نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

مقالهٔ پژوهشی

بررسی تأثیر حملات سایبری بر حسابرسی دیجیتال بر اساس نظریه مجرمانه بِکِر[۱،۲]

آوان جمشیدی*[۳] و جواد جمشیدی[۴]

نشریه علمی حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال اول، پیاپی ۱، بهار و تابستان ۱۴۰۴
صص ۱۰۰ - ۱۱۶

تاریخ دریافت: ۱۴۰۳/۱۱/۲۱
تاریخ بازنگری: ۱۴۰۴/۰۴/۱۱
تاریخ پذیرش: ۱۴۰۴/۰۶/۱۱

چکیده

هدف این پژوهش بررسی تأثیر حملات سایبری بر فرآیندهای حسابرسی دیجیتال با بهره‌گیری از نظریه مجرمانه بکر است. داده‌ها از طریق مطالعه اسناد و گزارش‌های مرتبط با حملات سایبری و مصاحبه با کارشناسان حوزه حسابرسی و امنیت سایبری در سال ۱۴۰۳ جمع آوری و با ۱۵ نفر اشباع نظری حاصل شد. روش تحلیل تم با کمک نرم افزار مکس کیودا انجام شد. یافته‌ها نشان داد که حملات سایبری، تأثیرات متعددی بر حسابرسی دیجیتال دارند که در پنج محوری اصلی قابل طبقه‌بندی هستند: تاثیرات مستقیم حملات؛ حملات سایبری به‌طور مستقیم بر دقت، صحت و کارایی سیستم‌های حسابرسی دیجیتال تأثیر می‌گذارند. ریسک ها و هزینه ها؛ افزایش هزینه‌های امنیتی و ریسک‌های قانونی می‌تواند این رفتارها را محدود کند. تدابیر پیشگیرانه؛ این تدابیر می‌تواند آسیب‌پذیری سازمان‌ها را به‌طور چشمگیری کاهش دهد. افزایش هزینه‌ها و کاهش بهره‌وری؛ حملات باعث افزایش هزینه‌های امنیتی و کاهش کارایی تیم‌های حسابرسی شده است. منافع مهاجمان سایبری؛ مهاجمان با هدف دستیابی به اطلاعات حساس و منافع مالی، از ضعف‌های امنیتی سوءاستفاده می‌کنند. پیامدهای اجتماعی و اخلاقی: کاهش اعتماد به سیستم‌های حسابرسی دیجیتال و نگرانی‌های مرتبط با حفظ محرمانگی اطلاعات از پیامدهای کلیدی هستند . حملات سایبری تأثیر منفی قابل توجهی بر کارایی و امنیت حسابرسی دیجیتال دارند. نظریه بکر نشان می‌دهد که ایجاد بازدارندگی از طریق افزایش هزینه‌های ارتکاب جرم (مانند مجازات‌های شدیدتر و تقویت سیستم‌های امنیتی) می‌تواند تأثیر مثبتی در کاهش این تهدیدات داشته باشد . همچنین با توجه به اهمیت روزافزون حسابرسی دیجیتال در دنیای مدرن، مقابله با حملات سایبری نه تنها یک نیاز فنّی، بلکه یک ضرورت استراتژیک است.

واژه‌های کلیدی: *امنیت اطلاعات، حملات سایبری، حسابرسی دیجیتال، نظریه مجرمانه بکر.*
طبقه‌بندی موضوعی: *M4* .

---

[1] https://doi.org/10.22034/JISTA.2025.540907.1058

[۲]. مقاله منتخب بیست و دومین همایش ملی حسابداری ایران

[۳]. دکترا حسابداری، دانشکده علوم اجتماعی و اقتصادی دانشگاه الزهراء، تهران، ایران./ مدرس مدعو دانشگاه ملی مهارت، تهران، ایران. (نویسنده مسئول). Email: t.jamshidi@alzahra.ac.ir

[۴]. کارشناسی ارشد، گروه حقوق، جزا و جرم شناسی، دانشگاه پیام نور، تهران، ایران. Email: javad jamshidi@yahoo.com

مقدمه

در دنیای امروز، پیشرفت فناوری‌های اطلاعاتی و ارتباطی، به یکی از مؤلفه‌های اصلی تحولات در حوزه‌های مالی و حسابرسی تبدیل شده است. حسابرسی دیجیتال با بهره‌گیری از ابزارهایی همچون هوش مصنوعی، داده‌کاوی و سیستم‌های پیشرفته تحلیل اطلاعات، فرآیندهای حسابرسی را بهبود بخشیده و دقت و کارایی آن‌ها را افزایش داده است. با این حال، این تحول فناورانه، سازمان‌ها و فرآیندهای حسابرسی را در برابر تهدیدات جدیدی همچون حملات سایبری آسیب‌پذیر کرده است. حملات سایبری نظیر هک، سرقت داده‌ها، باج‌افزارها و دستکاری اطلاعات، نه‌تنها می‌توانند اعتبار و امنیت اطلاعات حسابرسی‌شده را به خطر بیندازند، بلکه موجب کاهش اعتماد عمومی به سیستم‌های دیجیتال نیز می‌شوند(اسدی و همکاران، ۱۴۰۱: ۴۵).

تحول دیجیتال و استفاده از فناوری‌های نوین مانند هوش مصنوعی، بلاکچین و تحلیل داده‌های کلان، انقلابی در فرآیندهای حسابرسی ایجاد کرده است. این فناوری‌ها با افزایش دقت، شفافیت و سرعت، توانسته‌اند به‌طور چشمگیری کارایی حسابرسی را بهبود بخشند(سیریوز و همکاران[1]، ۲۰۲۰: ۳۴). با این حال، وابستگی روزافزون به زیرساخت‌های دیجیتال، محیط حسابرسی را به هدفی جذاب برای حملات سایبری تبدیل کرده است. این حملات، شامل سرقت اطلاعات مالی، دستکاری داده‌ها، باج‌افزارها و ایجاد اختلال در زیرساخت‌های فناوری، می‌توانند امنیت و اعتبار حسابرسی دیجیتال را به‌شدت تهدید کنند. در این میان، نظریه جرم بکر[2] که رفتارهای مجرمانه را از منظر اقتصادی و تحلیل هزینه–فایده بررسی می‌کند، چارچوبی مناسب برای تحلیل انگیزه‌ها و رفتارهای مجرمان سایبری ارائه می‌دهد. بر اساس این نظریه، افراد زمانی به فعالیت‌های مجرمانه روی می‌آورند که مزایای بالقوه این اقدامات از هزینه‌های احتمالی آن (مانند خطر شناسایی و مجازات) بیشتر باشد(بکر، ۱۹۶۸: ۱۷۷). از دیدگاه نظریه مجرمانه بِکِر، مجرمان از جمله هکرها، تصمیمات خود را بر اساس یک تحلیل منطقی از هزینه‌ها و منافع اتخاذ می‌کنند. اگر هزینه‌های ارتکاب جرم (مانند احتمال کشف و مجازات) پایین باشد و منافع آن (مانند دسترسی به داده‌های ارزشمند) بالا، احتمال وقوع جرم افزایش می‌یابد. در این

[1] Sirois et al
[2] Becker

چارچوب، ضعف در امنیت سایبری سازمان‌ها و جذابیت داده‌های حسابرسی دیجیتال، حملات سایبری را به یکی از بزرگ‌ترین چالش‌های پیش روی حسابرسی دیجیتال تبدیل کرده است. حملات سایبری علاوه بر تهدید امنیت داده‌ها، پیامدهای اقتصادی و سازمانی گسترده‌ای دارند. این حملات هزینه‌های مستقیم و غیرمستقیمی از جمله هزینه‌های بازیابی اطلاعات، تقویت زیرساخت‌های امنیتی و جبران خسارت‌های وارده به ذینفعان، به سازمان‌ها تحمیل می‌کنند. طبق گزارش موسسه پی دبلیو سی[1] (۲۰۲۲)، این هزینه‌ها در سال‌های اخیر، به‌طور قابل‌توجهی افزایش یافته است. علاوه بر این، اختلال در فرآیندهای حسابرسی دیجیتال می‌تواند اعتماد ذینفعان به گزارش‌های مالی را کاهش داده و به اعتبار سازمان لطمه بزند(گوش و شرمن[2]،۲۰۲۱: ۴۵)

از سوی دیگر، تحلیل حملات سایبری در چارچوب نظریه بکر نشان می‌دهد که افزایش امنیت سایبری و کاهش آسیب‌پذیری‌ها می‌تواند انگیزه مجرمان را کاهش دهد. این موضوع، نیازمند شناسایی دقیق الگوهای رفتاری مجرمان سایبری و طراحی راهکارهایی برای کاهش جذابیت اهداف دیجیتال است(اندرسون و موور[3]،۲۰۲۰: ۳۷). همچنین، تغییرات قانونی و مقررات سخت‌گیرانه‌تر در مقابله با جرایم سایبری، نقشی کلیدی در بهبود امنیت حسابرسی دیجیتال ایفا می‌کنند(بوهم و اسشورتز[4]،۲۰۲۱:۳۵). این پژوهش با استفاده از نظریه مجرمانه بکر، به بررسی تأثیر حملات سایبری بر حسابرسی دیجیتال می‌پردازد. هدف اصلی این مطالعه، شناسایی الگوهای حملات سایبری، ارزیابی پیامدهای آن‌ها بر فرآیندهای حسابرسی و ارائه راهکارهایی برای کاهش ریسک‌های مرتبط است. حملات سایبری در حوزه حسابرسی دیجیتال نیز اغلب با هدف دستیابی به منافع مالی یا اطلاعات حساس انجام می‌شود که این موضوع نیاز به تحلیل دقیق‌تری از ابعاد این تهدیدات را نشان می‌دهد(زارع و همکاران،۱۴۰۲: ۳۰).

حملات سایبری، یکی از حوزه‌هایی است که در سال های اخیر افزایش زیادی داشته است. بعضی از دلایل رشد این حملات، این است که ابزارهای مورد استفاده نیاز به مهارت‌های بالایی ندارد و گاهی هکرهای تازه کار، جرم‌هایی را مرتکب شده‌اند که اثرات بااهمیتی بر شرکت

[1] PwC
[2] Ghosh & Sharman
[3] Anderson & Moore
[4] Böhme & Schwartz

گذاشته و هیچ برنامه‌ای برای اختلاس خود نداشته‌اند، از سوی دیگر، بعضی هکرهای حرفه‌ای، به عنوان مشاورانی عمل می‌کردند که مجرمان می‌توانستند با تخصص آنها به اسرار شرکت دست پیدا کرده و باعث وقوع تقلب شوند(رویایی، ۱۳۸۸). به همین دلیل، حملات سایبری به یکی از تهدیدات بزرگ عصر دیجیتال تبدیل شده‌اند و تاثیرات زیادی بر جنبه‌های مختلف فناوری اطلاعات، به ویژه حسابرسی دیجیتال، گذاشته‌اند(گوهانگ و همکاران[1]،۲۰۲۵).

حسابرسی دیجیتال که شامل ارزیابی و بررسی سیستم‌های مالی و اطلاعاتی، از طریق ابزارهای دیجیتال است، زمانی که با حملات سایبری مواجه می‌شود، ممکن است با مشکلاتی مانند دستکاری داده‌ها، از دست رفتن اطلاعات و اختلال در فرآیندهای حسابرسی مواجه شود. این مسئله بر کیفیت حسابرسی و دقت نتایج آن تأثیر منفی می‌گذارد(نخعی و برزگراول،۱۴۰۲: ۱۲). مسئله اصلی این است که چگونه حملات سایبری بر فرآیندهای حسابرسی دیجیتال تأثیر می‌گذارند و پیامدهای این تأثیرات برای سازمان‌ها و جامعه چیست؟ همچنین، چگونه می‌توان با استفاده از نظریه جرم بکر، رفتار و انگیزه‌های مجرمان سایبری را تحلیل و راهکارهای پیشگیرانه‌ای برای کاهش این تهدیدات طراحی کرد؟ براساس این نظریه، برای کاهش حملات سایبری در حوزه حسابرسی دیجیتال، لازم است هزینه‌های ارتکاب جرم افزایش یابد (مانند تقویت سیستم‌های نظارتی و افزایش مجازات‌ها) و در عین حال، مزایای احتمالی آن (مانند رمزنگاری داده‌ها و کاهش ارزش اطلاعات برای مجرمان)، کاهش پیدا کند. این راهکارها می‌توانند به‌طور مستقیم به کاهش آسیب‌پذیری حسابرسی دیجیتال و افزایش امنیت آن کمک کنند. این تحقیق، با تحلیل تعامل میان حملات سایبری و حسابرسی دیجیتال از منظر نظریه جرم بکر، تلاش می‌کند راهکارهایی کاربردی برای کاهش آسیب‌ها و افزایش اعتماد عمومی به سیستم‌های دیجیتال ارائه دهد.

مبانی نظری

حملات سایبری، به اقداماتی اطلاق می‌شود که با هدف نفوذ به سیستم‌ها، شبکه‌ها یا اطلاعات حساس سازمان‌ها انجام می‌شود. این حملات می‌توانند در قالب‌های مختلفی از جمله

[1] Guohong

ویروس‌ها، بدافزارها، فیشینگ[1]، حملات انکار سرویس[2] و حملات نفوذی به شبکه بروز کنند. این حملات می‌توانند موجب از دست رفتن داده‌ها، دستکاری اطلاعات و یا حتی تخریب سیستم‌ها شوند.

حسابرسی دیجیتال، به فرآیند بررسی و ارزیابی سیستم‌های فناوری اطلاعات، داده‌ها و مستندات مالی با استفاده از ابزارهای دیجیتال و نرم‌افزارهای خاص اطلاق می‌شود. این نوع حسابرسی قادر به شناسایی مشکلات و خطاهای مالی و امنیتی در سازمان‌ها است. هدف اصلی حسابرسی دیجیتال تضمین صحت داده‌ها و جلوگیری از هرگونه تقلب یا دستکاری در اطلاعات است(گوانگ[3]،۲۰۲۵: ۴۰).

نظریه مجرمانه بکر

بر اساس نظریه مجرمانه بکر، جرم نتیجه ارزیابی هزینه و فایده توسط فرد مجرم است. افراد ممکن است زمانی به ارتکاب جرم بپردازند که مزایای آن بیشتر از هزینه‌های آن باشد. در زمینه حملات سایبری، مجرمان ممکن است حملات خود را با هدف دستیابی به منافع مالی یا اطلاعات حساس انجام دهند، با ارزیابی این که خطر کشف و مجازات نسبت به منافع به دست آمده کم است(بکر،۱۹۶۸: ۱۷۶).

تاثیر حملات سایبری بر حسابرسی دیجیتال

حملات سایبری می‌توانند بر فرایند حسابرسی دیجیتال اثرات منفی زیادی بگذارند:

۱) از دست رفتن داده‌ها: حملات سایبری می‌توانند منجر به از دست رفتن داده‌های مهم حسابرسی شوند که موجب به چالش کشیده شدن صحت گزارش‌ها و تحلیل‌ها می‌شود.

۲) اختلال در فرآیندهای حسابرسی: با ورود بدافزار یا حملات DDOS، سیستم‌های حسابرسی دیجیتال ممکن است برای مدت زمان قابل توجهی از دسترس خارج شوند، که باعث اختلال در روند حسابرسی و گزارش‌دهی می‌شود.

---

[1] Phishing
[2] Denial of Service (DoS)
[33] Guohong

۳) افزایش خطر تقلب و تخلفات مالی: مجرمان سایبری می‌توانند از حملات خود برای دستکاری داده‌ها و ایجاد گزارش‌های غلط استفاده کنند که موجب آسیب به اعتبار و صحت نتایج حسابرسی می‌شود.

۴) کاهش اعتماد به سیستم‌ها: حملات سایبری می‌توانند باعث کاهش اعتماد سازمان‌ها و مشتریان به سیستم‌های حسابرسی دیجیتال شوند که در نهایت، باعث کاهش اثربخشی این سیستم‌ها می‌شود.

مطالعات زیادی در این زمینه انجام گرفت. وانگ[1](۲۰۲۵) در پژوهشی به بررسی تحول دیجیتال، ریسک حسابرسی، و انتقال کم کربن شرکت‌های انرژی چین پرداخت. یافته‌های پژوهش او، ناهمگونی‌های کلیدی در این رابطه را برجسته می‌کند. تأثیر تحول دیجیتال در مناطق مختلف چین متفاوت و تحت تأثیر نوع مؤسسه حسابرسی است. این موضوع، نشان می‌دهد که منطقه شرقی و شرکت‌هایی که توسط موسسات حسابرسی غیراز موسسات بزرگ حسابرسی، حسابرسی می‌شوند، مهم‌ترین مزایای دیجیتالی‌سازی را در زمینه انتقال‌های کم کربن، تجربه می‌کنند. این بینش‌ها، راهنمایی‌های ارزشمندی را برای شرکت‌های انرژی و سیاست گذارانی ارائه می‌دهد که پیچیدگی‌های نوآوری دیجیتال و توسعه پایدار در بخش انرژی چین را بررسی می‌کنند.

گوهانگ و همکاران(۲۰۲۵) در پژوهشی به بررسی تخصص فناوری اطلاعات کمیته حسابرسی و تأثیر آن بر افشای اطلاعات ریسک امنیت سایبری پرداختند. نتایج نشان داد که تخصص فناوری اطلاعات کمیته‌های حسابرسی، به طور معناداری افشای اطلاعات ریسک‌های امنیت سایبری را بهبود می‌بخشد. این اثر در شرکت‌هایی که شفافیت گزارش‌گری مالی کمتری دارند، شرکت‌هایی با حاکمیت ضعیف‌تر و شرکت‌هایی با عدم تقارن اطلاعاتی پایین‌تر، مشهودتر است. علاوه بر این، سطح پذیرش هوش مصنوعی، کیفیت کنترل‌های داخلی و کیفیت افشای اطلاعات کانال‌های بالقوه در این رابطه تأثیرگذار هستند.

آگیوا و همکاران[2](۲۰۲۱) در پژوهشی به کاربرد فناوری های دیجیتال در گزارشگری مالی و حسابرسی پرداختند. یافته های پژوهش آنان، روندهای اصلی در توسعه گزارشگری مالی و

[1] Wang
[2] Ageeva et al.

حسابرسی یعنی یکپارچه شدن با محیط دیجیتال، شرح روش های بکارگیری کلان داده ها، انتقال به گزارشگری آنلاین و حسابرسی مستمر آن را مشخص می‌کند. همچنین، آنان، الگوریتمی برای کاربرد فناوری بلاکچین در حسابداری، گزارشگری و حسابرسی پیشنهاد و یک دسته‌بندی برای موارد تقلب در گزارشگری مالی در روسیه، ارائه و اقدامات پیشگیرانه مبتنی بر بلاکچین را بیان می‌کنند.

بنابی قدیم(۱۴۰۲)، در پژوهشی بررسی امنیت سایبری مبتنی بر شواهد حسابرسی پرداخت. نتایج نشان داد که کسب اطمینان در این زمینه و ارائه رهنمودهای سازنده(پیشگیرانه، یابند و اصلاحی) در خصوص افزایش امنیت سایبری توسط حسابرسان، یک رویکرد مبتنی بر شواهد برای مدیریت ریسک در عصر دیجیتالی شدن تجارت است. بطوری که در نتیجه مشارکت حسابرسان در کمک به مدیریت ریسک‌ها، شاخص‌های فزاینده امنیت باید در نرم افزار و همچنین، سیستم عامل کسب و کار ادغام شود، زیرا برای دستیابی به یک سپر دفاعی منسجم در مقابل خطرات سایبری، خود سیستم‌های اطلاعاتی باید به سطح مطلوبی از امنیت برسند.

روش‌شناسی پژوهش

این پژوهش از روش کیفی با رویکرد تحلیل تم است. داده‌ها از دو منبع اصلی مطالعه اسناد و گزارش‌های مرتبط با حملات سایبری و مصاحبه‌های نیمه‌ساختاریافته با کارشناسان حوزه حسابرسی و امنیت سایبری، جمع‌آوری شدند. مصاحبه‌ها بر اساس چارچوب از پیش تعیین‌شده انجام شد، اما به شرکت‌کنندگان اجازه داده شد نظرات و تجربیات خود را آزادانه بیان کنند. برای تحلیل داده‌ها، از نرم‌افزار مکس کیودا استفاده شد که امکان کدگذاری اولیه، گروه‌بندی کدها در مضامین اصلی و استخراج روابط میان آنها را فراهم کرد. در این پژوهش، روش نمونه‌گیری هدفمند و از متخصصان امنیت سایبری، حسابرسان و مدیران سازمان‌ها استفاده شده است. این افراد دارای تجربه کافی در حوزه حسابرسی دیجیتال و امنیت سایبری بودند. برای انتخاب آنها، معیارهایی مانند حداقل ۵ سال سابقه کار مرتبط، دانش در زمینه تهدیدات سایبری و حسابرسی دیجیتال و تجربه مدیریت ریسک سایبری در نظر گرفته شد. نمونه‌گیری از طریق شناسایی افراد واجد شرایط در شبکه‌های حرفه‌ای و همچنین استفاده از روش گلوله برفی در سال ۱۴۰۳ انجام شد، به این صورت که برخی از مصاحبه‌شوندگان اولیه، متخصصان دیگری را

معرفی کردند. مصاحبه‌ها تا رسیدن به اشباع نظری ادامه یافت و پس از مصاحبه با ۱۵ نفر، داده‌ها به اندازه‌ای تکراری شدند که اطلاعات جدیدی حاصل نشد.

یافته‌های پژوهش

با توجه به مراحل تحلیل تم، تحلیل اطلاعات پژوهش به صورت زیر انجام گرفت:

۱. آماده سازی داده‌ها: برای آماده سازی داده از سه روش؛ الف) مصاحبه کارشناسان امنیت سایبری، حسابرسان و مدیران سازمان‌ها و امنیت سایبری، ب) گزارش‌های حملات سایبری در حوزه حسابرسی. ج) مستندات مرتبط با جرایم سایبری و سیاست-های امنیتی

۲. کدگذاری اولیه: برای این کار ابتدا داده‌ها خط به خط خوانده شد و کدهای اولیه استخراج شد.

۳. سازمان‌دهی کدها به مضامین: کدهای مشابه به مضامین اصلی و فرعی گروه‌بندی شدند.

٤. نشان دادن روابط بین کدها

اطلاعات استخراج شده، در جداول ۱ الی ۳ نشان داده شده است.

جدول ۱. کدهای اولیه

مرحله	کدهای اولیه	تم ها	تعریف
تاثیرات مستقیم	کاهش دقت حسابرسی	تاثیرات مستقیم حملات سایبری	نحوه تاثیرات حملات سایبری بر فرایند حسابرسی از جمله کاهش دقت و اختلال در فرایندها است
	اختلال در سیستم های دیجیتال		
	کاهش اعتماد مشتریان		
ریسک ها و هزینه ها	افزایش هزینه های امنیتی	ریسک ها و هزینه ها(براساس نظریه بکر)	ارزیابی هزینه های مالی، زمانی و انسانی مرتبط با مدیریت حملات سایبری و ریسک های تصمیم گیری مهاجمان
	افزایش ریسک حسابرسان		
	کاهش بازدهی مالی		
	سرقت اطلاعات		

مرحله	کدهای اولیه	تم ها	تعریف
منافع مهاجمان سایبری	اهداف مالی	منافع مهاجمان سایبری	اهداف و انگیزه های مهاجمان برای انجام حملات از جمله کسب اطلاعات و منافع مالی
	دسترسی غیرمجاز به سیستم های حسابرسی		
تدابیر پیشگیرانه	آموزش و آگاهی حسابرسان	تدابیر پیشگیرانه	استراتژی ها و اقداماتی که برای کاهش آسیب پذیری حسابرسی دیجیتال و جلوگیری از حملات انجام می شود
	استفاده از فناوری های پیشرفته امنیتی		
	تدوین سیاست های امنیت سایبری		
پیامدهای اجتماعی و اخلاقی	کاهش اعتماد به حسابرسی دیجیتال	پیامدهای اجتماعی و اخلاقی	برای نشان دادن تاثیر حملات سایبری نسبت به دقت و محرمانگی گزارش های حسابرسی
	نگرانی های اخلاقی در حفظ محرمانگی		
	محرمانگی چالش‌های قانونی و حقوقی		

منبع: یافته پژوهشگران

جدول ۲. جدول روابط بین تم ها

تم اصلی	تعریف تم	کدهای مرتبط	نمونه شواهد
تاثیرات مستقیم حملات	- تاثیرات فوری و مستقیم حملات سایبری بر فرایندها و نتایج حسابرسی دیجیتال، شامل اختلالات عملیاتی و کاهش اعتماد	- کاهش دقت و صحت داده های حسابرسی - اختلال در سیستم های حسابرسی کاهش اعتماد مشتریان و ذینفعان	پس از حمله سایبری داده های حسابرسی ما دچار تغییرات ناخواسته ای شد که باعث بی اعتمادی مشتریان شد
ریسک ها و هزینه ها	- ارزیابی هزینه های مرتبط با حملات سایبری(مالی، زمانی و امنیتی) و ریسک های ناشی از تصمیم گیری مهاجمان براساس نظریه بکر	- افزایش هزینه های امنیتی - افزایش ریسک برای حسابرسان و سازمان ها کاهش بازدهی مالی	برای مقابله با این حملات مجبور شدیم بودجه امنیتی خود را دو برابر کنیم
منافع مهاجمان سایبری	- انگیزه ها و منافع مهاجمان سایبری، از جمله کسب	- سرقت اطلاعات حساس	مهاجمان با هدف سرقت اطلاعات مالی و فروش

تم اصلی	تعریف تم	کدهای مرتبط	نمونه شواهد
	اطلاعات ارزشمند، منافع مالی و تخریب سیستم های حسابرسی	- اهداف مالی و سودجویی دسترسی غیرمجاز به سیستم های و داده های حسابرسی	آنها به رقبا، به سیستم ما حمله کردند
تدابیر پیشگیرانه	- اقدامات و راهکارهایی برای کاهش آسیب پذیری سیستم های حسابرسی دیجیتال و جلوگیری از حملات سایبری	- استفاده از فناوری های پیشرفته امنیتی - آموزش کارکنان و حسابرسان تدوین سیاست های و قوانین امنیتی	آموزش کارکنان در مورد امنیت سایبری و به کارگیری سیستم های رمزگذاری پیشرفته توانست آسیبپذیری ما را کاهش دهد
پیامدهای اجتماعی و اخلاقی	- پیامدهای اجتماعی و اخلاقی حملات سایبری، شامل کاهش اعتماد به حسابرسی، نگرانی درباره محرمانگی اطلاعات های قانونی برای حسابرسان و سازمان ها	- کاهش اعتماد به حسابرسی دیجیتال - نگرانی های اخلاقی در حفظ محرمانگی چالش های قانونی و حقوقی	حملات سایبری باعث شده مشتریان نسبت به دقت و محرمانگی گزارش های حسابرسی دیجیتال بدبین شوند

منبع: یافته پژوهشگران

جدول ۳. جدول فراوانی در کدها در اسناد

کد	فراوانی در سند ۱	فراوانی سند ۲	فراوانی سند۳	کل فراوانی
ضعف امنیتی	۵	۳	۲	۱۰
خطای انسانی	۴	۲	۳	۹
سرقت اطلاعات	۳	۵	۴	۱۲
زیان مالی	۶	۴	۵	۱۵

منبع: یافته پژوهشگران

نتایج نشان داد که ضعف امنیتی و خطای انسانی، از عوامل مهم تسهیل کننده حملات هستند. زیان مالی و کاهش اعتماد عمومی به سیستم‌های حسابرسی دیجیتال، از مهمترین پیامدها هستند. همچنین، دسترسی به داده‌های حسابرس و هزینه پایین ابزارهای حمله ، انگیزه مهاجمان برای حملات سایبری را افزایش می‌دهد.

یافته‌های آماری

در جدول ۴، نتایج آمار توصیفی ارائه گردیده است.

جدول ۴. آمار توصیفی داده ها

متغیر	میانگین	انحراف	حداقل	حداکثر
شدت حملات سایبری	۴.۲۳	۰.۷۸	۲	۵
تاثیر بر حسابرسی	۳.۸۵	۱.۱۲	۱	۵
اعتماد عمومی	۴.۱۰	۰.۹۴	۲	۵

در جدول ۵، نتایج تحلیل همبستگی بین حملات سایبری و کیفیت حسابرسی دیجیتال، ارائه گردیده است.

جدول ۵. تحلیل همبستگی بین حملات سایبری و کیفیت حسابرسی دیجیتال

متغیرها	همبستگی	سطح معنی داری
حملات سایبری و دقت حسابرسی	۰.۶۵	۰.۰۰۱
حملات سایبری و اعتبار گزارش‌ها	۰.۵۸	۰.۰۰۳
حملات سایبری و تاثیر بر فرایندها	۰.۷۰	۰.۰۰۰

منبع: یافته پژوهشگران

بین حملات سایبری و دقت حسابرسی، ضریب همبستگی ۰.۶۵ با سطح معناداری ۰.۰۰۱ وجود دارد. این مقدار نشان‌دهنده همبستگی مثبت و نسبتاً قوی بین این دو متغیر است، به این معنا که افزایش حملات سایبری منجر به کاهش دقت حسابرسی می‌شود. بین حملات سایبری و اعتبار گزارش‌های حسابرسی، ضریب همبستگی ۰.۵۸ با سطح معناداری ۰.۰۰۳ به دست آمده است. این نتیجه نشان می‌دهد که حملات سایبری می‌توانند اعتبار گزارش‌های حسابرسی را کاهش دهند. بین حملات سایبری و تأثیر بر فرآیندهای حسابرسی همبستگی ۰.۷۰ با سطح

معناداری ۰.۰۰۰ گزارش شده است. این مقدار، بیانگر رابطه بسیار قوی بین این متغیرهاست، یعنی حملات سایبری تأثیر منفی قابل توجهی بر فرآیندهای حسابرسی دارند.

مرور یافته‌ها

تحلیل تماتیک نشان داد که حملات سایبری تأثیرات عمیقی بر حسابرسی دیجیتال دارند. این تأثیرات شامل افزایش آسیب‌پذیری‌ها، پیامدهای مالی و اعتباری، و انگیزه‌های مهاجمان است.

تحلیل و تفسیر تم‌ها

تم ۱: تأثیرات مستقیم حملات سایبری

توضیح: حملات سایبری به‌طور مستقیم بر دقت، صحت و کارایی سیستم‌های حسابرسی دیجیتال تأثیر می‌گذارند. این حملات منجر به اختلال در عملیات حسابرسی و کاهش اعتماد مشتریان می‌شوند.

اهمیت: کاهش دقت و اختلالات ناشی از حملات می‌تواند به از دست دادن اعتبار سازمان‌ها و حسابرسان منجر شود.

تم ۲: ریسک‌ها و هزینه‌ها (براساس نظریه بکر)

توضیح: نظریه مجرمانه بکر تأکید می‌کند که مهاجمان سایبری منافع و هزینه‌های احتمالی حملات خود را می‌سنجند. افزایش هزینه‌های امنیتی و ریسک‌های قانونی می‌تواند این رفتارها را محدود کند.

اهمیت: درک این جنبه به سازمان‌ها کمک می‌کند تا استراتژی‌های مؤثری برای کاهش ریسک‌ها تدوین کنند.

تم ۳: منافع مهاجمان سایبری

توضیح: مهاجمان اغلب به‌دنبال سرقت اطلاعات حساس یا دستیابی به منافع مالی هستند. این انگیزه‌ها با هزینه‌های پایین حملات سایبری و دسترسی آسان به ابزارهای هک تقویت می‌شوند.

اهمیت: شناسایی اهداف مهاجمان به سازمان‌ها امکان می‌دهد تدابیر امنیتی مناسب‌تری اتخاذ کنند.

تم ۴: تدابیر پیشگیرانه

توضیح: اقدامات پیشگیرانه شامل آموزش کارکنان، به‌کارگیری فناوری‌های امنیتی و تدوین سیاست‌های مناسب است. این تدابیر می‌تواند آسیب‌پذیری سازمان‌ها را به‌طور چشمگیری کاهش دهد.

اهمیت: پیشگیری مؤثرتر از مدیریت پیامدهای حملات سایبری است.

تم ۵: پیامدهای اجتماعی و اخلاقی

توضیح: حملات سایبری علاوه بر آسیب‌های فنی و مالی، پیامدهای اجتماعی مانند کاهش اعتماد عمومی به حسابرسی دیجیتال و نگرانی‌های اخلاقی در حفظ محرمانگی اطلاعات دارند.

اهمیت: این پیامدها می‌توانند بر روابط سازمان‌ها با مشتریان و سهامداران تأثیر منفی بگذارند

بحث و نتیجه‌گیری

این تحقیق نشان داد که حملات سایبری، تهدید جدی برای حسابرسی دیجیتال محسوب می‌شوند و می‌توانند پیامدهای مالی و اعتباری قابل توجهی داشته باشند. یافته‌ها تأکید می‌کنند که تقویت امنیت سایبری و آموزش کارکنان، اولویت اصلی سازمان‌ها است. برای کاهش انگیزه مهاجمان، هزینه‌های جرم باید افزایش یابد. سیاست‌گذاران و مدیران باید به رویکردی جامع و پیشگیرانه در مقابله با حملات سایبری توجه کنند. با توجه به اهمیت روزافزون حسابرسی دیجیتال در دنیای مدرن، مقابله با حملات سایبری نه تنها یک نیاز فنی، بلکه یک ضرورت استراتژیک است. تحقیقات پیشین نشان می‌دهند که حملات سایبری به یکی از چالش‌های اصلی در فرآیندهای حسابرسی دیجیتال تبدیل شده‌اند. برای نشان دادن اهمیت این پژوهش، یافته‌های پژوهش حاضر با مطالعات دیگر مقایسه و تحلیل می‌شود تا تصویر جامع‌تری از موضوع ارائه گردد

۱. حملات سایبری و تأثیرات عملیاتی بر حسابرسی دیجیتال مطالعات مختلف نشان داده‌اند که حملات سایبری می‌توانند فرآیندهای دیجیتال را مختل کنند. براساس مطالعه آدامز و همکاران (۲۰۲۰)، حملات سایبری منجر به تغییر یا حذف داده‌های حسابرسی شده و در نتیجه کیفیت گزارش‌ها کاهش می‌یابد. این تحقیق همچنین به کاهش اعتماد ذینفعان به سیستم‌های حسابرسی دیجیتال اشاره می‌کند. نتایج پژوهش حاضر، نشان داد که اختلال در داده‌ها و کاهش دقت گزارش‌های حسابرسی از تأثیرات مستقیم حملات سایبری است. هر دو تحقیق به تأثیرات مخرب حملات بر دقت و صحت داده‌ها تأکید دارند، اما تحقیق حاضر، بر نقش این اختلالات در کاهش اعتبار سازمان نیز تمرکز کرده است

۲. ریسک‌ها و هزینه‌ها براساس نظریه مجرمانه بکر نظریه بکر بر این ایده استوار است که مجرمان (در اینجا مهاجمان سایبری) منافع مورد انتظار را در برابر هزینه‌های احتمالی می‌سنجند. براساس مطالعه جانسون (۲۰۱۸)، کاهش هزینه‌های حمله و ضعف‌های امنیتی در سیستم‌ها باعث افزایش انگیزه مهاجمان می‌شود. جانسون پیشنهاد می‌کند که افزایش هزینه‌های امنیتی و پیچیده‌تر کردن سیستم‌ها می‌تواند این حملات را کاهش دهد. نتایج پژوهش حاضر، نشان داد که افزایش هزینه‌های امنیتی و استفاده از فناوری‌های پیشرفته، تصمیم‌گیری مهاجمان را تحت تأثیر قرار می‌دهد. هر دو تحقیق بر نقش هزینه‌ها و منافع مهاجمان تأکید دارند، اما تحقیق حاضر تأثیر آموزش کارکنان و قوانین سخت‌گیرانه را نیز بررسی کرده است

۳. انگیزه‌ها و منافع مهاجمان سایبری مهاجمان سایبری اغلب به دنبال دستیابی به اطلاعات حساس یا منافع مالی هستند. براساس مطالعه اسمیت و همکاران (۲۰۲۱)، انگیزه اصلی مهاجمان، سود مالی است. این مطالعه نشان می‌دهد که دسترسی آسان به ابزارهای حمله سایبری و عدم آمادگی سازمان‌ها، مهاجمان را تشویق می‌کند. یافته پژوهش حاضر، نشان می‌دهد مهاجمان سایبری با بهره‌گیری از ضعف‌های امنیتی و اهداف مالی، سیستم‌های حسابرسی دیجیتال را هدف قرار می‌دهند. در هر دو تحقیق، انگیزه‌های مالی به‌عنوان عامل اصلی شناسایی شده است، اما تحقیق حاضر به جزئیات بیشتری درباره نقش فناوری‌های غیرقانونی در افزایش این انگیزه‌ها پرداخته است.

٤. پیامدهای اجتماعی و اخلاقی حملات سایبری حملات سایبری علاوه بر پیامدهای فنی و مالی، چالش‌های اجتماعی و اخلاقی نیز ایجاد می‌کنند. براساس مطالعه براون (۲۰۱۹)، حملات سایبری باعث کاهش اعتماد عمومی به سیستم‌های دیجیتال و ایجاد نگرانی‌های اخلاقی درباره حفظ حریم خصوصی می‌شوند. نتایج پژوهش حاضر، نشان داد که کاهش اعتماد مشتریان و چالش‌های اخلاقی مرتبط با محرمانگی داده‌ها، از پیامدهای مهم حملات سایبری است. تحقیق حاضر با تأیید نتایج براون، به پیامدهای قانونی و حقوقی نیز پرداخته و تأکید کرده است که سازمان‌ها باید برای مقابله با این چالش‌ها اقدامات جدی‌تری انجام دهند.

٥. تدابیر پیشگیرانه برای مقابله با حملات سایبری پژوهش‌های مختلف بر اهمیت تدابیر پیشگیرانه برای کاهش آسیب‌پذیری سیستم‌ها تأکید دارند. براساس مطالعه کلارک (۲۰۲۲)، استفاده از فناوری‌های پیشرفته مانند بلاکچین و هوش مصنوعی، و همچنین آموزش کارکنان، می‌تواند

سطح امنیت سایبری را افزایش دهد. بر اساس یافته پژوهش حاضر، پیشنهاد شده است که علاوه بر فناوری‌های پیشرفته، سیاست‌های سخت‌گیرانه و قوانین مرتبط با امنیت سایبری نیز اجرا شود. تحقیق حاضر با تأیید نتایج کلارک، تأکید بیشتری بر نقش سیاست‌گذاری و فرهنگ‌سازی امنیتی داشته است. نتایج تحقیق حاضر با یافته‌های تحقیقات دیگر در تأثیرات مخرب حملات سایبری، نقش هزینه‌ها و منافع مهاجمان، و اهمیت تدابیر پیشگیرانه همخوانی دارد. تحقیق حاضر به‌طور خاص براساس نظریه مجرمانه بکر انجام شده و به تحلیل تصمیم‌گیری مهاجمان براساس هزینه‌ها و منافع پرداخته است. همچنین، پیامدهای اجتماعی و قانونی حملات سایبری با جزئیات بیشتری بررسی شده‌اند.

براساس یافته‌های این پژوهش، پیشنهاداتی به شرح زیر ارائه می‌گردد:

۱. تقویت زیرساخت‌های امنیتی: یافته‌ها نشان می‌دهند که ضعف در زیرساخت‌های امنیتی، اصلی‌ترین عامل تسهیل حملات است. پیشنهاد می‌شود که سازمان‌ها به سرمایه‌گذاری در ابزارهای پیشرفته امنیت سایبری مانند سیستم‌های تشخیص نفوذ[1] و رمزگذاری قوی بپردازند.
۲. آموزش کارکنان: باتوجه به اینکه خطای انسانی، یکی از عوامل اصلی نفوذ مهاجمان است، برگزاری دوره‌های آموزشی مداوم برای کارکنان در مورد تهدیدات سایبری ضروری است.
۳. تقویت بازدارندگی قانونی: برای کاهش انگیزه مهاجمان، لازم است مجازات‌های قانونی شدیدتر و سیاست‌های بازدارنده اعمال شود.

ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.
مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.
تعارض منافع: بنا بر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.
تعهد کپی‌رایت: طبق تعهد نویسندگان حق کپی‌رایت رعایت شده‌است.

[1] IDS

منابع

بنابی قدیم، رحیم،(۱۴۰۲). امنیت سایبری مبتنی بر شواهد حسابرسی، چهارمین کنفرانس ملی پدافند سایبری، مراغه، http3s://civilica.com/doc/1917436

زارع بهنمیری، محمد جواد؛ ملکی، محمد حسن؛ حسنخانی، فاطمه و رامشه، منیژه . (۱۴۰۲). ارائه چارچوبی برای شناسایی و تحلیل پیشران‌های کلیدی اثرگذار روی آینده حسابرسی در ایران با تمرکز بر فناوری بلاک‌چین . *پژوهش‌های تجربی حسابداری، ۱۳(۳)، ۵۶-۲۷*، doi: 10.22051/jera.2023.41640.3047

نخعی، حبیب‌الله؛ برزگراول، محمد.(۱۴۰۲)، بررسی تاثیر فناوریهای دیجیتالی بر کیفیت گزارشگری مالی و حسابرسی، *فصلنامه رویکردهای نوین در علوم مدیریت*، جلد۴،شماره۲.

References

Anderson, R., & Moore, T. (2020). The economics of information security. Science.

Ageeva, O., Karp, M., & Sidorov, A. (2020, March). The application of digital technologies in financial reporting and auditing. In *Institute of Scientific Communications Conference* (pp. 1526-1534). Cham: Springer International Publishing.

Becker, G. S. (1968). Crime and Punishment: An Economic *Approach. Journal of Political Economy*, 76(2), 169-217.

Böhme, R., & Schwartz, G. (2021). Cybercrime and its economic impact. *Journal of Cyber Policy.*

Bonabi Ghadim, Rahim, (2024). Cybersecurity based on audit evidence, *Fourth National Conference on Cyber Defense, Maragha,* http://civilica.com/doc/1917436.(in persian)

Ghosh, S., & Sharman, R. (2021). Trust and security in digital auditing systems. *Computers & Security.*

Nakhaei, Habibullah; Barzegrawal, Mohammad. (۲۰۲٤), Studying the impact of digital technologies on the quality of financial reporting and auditing, *Quarterly Journal of New Approaches in Management Sciences*, Volume 4, Number 2.(in persian)

National Institute of Standards and Technology (NIST). "Cybersecurity Framework for Critical Infrastructure." Available at: https://www.nist.gov/cyberframework.

PwC Global (2023). "Digital Auditing and Cybersecurity: A Practical Guide for Organizations*." PricewaterhouseCoopers Publications.*

PwC. (2022). Cyber threats in the age of digital transformation. PwC Insights.

Sirois, L. P., Bédard, J., & Bera, P. (2020). The role of technology in modern auditing. *Accounting Horizons*.

Zare Bahnamiri, M. J. , Maleki, M. H. , Hasankhani, F. and Ramsheh, M. (2023). A Framework for Identifying and Analyzing Key Drivers Affecting Future of Auditing in Iran with a Focus on Blockchain Technology. *Empirical Research in Accounting*, *13*(3), 27-56. doi: 10.22051/jera.2023.41640.3047.(in persian)

Zheng Guohong , Xia Zhongwei , He Feng, Xiao Zhongyi.(2025). The audit committee's IT expertise and its impact on the disclosure of cybersecurity risk, *Research in International Business and Finance* 73 (2025).

Wang. L. (2025), Digital transformation, audit risk, and the low-carbon transition of China's energy enterprises, *Finance Research Letters*, 106445

COPYRIGHTS

This license allows others to download the works and share them with others as long as they credit them, but they can't change them in any way or use them commercially.