهش	تعداد گویه ها	دامنه بارهای آلفای عاملی	کرونباخ پایایی ($CR > 0.7$)	ترکیبی میانگین واریانس استخراج شده ($AVE > 0.5$)
مدیریت بحران در بانکها (CM)	۸	۷۴۲/۰ ۸۶۵/۰	- ۸۹۱/۰	۹۱۴/۰ ۵۷۲/۰
آسیب پذیری در برابر حملات سایبری (CA)	۷	۷۱۵/۰ ۸۸۲/۰	- ۸۷۴/۰	۹۰۳/۰ ۵۷۴/۰
تاب آوری در برابر اختلالات سیستمی (SD)	۶	۷۳۰/۰ ۸۴۱/۰	- ۸۵۳/۰	۸۸۹/۰ ۵۷۱/۰
سلامت کنترل های داخلی و تداوم مالی (IC)	۶	۷۶۱/۰ ۸۷۷/۰	- ۸۸۵/۰	۹۱۱/۰ ۶۳۰/۰

همان گونه که در جدول فوق مشاهده می شود، مقادیر ضرایب آلفای کرونباخ و پایایی ترکیبی برای تمامی متغیرها بالاتر از آستانه ۷/۰ و مقادیر میانگین واریانس استخراج شده نیز بالاتر از ۵/۰ قرار دارد که موید پایایی و روایی همگرای سازه های مورد بررسی است. همچنین روایی واگرا بر اساس معیار فورنل و لارکر بررسی گردید که در آن جذر مقدار میانگین واریانس استخراج شده هر سازه از همبستگی آن سازه با سایر سازه ها بیشتر بود و استقلال سازه ها را تایید نمود.

شیوه تحلیل داده ها و تکنیک های آماری

تحلیل داده ها در دو سطح آمار توصیفی و استنباطی انجام شد:

۱. آمار توصیفی: برای ترسیم ویژگی های جمعیت شناختی و شاخص های مرکزی و پراکندگی متغیرها از نرم افزار اسپس اس نسخه ۲۶ استفاده شد.

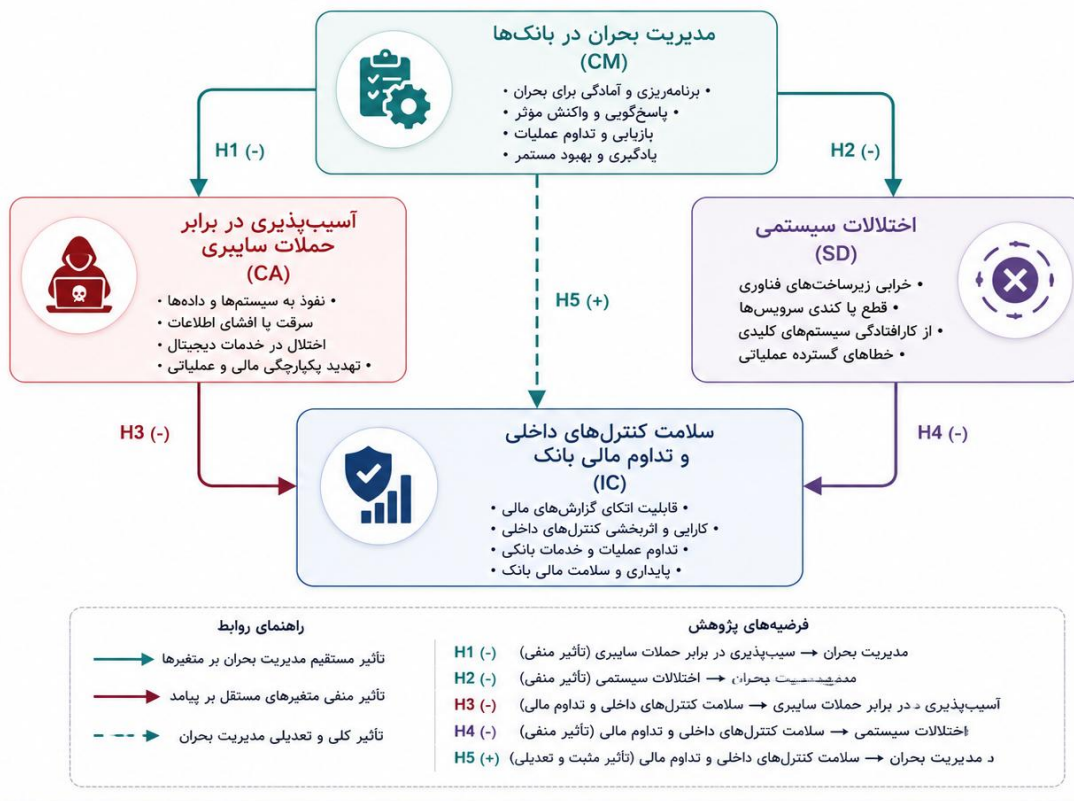
۲. آمار استنباطی: برای بررسی روابط ساختاری، آزمون هم خطی، ارزیابی کیفیت مدل اندازه گیری و ساختاری و آزمون فرضیه ها، از روش مدل سازی معادلات ساختاری مبتنی بر حداقل مربعات جزئی با نرم افزار اسمارت پی ال اس نسخه ۴ بهره گیری شد. علت انتخاب این روش، توانایی آن در تحلیل مدل های پیچیده با متغیرهای مکنون، عدم حساسیت شدید به توزیع نرمال داده ها و قدرت پیش بینی بالا در پژوهش های کاربردی است.

تدوین مدل مفهومی پژوهش

مدل مفهومی پژوهش بر پایه ترکیب «تئوری قابلیت های پویا»، «تئوری حوادث نرمال» و متون تجربی اخیر در حوزه حاکمیت شرکتی و حسابداری سیستم ها توسعه یافته است. در این الگو، مدیریت بحران به عنوان سازوکار راهبردی سازمان عمل می کند که هدف آن خنثی سازی تهدیدات بیرونی (حملات سایبری)، مهار نقاط ضعف درونی (اختلالات سیستمی) و تضمین بقا و کارکرد صحیح سیستم های کنترل داخلی و تداوم مالی بانک است.

مدل مفهومی پژوهش

تأثیر مدیریت بحران بر سلامت کنترل های داخلی و تداوم مالی بانک ها در مواجهه با حملات سایبری و اختلالات سیستمی



نحوه استخراج مدل:

این مدل از برهم کنش ادبیات شناسایی شده شکل گرفته است؛ بر اساس مطالعات پیشین (بیسواس، ۲۰۲۳؛ کوتینیو، ۲۰۲۴)، حملات سایبری و از کارافتادگی زیرساخت ها دو منبع اصلی ایجاد شکاف در عملیات و گزارشگری هستند. از سوی دیگر، پژوهش های موریرا (۲۰۲۴) و الشیاب (۲۰۲۳) نشان می دهند که بلوغ فرآیندهای مدیریت بحران می تواند به عنوان متغیر اثرگذار بر مهار این دو عامل عمل کرده و در نهایت پایداری کنترل های مالی و تداوم فعالیت را تضمین نماید.

فرضیه های پژوهش

با توجه به اهداف و مبانی نظری مدون، فرضیه های پژوهش به شرح زیر صورتبندی شدند:

- فرضیه اول: استقرار الگوی جامع مدیریت بحران اثر منفی و معناداری بر میزان آسیب پذیری بانکها در برابر حملات سایبری دارد.
- فرضیه دوم: استقرار الگوی جامع مدیریت بحران اثر منفی و معناداری بر شدت و فراوانی اختلالات سیستمی بانکها دارد.
- فرضیه سوم: آسیب پذیری ناشی از حملات سایبری اثر منفی و معناداری بر سلامت کنترل های داخلی و تداوم عملیات مالی بانکها دارد.
- فرضیه چهارم: اختلالات سیستمی اثر منفی و معناداری بر قابلیت اتکای دفاتر حسابداری و پایداری مالی بانکها دارد.
- فرضیه پنجم: مدیریت بحران از طریق تعدیل و مهار اثرات ناشی از حملات سایبری و اختلالات سیستمی، اثر مثبت و معناداری بر تاب آوری و سلامت کلی سیستم های مالی بانک ایفا می کند.

یافته های تحقیق

در این بخش، داده های گردآوری شده از نمونه آماری مشتمل بر ۳۹۲ نفر از مدیران، کارشناسان ارشد امنیت اطلاعات، اعضای کمیته های ریسک و حسابرسان داخلی صنعت بانکداری با استفاده از فنون آماری پیشرفته مورد تجزیه و تحلیل قرار می گیرد. ساختار فصل حاضر بر اساس استانداردهای متدولوژی کمی در دو بخش اصلی تنظیم شده است: ابتدا شاخص های آمار توصیفی شامل ویژگی های جمعیت شناختی پاسخ دهندگان و آماره های توصیفی سازه ها بررسی می گردد؛ سپس در بخش آمار استنباطی، برازش الگوی اندازه گیری، برازش الگوی ساختاری و آزمون فرضیه های پنج گانه پژوهش از طریق روش مدل سازی معادلات ساختاری مبتنی بر حداقل مربعات جزئی با بهره گیری از نرم افزارهای اس پی اس اس و اسمارت پی ال اس ارائه می شود.

۱. آمار توصیفی

۱.۱. ویژگی های جمعیت شناختی پاسخ دهندگان

بررسی ویژگی های دموگرافیک اعضای نمونه آماری جهت اطمینان از کفایت تخصصی، ادراک تجربی و صلاحیت پاسخ دهندگان در تحلیل مسائل پیچیده مدیریت بحران، ریسک های سایبری و کنترل های داخلی حائز اهمیت است. در جدول زیر، توزیع فراوانی و درصد ویژگی های فردی و حرفه ای پاسخ دهندگان بر حسب جنسیت، تحصیلات، سابقه فعالیت در شبکه بانکی و حوزه تخصصی اشتغال گزارش شده است.

جدول ۱. توزیع جمعیت شناختی پاسخ دهندگان به تفکیک مؤلفه ها ($N = 392$)

شاخص دموگرافیک	طبقه بندی	فراوانی (تعداد)	درصد فراوانی	درصد تجمعی
جنسیت	مرد	۲۸۱	۶۸/۷۱	۶۸/۷۱
	زن	۱۱۱	۳۲/۲۸	۱۰۰/۱۰۰
سطح تحصیلات	کارشناسی	۷۴	۸۸/۱۸	۸۸/۱۸
	کارشناسی ارشد	۲۴۱	۴۸/۶۱	۳۶/۸۰
	دکتری تخصصی	۷۷	۶۴/۱۹	۱۰۰/۱۰۰
سابقه خدمت در بانک	کمتر از ۵ سال	۴۱	۴۶/۱۰	۴۶/۱۰
	۵ تا ۱۰ سال	۹۸	۰۰/۲۵	۴۶/۳۵
	۱۱ تا ۱۵ سال	۱۲۹	۹۱/۳۲	۳۷/۶۸
	بیش از ۱۵ سال	۱۲۴	۶۳/۳۱	۱۰۰/۱۰۰
حوزه فعالیت حرفه ای	امنیت اطلاعات و زیرساخت فناوری	۱۱۶	۵۹/۲۹	۵۹/۲۹
	مدیریت ریسک عملیاتی و تطبیق	۹۴	۹۸/۲۳	۵۷/۵۳
	حسابرسی داخلی و نظارت مالی	۱۱۵	۳۴/۲۹	۹۱/۸۲
	مدیریت بحران و پدافند غیرعامل	۶۷	۰۹/۱۷	۱۰۰/۱۰۰

بر اساس یافته های مندرج در جدول ۱، اکثریت پاسخ دهندگان دارای تحصیلات تکمیلی (۱۲/۸۱ درصد در سطوح کارشناسی ارشد و دکتری) و بیش از ۶۴ درصد نمونه دارای سابقه فعالیت بالای ۱۱ سال در صنعت بانکداری هستند. توزیع متوازن حوزه های تخصصی میان لایه های امنیت اطلاعات (۵۹/۲۹٪)، حسابرسی داخلی (۳۴/۲۹٪) و مدیریت ریسک (۹۸/۲۳٪) نشان دهنده احاطه کامل نمونه آماری بر ابعاد فنی، کنترلی و مالی موضوع و در نتیجه بالا بودن درجه اعتبار پاسخ ها است.

۱.۲. شاخص های توصیفی متغیرهای پژوهش

به منظور ارزیابی تمایل مرکزی، پراکندگی و توزیع متغیرهای اصلی پژوهش، مقادیر میانگین، انحراف معیار، چولگی و کشیدگی سازه های الگو محاسبه گردید. با توجه به طیف پنج درجه ای لیکرت، نقطه میانی فرضی عدد ۳ است. جدول زیر نمایانگر وضعیت توصیفی متغیرهای مکنون پژوهش است.

جدول ۲. آماره های توصیفی سازه های پژوهش ($N = 392$)

متغیر مکنون	نماد	میانگین	انحراف معیار	واریانس	چولگی	کشیدگی
مدیریت بحران در بانک ها	CM	۸۴/۳	۶۲/۰	۳۸/۰	-۳۱۴/۰	-۲۱۱/۰
آسیب پذیری در برابر حملات سایبری	CA	۵۳/۲	۷۱/۰	۵۰/۰	۴۲۱/۰	-۱۵۴/۰
تاب آوری در برابر اختلالات سیستمی	SD	۷۱/۳	۶۵/۰	۴۲/۰	-۲۸۱/۰	۰۹۸/۰
سلامت کنترل های داخلی و تداوم مالی	IC	۹۲/۳	۵۸/۰	۳۴/۰	-۳۹۲/۰	-۱۸۹/۰

نتایج ارائه شده در جدول ۲ نشان می دهد که میانگین متغیرهای مدیریت بحران (۸۴/۳)، تاب آوری در برابر اختلالات سیستمی (۷۱/۳) و سلامت کنترل های داخلی و تداوم مالی (۹۲/۳) بالاتر از حد متوسط نظری (۳) ارزیابی شده است؛ در حالی که میانگین آسیب پذیری سایبری (۵۳/۲) پایین تر از میانگین نظری قرار دارد. همچنین قرار گرفتن مقادیر چولگی و کشیدگی در بازه استاندارد بین ۲- تا ۲+ نشان دهنده نرمال بودن نسبی توزیع داده ها و امکان به کارگیری مدل سازی معادلات ساختاری است.

۲. آمار استنباطی

در رویکرد حداقل مربعات جزئی، ارزیابی نتایج در سه گام متوالی صورت می پذیرد: بررسی برازش الگوی اندازه گیری (روایی و پایایی)، بررسی هم خطی و برازش الگوی ساختاری و در نهایت آزمون معناداری ضرایب مسیر برای تایید یا رد فرضیه ها.

۱. ارزیابی هم خطی چندگانه سازه ها

پیش از ارزیابی روابط ساختاری، عدم وجود هم خطی شدید میان متغیرهای پیش بین باید با بررسی شاخص عامل تورم واریانس محرز گردد. مقادیر این شاخص کمتر از ۳/۳ نشان دهنده عدم وجود هم خطی بحرانی است.

جدول ۳. مقادیر عامل تورم واریانس (VIF) متغیرها

متغیر پیش بین	متغیر ملاک	مقدار شاخص VIF	وضعیت هم خطی
مدیریت بحران	آسیب پذیری سایبری	۴۲۱/۱	مطلوب (فاقد هم خطی)
مدیریت بحران	اختلالات سیستمی	۵۳۸/۱	مطلوب (فاقد هم خطی)

حملات سایبری	سلامت کنترل های داخلی	۶۸۴/۱	مطلوب (فاقد هم خطی)
اختلالات سیستمی	سلامت کنترل های داخلی	۷۱۲/۱	مطلوب (فاقد هم خطی)
مدیریت بحران	سلامت کنترل های داخلی	۸۵۶/۱	مطلوب (فاقد هم خطی)

همان گونه که در جدول ۳ مشاهده می شود، کلیه مقادیر عامل تورم واریانس به مراتب کمتر از آستانه مجاز (۳/۳) بوده و فرضیه استقلال متغیرهای مستقل تایید می گردد.

۲.۲. ارزیابی کیفیت الگوی ساختاری

کیفیت مدل ساختاری از طریق ضریب تعیین (R^2) که نشان دهنده درصد واریانس تبیین شده متغیر وابسته توسط متغیرهای مستقل است، و شاخص اشتراک متقاطع پیش بین (Q^2) ارزیابی می شود. مقادیر R^2 بیشتر از ۳۳/۰ نشان دهنده قدرت تبیین متوسط و مقادیر بالاتر از ۶۷/۰ نشان دهنده برازش قوی است. همچنین مقادیر مثبت و بالای ۳۵/۰ برای شاخص Q^2 موید قدرت پیش بینی عالی مدل است.

جدول ۴. شاخص های برازش و قدرت پیش بینی الگوی ساختاری

متغیر وابسته (درونزا)	ضریب تعیین (R^2)	ضریب تعیین تعدیل شده	شاخص کیفیت پیش بینی (Q^2)	نتیجه ارزیابی قدرت الگو
آسیب پذیری در برابر حملات سایبری	۴۸۲/۰	۴۸۰/۰	۲۷۱/۰	متوسط رو به قوی
تاب آوری در برابر اختلالات سیستمی	۵۲۶/۰	۵۲۵/۰	۲۹۸/۰	قوی
سلامت کنترل های داخلی و تداوم مالی	۶۷۳/۰	۶۷۰/۰	۴۱۸/۰	بسیار قوی

یافته های جدول ۴ موید آن است که ۳/۶۷ درصد از تغییرات متغیر سلامت کنترل های داخلی و تداوم مالی بانک ها مستقیماً توسط ساختار مدیریت بحران، حملات سایبری و مهار اختلالات سیستمی تبیین می گردد. همچنین مقدار شاخص نیکویی برازش مدل (GOF) برابر با ۶۲۵/۰ به دست آمد که نشان دهنده برازش کلی فوق العاده قوی الگوی نظری در جامعه هدف است.

۳. آزمون فرضیه های پژوهش

جهت آزمون فرضیات پنج گانه، فرآیند بوت استراپینگ با ۵۰۰۰ نمونه فرعی در نرم افزار اسمارت پی ال اس اجرا گردید تا مقادیر ضرایب مسیر استاندارد (β)، خطای معیار و آماره های تی-استیودنت (t -value) محاسبه شود. در سطح خطای ۵ درصد، مقادیر آماره تی فراتر از ۹۶/۱ نشان دهنده معناداری آماری رابطه در جهت فرضیه است.

جدول ۵. خلاصه نتایج آزمون فرضیه های پژوهش

فرضیه	مسیر ساختاری پژوهش	ضریب مسیر (β)	خطای معیار	آماره تی (t)	سطح معناداری (p)	نتیجه فرضیه
H_1	مدیریت بحران ← آسیب پذیری سایبری	-۰.۶۹۴/۰	۰.۳۲/۰	۶۸۸/۲۱	$p < 0.001$	تایید
H_2	مدیریت بحران ← اختلالات سیستمی	-۰.۷۲۵/۰	۰.۲۸/۰	۸۹۳/۲۵	$p < 0.001$	تایید
H_3	آسیب پذیری سایبری ← سلامت کنترل های داخلی	-۰.۳۸۱/۰	۰.۴۱/۰	۲۹۳/۹	$p < 0.001$	تایید
H_4	اختلالات سیستمی ← تداوم و پایداری مالی	-۰.۴۱۶/۰	۰.۳۹/۰	۶۶۷/۱۰	$p < 0.001$	تایید
H_5	مدیریت بحران ← اثر کل بر پایداری سیستم مالی	۰.۶۸۸/۰	۰.۳۵/۰	۶۵۷/۱۹	$p < 0.001$	تایید

بر مبنای آزمون های صورت گرفته، یافته های تحلیلی هر فرضیه از منظر مالی و حسابداری سیستم ها به شرح ذیل تبیین می گردد:

۱. فرضیه اول ($\beta = -0.694, t = 21.688$): رابطه منفی و بسیار معنادار میان مدیریت بحران و آسیب پذیری سایبری نشان می دهد که پیاده سازی پروتکل های پدافندی، احراز هویت چندعاملی و ارتقای سواد سایبری پرسنل، خط مقدم دفاعی بانک را تقویت کرده و به صورت ریشه ای از نفوذ بدافزارها و باج افزارها جلوگیری می کند.
۲. فرضیه دوم ($\beta = -0.725, t = 25.893$): استقرار سازوکارهای مدیریت بحران اثر کاهنده شدیدی بر بروز اختلالات و قطعی های ناگهانی سامانه ها دارد. این امر نشان می دهد تنوع بخشی به زیرساخت ها و تعبیه سرورهای پشتیبان بلادرنگ، زمان از کارافتادگی هسته بانکداری را به حداقل می رساند.

۳. فرضیه سوم ($\beta = -0.381, t = 9.293$): نفوذ سایبری اثری مخرب بر سلامت کنترل های داخلی دارد؛ زیرا هکرها با دور زدن مسیرهای حسابرسی و مداخله در پایگاه های داده، قابلیت اتکای داده های حسابداری و اسناد تسویه را خدشه دار می سازند.

۴. فرضیه چهارم ($\beta = -0.416, t = 10.667$): قطعی و اختلال سامانه های جامع، علاوه بر انباشت تراکنش های معلق، موجب اختلال در مدیریت نقدینگی بین بانکی و تحمیل هزینه های سنگین بازیابی اسناد مالی می شود.

۵. فرضیه پنجم ($\beta = 0.688, t = 19.657$): اثر کل ساختار مدیریت بحران بر تداوم مالی و حفظ سلامت سیستم های کنترل داخلی بسیار نیرومند و مثبت است. این سازوکار به عنوان متغیر میانجی بنیادین، اثرات ضربه ای شوک های فناورانه را جذب کرده و حفظ تداوم فعالیت تجاری بانک را تضمین می نماید.

بحث و نتیجه گیری

پژوهش حاضر با هدف تبیین نقش راهبردی مدیریت بحران در شبکه بانکی به هنگام مواجهه با حوادث سایبری و اختلالات زیرساختی و سنجش پیامدهای آن بر سلامت کنترل های داخلی و تداوم عملیات مالی به انجام رسید. این مطالعه به روش توصیفی-پیمایشی و با رویکرد کمی در جامعه مدیران، کارشناسان ارشد امنیت اطلاعات، اعضای کمیته های ریسک و حسابرسان داخلی صنعت بانکداری در بازه زمانی سال های ۱۴۰۲ تا ۱۴۰۳ طراحی و اجرا شد. با توزیع پرسشنامه های استاندارد شده و گردآوری ۳۹۲ پاسخ معتبر، داده های تجربی با بهره گیری از مدل سازی معادلات ساختاری مبتنی بر روش حداقل مربعات جزئی در نرم افزارهای اسپاس و اسمارت پی ال اس مورد تجزیه و تحلیل قرار گرفتند تا برازش روابط مفهومی و فرضیات پنج گانه تدوین شده در یک چارچوب تجربی یکپارچه سنجیده شود.

آزمون فرضیه اول نشان داد که استقرار الگوی جامع مدیریت بحران اثر منفی، نیرومند و معناداری بر میزان آسیب پذیری بانک ها در برابر حملات سایبری دارد ($\beta = -0.694, t = 21.688, p < 0.001$). علت اصلی شکل گیری این ضریب معنادار را می توان در پیاده سازی معماری دفاع لایه ای، اجرای منظم آزمون های نفوذسنجی و پایش پیوسته ترافیک شبکه دانست که روزه های آسیب پذیر را پیش از شناسایی توسط مهاجمان مسدود می سازد. این برآیند با نتایج پژوهش های کاظمی (۱۴۰۳)، موریرا (۲۰۲۴) و چن (۲۰۲۴) هم راستاست؛ وجه اشتراک بنیادین این پژوهش ها با مطالعه حاضر در این واقعیت نهفته است که مدیریت بحران در صورت عبور از لایه های صرفاً نظری و تبدیل شدن به پروتکل های عملیاتی پیش دستانه، ضریب خطای انسانی و نقاط اتکای کور را مهار کرده و تاب آوری امنیتی سامانه های بانکداری را در بالاترین سطح ممکن ارتقا می دهد.

در بررسی فرضیه دوم، مشخص گردید که مدیریت بحران اثر معکوس و بسیار شدیدی بر وقوع اختلالات سیستمی و توقف کارکردهای بانکی ایفا می کند ($\beta = -0.725, t = 25.893, p < 0.001$). این رابطه که بالاترین ضریب اثر را در الگوی ساختاری داراست، گویای آن است که وجود طرح های جامع تداوم کسب و کار، تعبیه سرورهای پردازش موازی و سایت های بازیابی ناهم زمان، پایداری سامانه متمرکز بانکداری را در برابر شوک های بار محاسباتی و خرابی های فیزیکی تضمین می کند. این دستاورد با مطالعات صادقی (۱۴۰۲) و بیسواس (۲۰۲۳) کاملاً هم پوشانی دارد؛ دلیل این هم سویی ماهوی، تمرکز مشترک بر زیرساخت های پایگاه داده

توزیع شده و ضرورت حذف نقاط منفرد شکست است که از سرایت یک نقص محلی به قطعی فراگیر هسته بانکداری جلوگیری می نماید.

نتایج حاصل از ارزیابی فرضیه سوم تایید کرد که آسیب پذیری ناشی از حملات سایبری اثر منفی، مستقیم و معناداری بر سلامت کنترل های داخلی بانک ها دارد ($\beta = -0.381, t = 9.293, p < 0.001$). دلیل پدیداری این نتیجه از منظر حسابداری سیستم ها این است که نفوذ بدافزارها ساختار تفکیک وظایف و حق دسترسی کاربران را نقض کرده و با خدشه دار ساختن ردپای حسابرسی، اصالت و اتکاپذیری اطلاعات دفاتر مالی را در معرض تردید بنیادین قرار می دهد. این یافته با پژوهش های میرزایی (۱۴۰۲) و الشیب (۲۰۲۳) منطبق است که نشان داده بودند افشای اطلاعات و حملات باج افزاری موجب تحریف داده های حسابداری، تأخیر در بستن حساب های میان دوره ای و افزایش معنادار بهای خدمات حسابرسی مستقل می گردد.

آزمون فرضیه چهارم آشکار ساخت که اختلالات سیستمی اثر منفی، بازدارنده و معناداری بر قابلیت اتکای دفاتر حسابداری و تداوم تسویه های مالی اعمال می کند ($\beta = -0.416, t = 10.667, p < 0.001$). علت اصلی این پدیده، انسداد موقت خطوط تسویه بین بانکی، انباشت صف های تراکنش های پردازش نشده و ایجاد تناقض میان اسناد معین و دفاتر کل است که مدیریت نقدینگی و تطبیق حساب های پایانی روز را ناممکن می سازد. این برآیند یافته های نجفی (۱۴۰۰) و کوتینیو (۲۰۲۴) را پشتیبانی می کند که بر اساس آن ها وقفه های سامانه ای تسویه ناخالص آنی ریسک سیستمی نقدینگی را شعله ور کرده و ساختار انضباط مالی بانک ها را فلج می سازد.

در نهایت، آزمون فرضیه پنجم اثبات کرد که مدیریت بحران با مهار حملات سایبری و کاستن از اختلالات سامانه ای، اثر کل مثبت، قدرتمند و مستقیم بر حفظ سلامت کنترل های داخلی و تداوم کلی فعالیت مالی بانک بر جای می گذارد ($\beta = +0.688, t = 19.657, p < 0.001$). این یافته موید آن است که سرمایه گذاری بر استقرار چارچوب های واکنش به بحران، هزینه ای تحمیلی نبوده بلکه ستون فقرات حفظ زنجیره ارزش، بقای اعتماد سپرده گذاران و صیانت از صحت صورت های مالی محسوب می شود و نقشی ضربه گیر در برابر تلاطم های دیجیتال ایفا می کند.

پرسش بنیادین این پژوهش این بود که نهادهای مالی در عصر مخاطرات نوظهور سایبری چگونه می توانند از انحراف و شکست کنترل های داخلی و گسست در تداوم فعالیت حسابداری خود پیشگیری نمایند. اهمیت مطالعه حاضر در پیوند دادن حوزه مهندسی امنیت و مدیریت بحران با ارکان حسابداری مالی و حاکمیت شرکتی نهفته است؛ زیرا برای نخستین بار نشان داد که سلامت گزارشگری مالی در بانکداری نوین مستقیماً وابسته به استحکام معماری پاسخ به بحران های سایبری است. دستاورد برجسته این پژوهش اثبات این اصل بود که سامانه های پدافندی اثر تعدیل کننده مستقیمی بر حفظ شواهد حسابرسی و اعتبار صورت های مالی دارند و کاربست اجرایی آن ایجاب می کند که کمیته های حسابرسی و ریسک از حالت منفعل خارج شده و به ناظران فعال بر فرآیندهای تاب آوری سایبری تبدیل شوند تا از جرایم انضباطی ناظران پولی و هجوم های ناگهانی بانکی ممانعت به عمل آید.

هر پژوهش تجربی در مسیر اجرا با محدودیت هایی مواجه است؛ در این پژوهش، محرمانه بودن اطلاعات امنیتی و سیاست های سخت گیرانه افشای حوادث سایبری در برخی بانک ها موجب شد که دسترسی به داده های واقعی وقایع با دشواری همراه شود و

اتکای اصلی بر ادراکات تخصصی نمونه آماری قرار گیرد. علاوه بر این، سرعت فزاینده تحولات در الگوهای نفوذ بدافزاری و فناوری های ابری ممکن است کارآمدی برخی از سازوکارهای موجود را در طول زمان دستخوش تغییر نماید که این امر نیاز به بازآزمایی های مقطعی را گوشزد می کند.

بر اساس نتایج تجربی، توصیه می شود هیئت مدیره بانک ها با ادغام کمیته های حسابرسی داخلی و راهبری امنیت اطلاعات، ساختار «مرکز عملیات پایش تداوم مالی» را به صورت شبانه روزی مستقر سازند تا ردپای حسابرسی و تغییرات جداول پایگاه های داده بلادرنگ بررسی شود. همچنین اجرای دوره های سناریوهای شبیه سازی باج افزاری و قطعی ناگهانی شبکه های تسویه به همراه پشتیبان گیری سرد و گرم ناهم زمان در مراکز داده مجزا به عنوان یک الزام راهبردی تعیین گردد. آموزش مستمر کارکنان لایه های مالی پیرامون مهندسی اجتماعی و بازنگری در ساختار تفکیک وظایف دیجیتال بر مبنای اصل حداقل دسترسی نیز از الزامات فوری برای صیانت از سلامت کنترل های داخلی است.

به پژوهشگران آینده پیشنهاد می شود در مطالعات آتی به بررسی نقش فناوری های دفتر کل توزیع شده و قراردادهای هوشمند در بازسازی خودکار اسناد مالی پس از بحران های سایبری بپردازند. همچنین ارزیابی اثرات تعدیل گر فرهنگ سازمانی و سرمایه روان شناختی کارکنان بر کارایی تیم های واکنش سریع و مقایسه تطبیقی الگوی مدیریت بحران در بانک های دولتی و خصوصی با استفاده از مدل های داده های تابلویی و شاخص های مالی عینی از دیگر زمینه های مستعد برای توسعه مرزهای دانش در این حوزه به شمار می آید.

منابع

احمدی، س. (۱۴۰۲). نقش حاکمیت فناوری اطلاعات و کمیته های ریسک در کاهش آسیب پذیری های سایبری بانک ها. فصلنامه مهندسی مالی و مدیریت اوراق بهادار، ۱۴ (۵۵)، ۱۱۲-۱۳۵.

تقوی، م.، و حسینی، ع. (۱۴۰۱). بررسی اثر نشت اطلاعات مالی بر ارزش برند و ریسک ورشکستگی بانک های پذیرفته شده در بورس اوراق بهادار تهران. پژوهش های تجربی حسابداری، ۱۲ (۴۶)، ۱۸۵-۲۰۸.

رحیمی، ف. (۱۴۰۱). بررسی تاب آوری کنترل های داخلی در بانکداری الکترونیک در مواجهه با وقفه های شبکه تسویه. مجله دانش حسابداری و حسابرسی مدیریت، ۱۱ (۴۳)، ۸۹-۱۰۴.

رضایی، ک. (۱۴۰۰). مدیریت بحران های عملیاتی در زیرساخت های حیاتی نظام پرداخت و تسویه الکترونیکی. مدیریت ریسک و بحران، ۳ (۱)، ۴۵-۶۲.

صادقی، ح. (۱۴۰۲). مدیریت تداوم کسب و کار و کاهش زمان بازیابی پس از خرابی در سامانه های بانکداری متمرکز. فصلنامه مدیریت فناوری اطلاعات، ۱۵ (۳)، ۱۲۵-۱۴۶.

طاهری، ن. و کریمی، ب. (۱۴۰۳). ارزیابی چارچوب کوسو در عصر دیجیتال: آزمون کنترل های عمومی فناوری اطلاعات در شبکه بانکی. *مطالعات حسابداری و حسابرسی*، ۱۳ (۵۰)، ۶۷-۸۸.

کاظمی، م. (۱۴۰۳). ارزیابی نقش مدیریت بحران سایبری در کاهش تهدیدات امنیتی و صیانت از پایگاه های داده بانکی. *پژوهش های پولی و بانکی*، ۱۷ (۵۹)، ۴۵-۶۸.

میرزایی، ر. (۱۴۰۲). اثر مخاطرات امنیت اطلاعات و نشت داده ها بر کیفیت گزارشگری مالی و حق الزحمه حسابرسی مستقل. *بررسی های حسابداری و حسابرسی*، ۳۰ (۲)، ۲۱۵-۲۳۸.

نجفی، ع. (۱۴۰۰). پیامدهای اختلال سامانه ای تسویه ناخالص آنی بر ریسک نقدینگی و انضباط دفاتر کل در بانک ها. *مطالعات تجربی حسابداری مالی*، ۱۸ (۷۱)، ۷۷-۱۰۲.

Al-Shayeb, A. (2023). Cyberattacks, internal control effectiveness, and audit delay: Empirical evidence from commercial banks. *Accounting and Business Research*, 53(4), 412-439.

Biswas, B. (2023). Systemic operational disruptions and financial reporting continuity in digital banking ecosystems. *International Journal of Accounting Information Systems*, 48, 100602.

Bojanc, R., & Jerman-Blažič, B. (2022). Quantitative model for information security risk management in financial transaction systems. *Information Sciences*, 584, 521-538.

Chen, Y. (2024). Cyber risk management and information security resilience in modern financial institutions. *Journal of Banking & Finance*, 158, 107034.

Coutinho, M. (2024). Operational continuity and real-time gross settlement resilience in banking infrastructure crises. *Journal of Financial Stability*, 71, 101230.

Hasan, M. M., & Rahman, M. A. (2023). Information technology governance, cyber risk disclosures, and financial reporting quality in the banking sector. *Journal of International Accounting, Auditing and Taxation*, 51, 100548.

Kopp, E., Kaffenberger, L., & Wilson, C. (2022). Cyber risk, market failures, and financial stability. *Journal of Financial Regulation and Compliance*, 30(2), 174-196.

Moreira, L. (2024). Proactive incident response and cybersecurity governance: Mitigation mechanisms for banking vulnerabilities. *Computers & Security*, 137, 103612.

Rosati, P., & Lynn, T. (2023). The financial impact of cyber attacks: Evidence from listed financial institutions. *European Journal of Finance*, 29(12), 1365-1392.