Journal of
Information System and Technology Auditing

Research Paper

Design and Validation of an Organizational Cyber Resilience Governance Framework Based on Artificial Intelligence and Risk Management: A Mixed-methods Approach to Information Technology Governance [1]

Amirhossein Kafi* [2], Mohammadali Soltanshahi [3], Mojtaba Reessafari[4] and Amirmohammad Kafi[5]

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 2, No. 1, Spring & Summer 2026
pp. 263 - 302

Received: 2026.08.05
Revised: 2026.09.14
Accepted: 2026.10.17

Abstract

With the rapid expansion of digital transformation and the growing sophistication of cyber threats, organizations require governance approaches that extend beyond traditional security controls to ensure business continuity and protect information assets. This study aims to design and validate an organizational cyber resilience governance framework based on artificial intelligence (AI) and risk management. The research is applied of purpose and adopts an exploratory mixed-methods design. In the qualitative phase, framework components were identified and refined through a systematic literature review of scientific publications published between 2020 to 2025, analysis of internationally recognized standards and frameworks—including The NIST Cybersecurity Framework (CSF) 2.0, NIST AI Risk Management Framework (AI RMF), COBIT 2019, ISO/IEC 27001:2022, ISO 31000, and COSO Enterprise Risk Management (ERM)—and a Delphi study involving experts in cybersecurity, risk management, and information technology governance. In the quantitative phase, the proposed framework was validated using a researcher-developed questionnaire and Partial Least Squares Structural Equation Modeling (PLS-SEM). The findings Identified five core dimensions: Corporate Governance, Cyber Governance, Cyber Risk Management, Artificial Intelligence, and Continuous Learning. Their systematic integration strengthens organizational capabilities for predicting, preventing, detecting, responding to, recovering from, and adapting to cyber threats. The study contributes an integrated governance framework that combines corporate governance, risk management, and AI capabilities to enhance organizational cyber resilience and support strategic decision-making in an evolving cyber threat landscape.

Keywords: Cyber Resilience Governance, Artificial Intelligence, Cyber Risk Management, Corporate Governance, Cybersecurity.

JEL classification: *M15, M14, D81, O33, L86*

---

[1] https://doi.org/10.22034/JISTA.2026.595585.1093
[1] Selected paper of the 2nd National Conference on Corporate Governance and Information Technology Risk Management
[2] PhD in Information Technology, Expert in Technological Innovation and Smart Banking Strategies, Member of Bank Sepah Research Club, Tehran, Iran. (Corresponding Author). Email: amirhkafi@gmail.com
[3] PhD in Information Technology, Expert in Artificial Intelligence and Smart Systems Development, Member of Bank Sepah Research Club, Tehran, Iran. Email: ali.soltanshahi@gmail.com
[4] PhD in Information Technology, Expert in Digital Transformation and Smart Governance, Member of Bank Sepah Research Club, Tehran, Iran. Email: mgrd81@gmail.com
[5] PhD in Information Technology, Expert in Financial Technologies and Smart Systems Analysis, Member of Sky Innovation Core, Tehran, Iran. Email: amirmkafi@gmail.com.

1. INTRODUCTION

The rapid expansion of digital transformation, cloud-based services, interconnected information systems, and data-driven decision-making has fundamentally changed the operational environment of contemporary organizations. At the same time, the increasing frequency, complexity, and adaptability of cyber threats have exposed organizations to risks that cannot be effectively addressed through conventional information security controls alone. Cyber incidents can disrupt critical services, compromise information assets, damage organizational reputation, generate financial losses, and undermine strategic objectives. Consequently, organizations increasingly need to move from a predominantly preventive security perspective toward a broader concept of organizational cyber resilience that encompasses prediction, prevention, detection, response, recovery, and adaptation.

Cyber resilience is not solely a technical issue; rather, it is closely associated with organizational governance, risk management, decision-making, organizational learning, and the effective use of emerging technologies. In particular, artificial intelligence (AI) provides significant opportunities for identifying anomalous behavior, predicting cyber threats, supporting risk assessment, accelerating incident detection, and improving strategic decision-making. However, the use of AI also introduces new governance, security, ethical, and operational risks that must themselves be systematically managed.

Despite the growing literature on cybersecurity, cyber resilience, artificial intelligence, and risk management, these areas have often been examined separately. Existing approaches provide valuable guidance but do not necessarily offer an integrated organizational governance framework that simultaneously connects corporate governance, cyber governance, cyber risk management, AI capabilities, and continuous learning. This research therefore aims to design and validate an integrated organizational cyber resilience governance framework based on artificial intelligence and risk management. The study seeks to provide a governance-oriented approach capable of strengthening organizational resilience against evolving cyber threats while supporting effective strategic decision-making.

2. MATERIALS AND METHODS

This research is applied in terms of purpose and employs an exploratory mixed-methods design consisting of qualitative and quantitative phases. In the qualitative phase, the conceptual foundations and components of the proposed framework were identified through a systematic review of scientific publications published between 2020 and 2025. In addition, internationally recognized standards and frameworks relevant to cybersecurity, artificial intelligence, information technology governance, and risk management were examined.

The principal reference frameworks included the NIST Cybersecurity Framework (CSF) 2.0, NIST Artificial Intelligence Risk Management Framework (AI RMF), COBIT 2019, ISO/IEC 27001:2022, ISO 31000, and COSO Enterprise Risk Management (ERM). The identified concepts and components were subsequently refined and assessed using the Delphi method. A panel of experts with knowledge and professional experience in cybersecurity, risk management, and information technology governance participated in this phase.

Following the qualitative phase, a researcher-developed questionnaire was designed based on the validated conceptual components. The quantitative phase was conducted to assess and validate the proposed framework using Partial Least Squares Structural Equation Modeling (PLS-SEM). This approach enabled the relationships among the identified dimensions and the overall structure of the proposed organizational cyber resilience governance framework to be examined.

3. RESULTS AND DISCUSSION

The findings of the qualitative and quantitative phases indicate that organizational cyber resilience governance can be conceptualized through five core and interrelated dimensions: Corporate Governance, Cyber Governance, Cyber Risk Management, Artificial Intelligence, and Continuous Learning. Rather than functioning as independent components, these dimensions form an integrated governance mechanism in which organizational oversight, cyber governance, risk-based decision-making, AI-enabled capabilities, and organizational learning mutually reinforce one another.

Table 1

Core Dimensions of the Proposed Organizational Cyber Resilience Governance Framework

No.	Core Dimension	Primary Role in Cyber Resilience
1	Corporate Governance	Strategic oversight, accountability, policies, and decision-making
2	Cyber Governance	Direction, control, coordination, and oversight of cybersecurity
3	Cyber Risk Management	Identification, assessment, treatment, monitoring, and control of cyber risks
4	Artificial Intelligence	Threat prediction, anomaly detection, analysis, automation, and decision support
5	Continuous Learning	Organizational learning, adaptation, improvement, and knowledge development

The first dimension, **Corporate Governance**, establishes the strategic foundation of cyber resilience. It determines organizational accountability, management commitment, policies, decision-making structures, and alignment between cybersecurity objectives and broader organizational goals. Effective corporate governance ensures that cyber resilience is treated as an enterprise-level concern rather than being limited to the information technology function.

The second dimension, **Cyber Governance**, translates organizational governance principles into cybersecurity-related direction and control. It provides mechanisms for establishing cybersecurity responsibilities, monitoring cyber capabilities, coordinating security activities, and ensuring that cybersecurity initiatives are aligned with organizational priorities. The integration of cyber governance with corporate governance strengthens accountability and facilitates coordinated responses to cyber-related risks.

The third dimension, **Cyber Risk Management**, provides a systematic mechanism for identifying and assessing cyber threats and vulnerabilities, determining their potential organizational impacts, selecting appropriate risk responses, and continuously monitoring the risk environment. This dimension connects cybersecurity activities with enterprise risk management and enables organizations to prioritize resources according to the significance and potential consequences of cyber risks.

The fourth dimension, **Artificial Intelligence**, represents an enabling technological capability within the framework. AI can enhance the organization's ability to analyze large volumes of security-related data, identify patterns and anomalies, predict emerging threats, support risk analysis, and improve the speed and quality of response. Nevertheless, AI should not be viewed merely as a technological solution. Its implementation requires appropriate governance, risk controls, transparency, accountability, and continuous monitoring to ensure that AI-related risks do not undermine organizational resilience.

The fifth dimension, **Continuous Learning**, ensures that cyber resilience evolves in response to changes in the threat environment, organizational experience, technological developments, and lessons learned from incidents. Continuous learning enables organizations to transform experience and knowledge into improvements in policies, controls, processes, capabilities, and decision-making mechanisms.

Table 2

Contribution of the Five Dimensions to the Cyber Resilience Lifecycle

Main Supporting Dimensions	Cyber Resilience Capability
Artificial Intelligence; Cyber Risk Management	Prediction
Cyber Governance; Cyber Risk Management	Prevention
Artificial Intelligence; Cyber Governance	Detection
Cyber Governance; Cyber Risk Management; Artificial Intelligence	Response
Corporate Governance; Cyber Risk Management	Recovery
Continuous Learning; Corporate Governance; Artificial Intelligence	Adaptation

The integrated interaction among these five dimensions strengthens the organization's capabilities across the complete cyber resilience lifecycle. AI contributes particularly to prediction and detection, while risk management supports prioritization and appropriate responses. Governance provides the organizational authority and coordination necessary for effective prevention, response, and recovery. Continuous learning then enables the organization to adapt its capabilities based on emerging threats and previous experiences.

The proposed framework therefore extends conventional cybersecurity models by positioning cyber resilience within a broader governance architecture. Its primary value lies not in treating AI, risk management, and governance as separate mechanisms, but in establishing systematic relationships among them. This integration can improve the organization's ability to anticipate threats, make risk-informed decisions, respond effectively to incidents, recover critical operations, and continuously adapt to a changing cyber environment.

4. CONCLUSION

This study developed and validated an integrated organizational cyber resilience governance framework based on artificial intelligence and risk management using an exploratory mixed-methods approach. The findings identified five core dimensions: Corporate Governance, Cyber Governance, Cyber Risk Management, Artificial Intelligence, and Continuous Learning. The results demonstrate that effective cyber resilience requires more than the implementation of technical security controls; it depends on the coordinated interaction of governance structures, risk management practices, AI-enabled capabilities, and organizational learning.

The proposed framework provides an integrated perspective for embedding cyber resilience within organizational and information technology governance. By connecting strategic governance with cyber risk management and AI capabilities, organizations can improve their capacity to predict, prevent, detect, respond to, recover from, and adapt to cyber threats. The framework can therefore serve as a conceptual and practical foundation for organizations seeking to strengthen cyber resilience and improve strategic decision-making under conditions of increasing cyber uncertainty and technological change.

COPYRIGHT

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.

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

مقالهٔ پژوهشی

طراحی و اعتبارسنجی چارچوب حاکمیت تاب‌آوری سایبری سازمانی مبتنی بر هوش مصنوعی و مدیریت ریسک: رویکردی آمیخته در حاکمیت فناوری اطلاعات[1]

امیرحسین کافی*[2]، محمدعلی سلطانشاهی[3]، مجتبی رئیس صفری[4] و امیرمحمد کافی[5]

حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال دوم، پیاپی ۱، بهار و تابستان ۱۴۰۵
صص ۲۶۳ - ۳۰۲

تاریخ دریافت: ۱۴۰۵/۰۵/۱۴
تاریخ بازنگری: ۱۴۰۵/۰۶/۲۳
تاریخ پذیرش: ۱۴۰۵/۰۷/۲۵

چکیده

با گسترش تحول دیجیتال و افزایش پیچیدگی تهدیدهای سایبری، سازمان‌ها برای حفظ تداوم کسب‌وکار و حفاظت از دارایی‌های اطلاعاتی، نیازمند رویکردهایی فراتر از کنترل‌های سنتی امنیت اطلاعات هستند. پژوهش حاضر با هدف طراحی چارچوب حاکمیت تاب‌آوری سایبری سازمانی مبتنی بر هوش مصنوعی و مدیریت ریسک انجام شده است. این پژوهش از نظر هدف کاربردی و از نظر روش، آمیخته اکتشافی است. در مرحله کیفی، با مرور نظام‌مند منابع علمی منتشرشده طی سال‌های ۲۰۲۰ تا ۲۰۲۵، تحلیل استانداردها و چارچوب‌های شامل NIST CSF 2.0، NIST AI RMF، COBIT 2019، ISO/IEC 27001:2022، ISO 31000 و COSO ERM و نیز بهره‌گیری از روش دلفی با مشارکت خبرگان حوزه امنیت سایبری، مدیریت ریسک و حاکمیت فناوری اطلاعات، مؤلفه‌های چارچوب استخراج و پالایش شد. در مرحله کمی نیز اعتبار چارچوب پیشنهادی از طریق پرسشنامه محقق‌ساخته و مدل‌یابی معادلات ساختاری مبتنی بر حداقل مربعات جزئی مورد ارزیابی قرار گرفت. یافته‌های پژوهش نشان داد که چارچوب پیشنهادی از پنج بُعد اصلی شامل حاکمیت شرکتی، حاکمیت سایبری، مدیریت ریسک سایبری، هوش مصنوعی و یادگیری مستمر تشکیل شده است که تعامل نظام‌مند آن‌ها موجب ارتقای پیش‌بینی، پیشگیری، تشخیص، پاسخ، بازیابی و انطباق سازمان در برابر تهدیدهای سایبری می‌شود. نوآوری پژوهش در ارائه چارچوبی یکپارچه است که با تلفیق اصول حاکمیت شرکتی، مدیریت ریسک و قابلیت‌های هوش مصنوعی، زمینه افزایش تاب‌آوری سایبری و بهبود کیفیت تصمیم‌گیری راهبردی سازمان‌ها را فراهم می‌سازد.

واژه‌های کلیدی: *حاکمیت تاب‌آوری سایبری، هوش مصنوعی، مدیریت ریسک سایبری، حاکمیت شرکتی، امنیت سایبری.*

طبقه‌بندی موضوعی: *M15, M14, D81, O33, L86.*

---

[1] https://doi.org/10.22034/JISTA.2026.595585.1093

[1] مقاله منتخب دومین همایش ملی حاکمیت شرکتی و مدیریت ریسک‌های فناوری اطلاعات

[2] دانشجوی دکتری فناوری اطلاعات، متخصص نوآوری فناورانه و راهبردهای بانکداری هوشمند، عضو باشگاه پژوهان بانک سپه، تهران، ایران. (نویسنده مسئول). (amirhkafi@gmail.com)

[3] دکتری فناوری اطلاعات، متخصص هوش مصنوعی و توسعه سامانه‌های هوشمند، عضو باشگاه پژوهان بانک سپه، تهران، ایران. (ali.soltanshahi@gmail.com)

[4] دکتری فناوری اطلاعات، متخصص تحول دیجیتال و حکمرانی هوشمند، عضو باشگاه پژوهان بانک سپه، تهران، ایران. (mgrd81@gmail.com)

[5] دانشجوی دکتری فناوری اطلاعات، متخصص فناوری‌های مالی و تحلیل سامانه‌های هوشمند، عضو هسته نوآوری اسکای، تهران، ایران (amirmkafi@gmail.com)

مقدمه

تحول دیجیتال در سال‌های اخیر، سازمان‌ها را با فرصت‌های بی‌سابقه‌ای در زمینه افزایش بهره‌وری، توسعه خدمات هوشمند و بهبود فرایندهای تصمیم‌گیری مواجه کرده است؛ بااین‌حال، همین تحول موجب گسترش سطح حملات سایبری، پیچیده‌تر شدن تهدیدها و افزایش وابستگی سازمان‌ها به زیرساخت‌های دیجیتال شده است. امروزه دارایی‌های اطلاعاتی، سامانه‌های عملیاتی، خدمات برخط و زنجیره‌های تأمین دیجیتال، بخش جدایی‌ناپذیر ارزش‌آفرینی سازمان‌ها محسوب می‌شوند و هرگونه اختلال در امنیت یا دسترس‌پذیری آن‌ها می‌تواند پیامدهای مالی، عملیاتی، حقوقی و اعتباری گسترده‌ای به همراه داشته باشد. بر همین اساس، امنیت سایبری دیگر صرفاً یک موضوع فنی تلقی نمی‌شود، بلکه به یکی از ارکان اساسی حاکمیت سازمانی، مدیریت ریسک و تداوم کسب‌وکار تبدیل شده است (مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۳-۴؛ آژانس اتحادیه اروپا برای امنیت سایبری، ۱۴۰۳: ۲۱-۲۰).

بررسی گزارش‌های بین‌المللی نشان می‌دهد که در سال‌های اخیر، حملات باج‌افزاری، حملات زنجیره تأمین، سوءاستفاده از هوش مصنوعی مولد، حملات مبتنی بر مهندسی اجتماعی و تهدیدات پیشرفته مداوم، از مهم‌ترین چالش‌های محیط امنیت سایبری بوده‌اند. این تهدیدها تنها زیرساخت‌های فناوری اطلاعات را هدف قرار نمی‌دهند، بلکه توان عملیاتی، اعتبار سازمان، اعتماد ذی‌نفعان و استمرار ارائه خدمات حیاتی را نیز تحت تأثیر قرار می‌دهند (آژانس اتحادیه اروپا برای امنیت سایبری، ۱۴۰۳: ۲۰-۲۱؛ آی‌بی‌ام، ۱۴۰۳: ۹-۱۷؛ مجمع جهانی اقتصاد، ۱۴۰۳: ۶ ، ۱۲). ازاین‌رو، رویکردهای سنتی امنیت اطلاعات که عمدتاً بر پیشگیری از نفوذ متمرکز بودند، به‌تنهایی پاسخگوی محیط پیچیده و پویای تهدیدات سایبری نیستند.

در چنین شرایطی، مفهوم تاب‌آوری سایبری[1] به‌عنوان رویکردی مکمل برای مدیریت امنیت سایبری مطرح شده است. برخلاف رویکردهای سنتی امنیت سایبری که تمرکز اصلی آن‌ها بر پیشگیری و حفاظت در برابر حملات است، تاب‌آوری سایبری بر توانایی سازمان برای آمادگی و پیش‌بینی، مقاومت در برابر اختلال، پاسخ‌گویی مؤثر، بازیابی سریع و انطباق با شرایط پس از وقوع حوادث سایبری تأکید دارد. از این منظر، هدف تاب‌آوری صرفاً جلوگیری از وقوع حادثه

[1] Cyber Resilience

نیست، بلکه حفظ و تداوم قابلیت‌های حیاتی سازمان در شرایط اختلال و بازگشت مؤثر به وضعیت عملیاتی مطلوب است (آژانس اتحادیه اروپا برای امنیت سایبری، ۱۴۰۳: ۲۰-۲۱، ۱۵،۱۰؛ مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۳-۴).

در کنار توسعه مفهوم تاب‌آوری سایبری، حاکمیت سازمانی نیز طی سال‌های اخیر دستخوش تحول قابل‌توجهی شده است. در گذشته، مسئولیت امنیت اطلاعات عمدتاً بر عهده واحد فناوری اطلاعات قرار داشت؛ اما امروزه هیئت‌مدیره، کمیته‌های ریسک، مدیران ارشد و سایر ذی‌نفعان نقش مستقیمی در سیاست‌گذاری، نظارت و مدیریت ریسک‌های سایبری بر عهده دارند. چارچوب‌های نوین حاکمیت و مدیریت فناوری اطلاعات، نظیر کوبیت ۲۰۱۹[1]، و چارچوب‌های مدیریت ریسک سازمانی، نظیر مدل مدیریت ریسک سازمانی کوزو[2] و استاندارد ایزو ۳۱۰۰۰[3]، بر همسوسازی تصمیمات راهبردی، مدیریت ریسک و سازوکارهای کنترلی سازمان تأکید دارند (ایساکا، ۱۳۹۹: ۱۰؛ کمیته سازمان‌های حامی کمیسیون تردوی، ۱۳۹۷: ۱۰، ۱۴؛ سازمان بین‌المللی استانداردسازی، ۱۳۹۷: ۱۴).

از سوی دیگر، گسترش حجم داده‌ها، پیچیدگی تهدیدها و سرعت تغییرات محیط سایبری موجب شده است که تحلیل انسانی به‌تنهایی برای شناسایی و مدیریت تمامی مخاطرات کافی نباشد. در چنین شرایطی، هوش مصنوعی به‌عنوان یکی از فناوری‌های تحول‌آفرین، ظرفیت قابل‌توجهی برای ارتقای امنیت سایبری و افزایش تاب‌آوری سازمانی ایجاد کرده است. الگوریتم‌های یادگیری ماشین، یادگیری عمیق، تحلیل رفتار کاربران، پردازش زبان طبیعی و تحلیل کلان‌داده‌ها می‌توانند در شناسایی الگوهای غیرعادی، تشخیص تهدیدها، کاهش هشدارهای کاذب و پشتیبانی از فرایند تصمیم‌گیری در مدیریت ریسک مورد استفاده قرار گیرند (آژانس اتحادیه اروپا برای امنیت سایبری، ۱۴۰۳: ۲۰-۲۱؛ مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۳-۴).

در مقابل، استفاده از هوش مصنوعی نیز با چالش‌هایی نظیر سوگیری الگوریتمی، حملات خصمانه علیه مدل‌های یادگیری ماشین، نبود شفافیت و تبیین‌پذیری در برخی تصمیمات هوشمند و مخاطرات حاکمیتی همراه است. به همین دلیل، در سال‌های اخیر مفهوم حاکمیت هوش

[1] COBIT 2019 (Control Objectives for Information and Related Technologies)
[2] COSO Enterprise Risk Management (COSO ERM)
[3] ISO 31000:2018 (Risk Management—Guidelines)

مصنوعی[1] نیز مورد توجه نهادهای بین‌المللی قرار گرفته است. در همین راستا، مؤسسه ملی استانداردها و فناوری ایالات متحده در سال ۲۰۲۳ چارچوب مدیریت ریسک هوش مصنوعی را با هدف ارائه رویکردی نظام‌مند برای شناسایی، ارزیابی و مدیریت ریسک‌های مرتبط با سامانه‌های هوش مصنوعی منتشر کرد (مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۴-۳). بنابراین، استفاده مؤثر از هوش مصنوعی در امنیت سایبری مستلزم استقرار سازوکارهای حاکمیتی، کنترل‌های مدیریتی و فرایندهای منسجم ارزیابی و مدیریت ریسک است.

اگرچه مطالعات متعددی در زمینه امنیت سایبری، مدیریت ریسک، حاکمیت فناوری اطلاعات، تاب‌آوری سایبری و کاربرد هوش مصنوعی انجام شده است، بررسی ادبیات پژوهش نشان می‌دهد که بخش قابل‌توجهی از این مطالعات هر یک بر یکی از ابعاد مسئله تمرکز داشته‌اند. برخی پژوهش‌ها بر کاربرد هوش مصنوعی در تشخیص و مدیریت تهدیدات سایبری تمرکز کرده‌اند، برخی دیگر چارچوب‌های مدیریت ریسک و بلوغ امنیت سایبری را بررسی کرده‌اند و گروهی نیز به حاکمیت و مدیریت فناوری اطلاعات پرداخته‌اند. بااین‌حال، همچنان نیاز به چارچوب‌های یکپارچه‌ای وجود دارد که بتوانند ارتباط میان حاکمیت سازمانی، مدیریت ریسک، هوش مصنوعی و تاب‌آوری سایبری را در سطح سازمانی تبیین کنند (مک‌اینتاش و همکاران، ۱۴۰۳: ۱۱، ۱۴؛ آلهیدایفی و همکاران، ۱۴۰۳: ۱۱).

این خلأ پژوهشی به‌ویژه در سازمان‌های بزرگ، بانک‌ها، شرکت‌های زیرساختی و نهادهای دولتی اهمیت بیشتری پیدا می‌کند؛ زیرا این سازمان‌ها علاوه بر تهدیدهای سایبری، با الزامات قانونی و مقرراتی، الزامات حاکمیت سازمانی، انتظارات ذی‌نفعان و ضرورت تداوم ارائه خدمات نیز مواجه هستند. در چنین سازمان‌هایی، اتخاذ تصمیمات امنیتی صرفاً بر اساس شاخص‌های فنی کافی نیست و لازم است ابعاد مدیریتی، راهبردی، اقتصادی و حاکمیتی نیز به‌صورت همزمان مورد توجه قرار گیرد (سازمان همکاری و توسعه اقتصادی، ۱۴۰۲؛ مجمع جهانی اقتصاد، ۱۴۰۳: ۶، ۱۲).

بر این اساس، مسئله اصلی پژوهش حاضر آن است که چگونه می‌توان با تلفیق اصول حاکمیت شرکتی، مدیریت ریسک و قابلیت‌های هوش مصنوعی، چارچوبی جامع برای افزایش تاب‌آوری سایبری سازمان طراحی کرد؛ چارچوبی که علاوه بر ارتقای توان پیشگیری، قابلیت

[1] AI Governance

شناسایی سریع تهدیدها، پشتیبانی از تصمیم‌گیری مدیریتی، پاسخ‌گویی هوشمند به حوادث، بازیابی سریع خدمات و یادگیری مستمر از رخدادهای امنیتی را نیز فراهم سازد.

هدف اصلی این پژوهش، طراحی و تبیین یک چارچوب حاکمیت تاب‌آوری سایبری سازمانی مبتنی بر هوش مصنوعی و مدیریت ریسک است که بتواند تعامل میان ساختارهای حاکمیتی، فرآیندهای مدیریت ریسک، فناوری‌های هوش مصنوعی و قابلیت‌های تاب‌آوری سایبری را به‌صورت نظام‌مند تشریح کند. همچنین این پژوهش درصدد است مؤلفه‌های اصلی این چارچوب، روابط میان آن‌ها و نقش هر یک در ارتقای تاب‌آوری سازمانی را مشخص کرده و زمینه لازم برای ارزیابی و پیاده‌سازی آن در سازمان‌های ایرانی را فراهم آورد.

اهمیت این پژوهش از دو جنبه نظری و کاربردی قابل تبیین است. از منظر نظری، پژوهش حاضر با یکپارچه‌سازی مفاهیم حاکمیت شرکتی، مدیریت ریسک، هوش مصنوعی و تاب‌آوری سایبری، مدلی مفهومی ارائه می‌کند که می‌تواند مبنای توسعه پژوهش‌های آینده قرار گیرد. از منظر کاربردی نیز چارچوب پیشنهادی می‌تواند به مدیران ارشد، اعضای هیئت‌مدیره، مدیران امنیت اطلاعات، مدیران فناوری اطلاعات و مدیران ریسک در طراحی سیاست‌های امنیتی، تخصیص منابع، اولویت‌بندی مخاطرات و افزایش آمادگی سازمان در برابر تهدیدهای سایبری کمک کند.

در این پژوهش، حاکمیت تاب‌آوری سایبری به مجموعه‌ای از ساختارها، سیاست‌ها، فرآیندها و سازوکارهای مدیریتی اطلاق می‌شود که با بهره‌گیری از اصول حاکمیت شرکتی، مدیریت ریسک و فناوری‌های هوش مصنوعی، توان سازمان را در پیش‌بینی، پیشگیری، مقاومت، پاسخ‌گویی، بازیابی و انطباق در برابر تهدیدهای سایبری افزایش می‌دهد. همچنین هوش مصنوعی به سامانه‌هایی اطلاق می‌شود که با استفاده از الگوریتم‌های یادگیری ماشین، یادگیری عمیق، تحلیل داده و استنتاج هوشمند، قابلیت شناسایی الگوهای تهدید، پیش‌بینی مخاطرات، تحلیل رفتار، اولویت‌بندی هشدارها و پشتیبانی از تصمیم‌گیری مدیران را فراهم می‌کنند. در این پژوهش، مدیریت ریسک سایبری نیز به فرآیند نظام‌مند شناسایی، تحلیل، ارزیابی، پاسخ و پایش مستمر مخاطرات سایبری بر اساس چارچوب‌های بین‌المللی مدیریت ریسک اطلاق می‌شود.

در نهایت، ساختار مقاله در پنج بخش تنظیم شده است. پس از مقدمه، در بخش دوم مبانی نظری و توسعه فرضیه‌ها با مرور و تحلیل یکپارچه پژوهش‌های داخلی و خارجی ارائه می‌شود. در بخش سوم روش‌شناسی پژوهش و نحوه طراحی چارچوب پیشنهادی تشریح خواهد شد. بخش چهارم به ارائه یافته‌های پژوهش و چارچوب نهایی اختصاص دارد و در پایان، نتایج، کاربردهای مدیریتی، محدودیت‌ها و پیشنهادهای پژوهشی در قالب بحث و نتیجه‌گیری ارائه می‌شود.

شکل ۱. روند تکامل رویکردهای امنیت سازمانی تا حاکمیت تاب‌آوری سایبری مبتنی بر هوش مصنوعی

مبانی نظری و توسعه فرضیه‌ها

حاکمیت شرکتی و حاکمیت سایبری

افزایش وابستگی سازمان‌ها به فناوری‌های دیجیتال موجب شده است که ریسک‌های سایبری از سطح مخاطرات عملیاتی فراتر رفته و به یکی از مهم‌ترین ریسک‌های راهبردی سازمان‌ها تبدیل شوند. در چنین شرایطی، حاکمیت شرکتی دیگر تنها بر نظارت مالی، رعایت مقررات و پاسخگویی مدیریتی متمرکز نیست، بلکه مدیریت ریسک‌های فناوری اطلاعات، امنیت سایبری و تاب‌آوری دیجیتال نیز به بخشی جدایی‌ناپذیر از مسئولیت‌های هیئت‌مدیره و مدیران ارشد تبدیل شده است (سازمان همکاری و توسعه اقتصادی، ۱۴۰۲).

مطابق تعریف سازمان همکاری و توسعه اقتصادی، حاکمیت شرکتی مجموعه‌ای از روابط میان هیئت‌مدیره، مدیران اجرایی، سهامداران و سایر ذی‌نفعان است که چارچوب لازم برای

تعیین اهداف سازمان، نحوه دستیابی به این اهداف و نظارت بر عملکرد را فراهم می‌کند (سازمان همکاری و توسعه اقتصادی، ۱۴۰۲). در این چارچوب، مدیریت ریسک‌های سایبری دیگر یک مسئولیت صرفاً فنی محسوب نمی‌شود، بلکه بخشی از نظام تصمیم‌گیری کلان سازمان است.

در سال‌های اخیر مفهوم حاکمیت سایبری[1] به‌عنوان توسعه‌ای از حاکمیت فناوری اطلاعات مطرح شده است. حاکمیت سایبری بر تعیین مسئولیت‌ها، سیاست‌گذاری امنیتی، تخصیص منابع، نظارت مستمر، مدیریت ریسک و ارزیابی عملکرد امنیت سایبری در سطح هیئت‌مدیره تأکید دارد نیز بیان می‌کند که ارزش‌آفرینی از فناوری اطلاعات تنها زمانی امکان‌پذیر است که میان اهداف کسب‌وکار، مدیریت ریسک، امنیت اطلاعات و کنترل‌های حاکمیتی هماهنگی وجود داشته باشد (ایساکا، ۱۳۹۹).

مطالعات جدید نشان می‌دهد سازمان‌هایی که هیئت‌مدیره آن‌ها دارای کمیته تخصصی امنیت سایبری هستند، در مدیریت رخدادهای امنیتی، بازیابی خدمات و کاهش خسارات مالی عملکرد بهتری نسبت به سایر سازمان‌ها دارند (دیلویت، ۱۴۰۳).

تاب‌آوری سایبری

مفهوم تاب‌آوری سایبری طی یک دهه گذشته به یکی از مهم‌ترین موضوعات پژوهش‌های امنیت اطلاعات تبدیل شده است. برخلاف رویکرد سنتی امنیت سایبری که هدف اصلی آن جلوگیری از وقوع حملات است، تاب‌آوری سایبری بر این فرض استوار است که هیچ سامانه‌ای مصون از نفوذ نیست و سازمان باید حتی در صورت موفقیت مهاجم نیز قادر به ادامه فعالیت‌های حیاتی خود باشد (مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۳-۴).

چارچوب جدید چارچوب امنیت سایبری مؤسسه ملی استانداردها و فناوری ایالات متحده ۲.۰[2] تاب‌آوری سایبری را مجموعه‌ای از قابلیت‌های سازمان در پنج مرحله اصلی معرفی می‌کند:

- شناسایی
- حفاظت
- کشف

[1] Cyber Governance
[2] National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0

- پاسخ
- بازیابی

در نسخه جدید این چارچوب، مؤلفه حاکمیت نیز به‌عنوان لایه راهبری به مدل اضافه شده است که نقش حاکمیت سازمانی را در امنیت سایبری برجسته می‌کند (مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۳-۴).

از دیدگاه از دیدگاه استاندارد ایزو/آی‌ای‌سی ۲۷۰۰۱:۲۰۲۲[1] نیز تاب‌آوری سایبری تنها با استقرار کنترل‌های امنیتی حاصل نمی‌شود، بلکه نیازمند مدیریت مستمر ریسک، بهبود فرآیندها، آموزش کارکنان، ارزیابی تهدیدها و آمادگی برای بازیابی است (سازمان بین‌المللی استانداردسازی، ۱۳۹۷: ۱۴).

در پژوهش‌های مرتبط با تاب‌آوری سایبری نیز بر ضرورت نگاه یکپارچه به امنیت، مدیریت ریسک و قابلیت‌های سازمانی تأکید شده است. در این چارچوب، تاب‌آوری سایبری را می‌توان به‌عنوان توانایی سازمان یا سامانه برای آمادگی در برابر تهدیدها، مقاومت در برابر اختلالات، پاسخ‌گویی مؤثر، بازیابی قابلیت‌های حیاتی و انطباق با شرایط پس از وقوع حادثه در نظر گرفت. همچنین، پژوهش‌های حوزه حاکمیت فناوری اطلاعات نشان می‌دهند که افزایش بلوغ سازوکارهای حاکمیتی می‌تواند به بهبود قابلیت سازمان در مدیریت ریسک‌های فناوری و افزایش ظرفیت پاسخ‌گویی و بازیابی در برابر اختلالات سایبری کمک کند (مک‌اینتاش و همکاران، ۱۴۰۳: ۱۱، ۱۴؛ آلهیدایفی و همکاران، ۱۴۰۳: ۱۱).

همچنین شارما[2] و همکاران (۲۰۲۳) بیان کردند که سازمان‌های دارای بلوغ بالاتر در حاکمیت فناوری اطلاعات، زمان بازیابی خدمات[3] را به‌طور معناداری کاهش داده‌اند.

مدیریت ریسک سایبری

مدیریت ریسک یکی از ارکان اصلی تاب‌آوری سازمانی است. مطابق استاندارد ایزو ۳۱۰۰۰:۲۰۱۸[4]، مدیریت ریسک فرآیندی نظام‌مند برای شناسایی، تحلیل، ارزیابی، پاسخ و

[1] ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements
[2] Sharma
[3] Recovery Time Objective
[4] ISO 31000:2018 — Risk management — Guidelines

پایش ریسک‌ها است که باید در تمام سطوح سازمان جاری باشد (سازمان بین‌المللی استانداردسازی، ۱۳۹۷: ۱۴). اگرچه این استاندارد پیش از سال ۲۰۲۰ منتشر شده است، اما همچنان معتبرترین مرجع جهانی مدیریت ریسک بوده و در پژوهش‌های جدید نیز به‌طور گسترده مورد استناد قرار می‌گیرد.

در حوزه امنیت سایبری، مدیریت ریسک به فرآیند شناسایی دارایی‌های حیاتی، تهدیدها، آسیب‌پذیری‌ها، احتمال وقوع رخداد و میزان اثر آن بر اهداف سازمان اشاره دارد (مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۳-۴).

چارچوب مدیریت ریسک سازمانی کمیته سازمان‌های حامی کمیسیون تردوی[1] نیز بر یکپارچگی میان تصمیمات راهبردی، کنترل‌های داخلی، مدیریت ریسک و حاکمیت شرکتی تأکید دارد و معتقد است ریسک‌های سایبری باید همانند سایر ریسک‌های راهبردی در سطح هیئت‌مدیره مدیریت شوند (کمیته سازمان‌های حامی کمیسیون تردوی، ۱۳۹۷: ۱۰، ۱۴).

گزارش شرکت آی‌بی‌ام[2] در سال ۲۰۲۴ می‌دهد میانگین هزینه هر رخداد نشت اطلاعات در سال ۲۰۲۴ به بیش از ۸/۴ میلیون دلار رسیده است. همچنین سازمان‌هایی که از سامانه‌های هوشمند تشخیص تهدید و مدیریت ریسک استفاده می‌کنند، زمان شناسایی حمله را به‌طور متوسط بیش از ۳۰ درصد کاهش داده‌اند (آی‌بی‌ام، ۱۴۰۳: ۹-۱۷).

ازاین‌رو، مدیریت ریسک دیگر صرفاً ابزاری برای کاهش احتمال وقوع تهدید نیست، بلکه سازوکاری برای افزایش تاب‌آوری و تضمین تداوم خدمات سازمانی محسوب می‌شود.

هوش مصنوعی در امنیت سایبری

رشد سریع حجم داده‌های امنیتی و پیچیدگی حملات سایبری موجب شده است که روش‌های سنتی تحلیل داده دیگر پاسخگوی نیاز سازمان‌ها نباشند. در چنین شرایطی، هوش مصنوعی به یکی از فناوری‌های کلیدی امنیت سایبری تبدیل شده است.

مطابق گزارش آژانس اتحادیه اروپا برای امنیت سایبری[3] در سال ۲۰۲۳، مهم‌ترین کاربردهای هوش مصنوعی در امنیت سایبری عبارت‌اند از:

[1] COSO Enterprise Risk Management (COSO ERM)
[2] IBM
[3] European Union Agency for Cybersecurity (ENISA)

- تشخیص ناهنجاری‌های رفتاری
- تحلیل ترافیک شبکه
- شناسایی بدافزارهای ناشناخته
- کشف حملات روز صفر[1]
- اولویت‌بندی هشدارهای امنیتی
- تحلیل رفتار کاربران
- پیش‌بینی تهدیدها

الگوریتم‌های یادگیری ماشین قادرند میلیون‌ها رویداد امنیتی را در مدت کوتاهی تحلیل کرده و الگوهایی را شناسایی کنند که برای تحلیل‌گران انسانی قابل مشاهده نیست.

علاوه بر این، هوش مصنوعی مولد نیز در سال‌های اخیر وارد حوزه امنیت سایبری شده است. این فناوری می‌تواند در تولید خودکار گزارش‌های امنیتی، تحلیل رخدادها، پاسخ‌گویی به حوادث و تولید سناریوهای حمله مورد استفاده قرار گیرد؛ هرچند همین فناوری می‌تواند توسط مهاجمان نیز برای طراحی حملات پیچیده‌تر مورد سوءاستفاده قرار گیرد (مجمع جهانی اقتصاد، ۱۴۰۳: ۶ ، ۱۲).

به همین دلیل، مؤسسه مؤسسه ملی استانداردها و فناوری در سال ۲۰۲۳ چارچوب چارچوب مدیریت ریسک هوش مصنوعی[2] را منتشر کرد که هدف آن مدیریت ریسک‌های مرتبط با سامانه‌های هوش مصنوعی از منظر اعتمادپذیری، شفافیت، عدالت، امنیت و پاسخگویی است (مؤسسه ملی استانداردها و فناوری، ۱۴۰۲: ۱۲).

[1] Zero-Day
[2] NIST Artificial Intelligence Risk Management Framework (AI RMF)

جدول ۱

مقایسه رویکردهای سنتی امنیت سایبری با رویکرد حاکمیت تاب‌آوری سایبری مبتنی بر هوش مصنوعی

شاخص	امنیت سایبری سنتی	حاکمیت تاب‌آوری سایبری مبتنی بر هوش مصنوعی
هدف اصلی	جلوگیری از نفوذ	حفظ تداوم کسب‌وکار در زمان حمله
مسئول اصلی	واحد فناوری اطلاعات	هیئت‌مدیره، مدیران ارشد و واحدهای تخصصی
تصمیم‌گیری	واکنشی	پیش‌بینانه و هوشمند
تحلیل داده	دستی و مبتنی بر قوانین	یادگیری ماشین و تحلیل بلادرنگ
مدیریت ریسک	دوره‌ای	مستمر و پویا
پاسخ به رخداد	پس از وقوع	پیش‌بینی، پاسخ خودکار و بازیابی هوشمند
یادگیری	محدود	یادگیری مستمر مبتنی بر داده

تحلیل یکپارچه پژوهش‌های پیشین

مرور پژوهش‌های انجام‌شده در سال‌های اخیر نشان می‌دهد که اگرچه ادبیات پژوهش در حوزه امنیت سایبری، مدیریت ریسک، حاکمیت فناوری اطلاعات و هوش مصنوعی به‌طور مستقل توسعه قابل‌توجهی یافته است، اما هنوز یک چارچوب جامع که این چهار حوزه را به‌صورت یکپارچه و از منظر حاکمیت سازمانی تلفیق کند، کمتر ارائه شده است. بخش عمده‌ای از مطالعات بر توسعه الگوریتم‌های هوش مصنوعی برای تشخیص نفوذ، شناسایی بدافزار یا تحلیل رفتار کاربران متمرکز بوده‌اند، در حالی که ابعاد مدیریتی، نقش هیئت‌مدیره، فرآیندهای

تصمیم‌گیری راهبردی و تعامل میان هوش مصنوعی و مدیریت ریسک کمتر مورد توجه قرار گرفته است (کور، اسلام و رضاق، ۲۰۲۲: ۷؛ شارما، ۲۰۲۳: ۹).

در پژوهش‌های داخلی نیز تمرکز عمدتاً بر ارزیابی بلوغ امنیت اطلاعات، مدیریت ریسک فناوری اطلاعات یا پیاده‌سازی استانداردهایی نظیر ایزو/آی‌ای‌سی ۲۷۰۰۱:۲۰۲۲ بوده و کمتر پژوهشی به طراحی چارچوبی یکپارچه برای حاکمیت تاب‌آوری سایبری مبتنی بر هوش مصنوعی پرداخته است. این خلأ پژوهشی، ضرورت توسعه مدلی بومی و در عین حال منطبق با استانداردهای بین‌المللی را برجسته می‌سازد. بر همین اساس، پژوهش حاضر با تلفیق چارچوب‌های امنیت سایبری مؤسسه ملی استانداردها و فناوری ایالات متحده ۲.۰، چارچوب مدیریت ریسک هوش مصنوعی مؤسسه ملی استانداردها و فناوری، اهداف حاکمیت و مدیریت فناوری اطلاعات ۲۰۱۹، استاندارد ایزو/آی‌ای‌سی ۲۷۰۰۱:۲۰۲۲ و استاندارد ایزو ۳۱۰۰۰:۲۰۱۸ در پی ارائه یک چارچوب حاکمیتی جامع است که بتواند نقش هوش مصنوعی را در تمامی مراحل چرخه مدیریت ریسک و ارتقای تاب‌آوری سایبری تبیین کند.

توسعه چارچوب مفهومی پژوهش

با توجه به مبانی نظری ارائه‌شده، بررسی پژوهش‌های پیشین و تحلیل استانداردهای بین‌المللی، می‌توان دریافت که هیچ‌یک از چارچوب‌های موجود به‌تنهایی قادر به پوشش هم‌زمان ابعاد حاکمیت شرکتی، مدیریت ریسک سایبری، هوش مصنوعی و تاب‌آوری سازمانی نیستند. برای نمونه، چارچوب چارچوب امنیت سایبری مؤسسه ملی استانداردها و فناوری ایالات متحده ۲.۰ بر چرخه مدیریت امنیت سایبری و حاکمیت تمرکز دارد، اما به نحوه بهره‌گیری از هوش مصنوعی در تصمیم‌گیری مدیریتی نمی‌پردازد (مؤسسه ملی استانداردها و فناوری ایالات متحده، ۱۴۰۲: ۳-۴). همچنین چارچوب مدیریت ریسک هوش مصنوعی مؤسسه ملی استانداردها و فناوری بر مدیریت ریسک سامانه‌های هوش مصنوعی متمرکز است و ارتباط مستقیمی با فرآیندهای حاکمیت سایبری سازمانی ارائه نمی‌کند. از سوی دیگر، چارچوب کوبیت ۲۰۱۹[1] سازوکارهای حاکمیتی فناوری اطلاعات را تبیین می‌کند، اما معماری عملیاتی مشخصی برای افزایش تاب‌آوری سایبری مبتنی بر هوش مصنوعی پیشنهاد نمی‌دهد (انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی، ۱۳۹۸: ۱۰، ۱۳، ۱۷).

[1] COBIT 2019

بر همین اساس، پژوهش حاضر با تلفیق نقاط قوت این چارچوب‌ها، مدلی مفهومی برای حاکمیت تاب‌آوری سایبری سازمانی مبتنی بر هوش مصنوعی و مدیریت ریسک ارائه می‌کند. در این مدل، تاب‌آوری سایبری نتیجه تعامل پویا میان پنج مؤلفه اصلی است:

- حاکمیت شرکتی
- حاکمیت سایبری
- مدیریت ریسک سایبری
- هوش مصنوعی
- بهبود مستمر و یادگیری سازمانی

در چارچوب پیشنهادی، حاکمیت شرکتی به‌عنوان لایه راهبردی، سیاست‌ها، اهداف، حدود مسئولیت‌ها و میزان ریسک‌پذیری سازمان را تعیین می‌کند. در سطح بعد، حاکمیت سایبری وظیفه تبدیل سیاست‌های کلان به سازوکارهای اجرایی، کنترل‌های امنیتی، پایش عملکرد و تخصیص منابع را بر عهده دارد. این لایه، ارتباط میان هیئت‌مدیره، مدیران ارشد، مدیران فناوری اطلاعات و واحدهای امنیت اطلاعات را برقرار می‌کند.

در ادامه، مدیریت ریسک سایبری به‌عنوان هسته تصمیم‌گیری عمل می‌کند و با شناسایی دارایی‌های حیاتی، تحلیل تهدیدها، ارزیابی آسیب‌پذیری‌ها، تعیین احتمال وقوع و برآورد پیامدهای حملات، اولویت‌های امنیتی سازمان را مشخص می‌سازد. داده‌های حاصل از این فرآیند به موتور هوش مصنوعی منتقل می‌شود تا تحلیل‌های پیشرفته و پیش‌بینی‌های لازم انجام گیرد.

در این چارچوب، هوش مصنوعی صرفاً ابزار تشخیص نفوذ نیست، بلکه نقش یک سامانه تصمیم‌یار مدیریتی را ایفا می‌کند. این سامانه با استفاده از الگوریتم‌های یادگیری ماشین، یادگیری عمیق و تحلیل داده‌های بلادرنگ، الگوهای تهدید را شناسایی کرده، احتمال وقوع رخدادهای امنیتی را پیش‌بینی می‌کند، هشدارها را اولویت‌بندی کرده و سناریوهای پاسخ مناسب را پیشنهاد می‌دهد. همچنین خروجی‌های این سامانه می‌تواند مبنای تصمیم‌گیری مدیران در تخصیص منابع، اصلاح سیاست‌ها و بازنگری کنترل‌های امنیتی قرار گیرد (آژانس اتحادیه اروپا برای امنیت سایبری، ۱۴۰۳: ۲۰-۲۱؛ مایکروسافت، ۱۴۰۳: ۸۱).

ویژگی متمایز چارچوب پیشنهادی، وجود چرخه بازخورد و یادگیری مستمر است. برخلاف مدل‌های خطی مدیریت ریسک، در این پژوهش نتایج حاصل از هر رخداد سایبری، داده‌های جدیدی برای آموزش مجدد مدل‌های هوش مصنوعی و بهبود سیاست‌های حاکمیتی فراهم می‌کند. به این ترتیب، چارچوب پیشنهادی از یک سامانه ایستا به یک سامانه یادگیرنده و تطبیق‌پذیر تبدیل می‌شود که می‌تواند همگام با تغییرات محیط تهدید تکامل یابد. این ویژگی با مفهوم «تاب‌آوری پویا» همسو است که در پژوهش‌های جدید به‌عنوان یکی از شاخص‌های بلوغ امنیت سایبری مطرح شده است (مجمع جهانی اقتصاد، ۱۴۰۳: ۱۸).

از منظر مدیریتی، چارچوب پیشنهادی سه مزیت اساسی دارد. نخست، ارتباط مستقیم میان تصمیمات هیئت‌مدیره و شاخص‌های عملیاتی امنیت سایبری را برقرار می‌کند. دوم، استفاده از هوش مصنوعی موجب افزایش سرعت و دقت تحلیل ریسک و کاهش زمان کشف و پاسخ به رخدادها می‌شود. سوم، با ایجاد چرخه یادگیری مستمر، زمینه بهبود مداوم سطح تاب‌آوری سازمان را فراهم می‌سازد. این سه ویژگی سبب می‌شود چارچوب پیشنهادی علاوه بر سازمان‌های تجاری، برای بانک‌ها، شرکت‌های زیرساختی، سازمان‌های دولتی و ارائه‌دهندگان خدمات حیاتی نیز قابل استفاده باشد.

شکل ۲. چارچوب پیشنهادی حاکمیت تاب‌آوری سایبری سازمانی مبتنی بر هوش مصنوعی و مدیریت ریسک

فرضیه‌های پژوهش

با توجه به مدل مفهومی پژوهش و مبانی نظری ارائه‌شده، فرضیه‌های زیر تدوین می‌شوند:

فرضیه ۱. حاکمیت شرکتی اثر مثبت و معناداری بر استقرار حاکمیت سایبری در سازمان دارد.

فرضیه ۲. حاکمیت سایبری اثر مثبت و معناداری بر اثربخشی مدیریت ریسک سایبری دارد.

فرضیه ۳. مدیریت ریسک سایبری اثر مثبت و معناداری بر به‌کارگیری هوش مصنوعی در تصمیم‌گیری‌های امنیتی دارد.

فرضیه ٤. به‌کارگیری هوش مصنوعی اثر مثبت و معناداری بر افزایش تاب‌آوری سایبری سازمان دارد.

فرضیه ۵. مدیریت ریسک سایبری به‌صورت مستقیم بر تاب‌آوری سایبری سازمان اثر مثبت و معناداری دارد.

فرضیه ٦. هوش مصنوعی نقش میانجی در رابطه بین مدیریت ریسک سایبری و تاب‌آوری سایبری سازمان ایفا می‌کند.

فرضیه ۷. حاکمیت سایبری نقش میانجی در رابطه بین حاکمیت شرکتی و مدیریت ریسک سایبری ایفا می‌کند.

بر اساس مبانی نظری و چارچوب مفهومی ارائه‌شده، پژوهش حاضر استدلال می‌کند که دستیابی به تاب‌آوری سایبری پایدار صرفاً از طریق استقرار کنترل‌های امنیتی امکان‌پذیر نیست، بلکه مستلزم یکپارچه‌سازی حاکمیت شرکتی، مدیریت ریسک و هوش مصنوعی در قالب یک نظام تصمیم‌گیری هوشمند است. چارچوب پیشنهادی با ایجاد پیوند میان این مؤلفه‌ها، نه‌تنها قابلیت پیش‌بینی و پاسخ‌گویی به تهدیدهای سایبری را ارتقا می‌دهد، بلکه از طریق چرخه بازخورد و یادگیری مستمر، زمینه بهبود مستمر تاب‌آوری سازمان را نیز فراهم می‌سازد.

روش‌شناسی پژوهش

پژوهش حاضر از نظر هدف، کاربردی و از نظر شیوه اجرا، آمیخته اکتشافی است. در این رویکرد، ابتدا با بهره‌گیری از مطالعات کتابخانه‌ای، مرور نظام‌مند ادبیات و اخذ نظر خبرگان، چارچوب حاکمیت تاب‌آوری سایبری سازمانی مبتنی بر هوش مصنوعی و مدیریت ریسک طراحی شد و سپس در مرحله کمی، اعتبار و روابط میان مؤلفه‌های چارچوب از طریق مدل‌یابی معادلات ساختاری مورد ارزیابی قرار گرفت.

استفاده از روش آمیخته به این دلیل انتخاب شد که طراحی یک چارچوب مفهومی، علاوه بر پشتوانه نظری، نیازمند بهره‌گیری از تجربیات متخصصان و ارزیابی تجربی روابط میان سازه‌ها است. این رویکرد در پژوهش‌های طراحی مدل و چارچوب‌های مدیریتی به‌طور گسترده مورد استفاده قرار گرفته و امکان افزایش اعتبار علمی یافته‌ها را فراهم می‌کند (کرسول و پلانو کلارک، ۲۰۲۱: ۲۰).

مرحله کیفی پژوهش

در بخش کیفی، ابتدا مرور نظام‌مند منابع علمی منتشرشده بین سال‌های ۲۰۲۰ تا ۲۰۲۵ انجام شد. منابع مورد بررسی شامل مقالات نمایه‌شده در پایگاه‌های اسکوپوس[1]، وب آو ساینس[2]، آی‌تریپل‌ایکسپلور[3]، اشپرینگر[4]، ساینس‌دایرکت[5] و کتابخانه دیجیتال ای‌سی‌ام[6] بودند. همچنین استانداردها و چارچوب‌های معتبر بین‌المللی شامل چارچوب امنیت سایبری مؤسسه ملی استانداردها و فناوری ۲.۰، چارچوب مدیریت ریسک هوش مصنوعی مؤسسه ملی استانداردها و فناوری، اهداف حاکمیت و مدیریت فناوری اطلاعات ۲۰۱۹، استاندارد ایزو/آی‌ای‌سی ۲۷۰۰۱:۲۰۲۲، استاندارد ایزو ۳۱۰۰۰ و مدیریت ریسک سازمانی کمیته سازمان‌های حامی کمیسیون تردوی نیز تحلیل شدند.

پس از استخراج مؤلفه‌های اولیه، چارچوب پیشنهادی با استفاده از روش دلفی مورد ارزیابی قرار گرفت. جامعه خبرگان شامل استادان دانشگاه در حوزه امنیت اطلاعات، مدیران ارشد فناوری اطلاعات، مدیران امنیت اطلاعات، متخصصان مدیریت ریسک و مشاوران حاکمیت فناوری اطلاعات بود.

نمونه‌گیری در این مرحله به‌صورت هدفمند انجام شد و تعداد ۱۸ نفر از خبرگان که حداقل دارای مدرک کارشناسی ارشد، بیش از ده سال سابقه حرفه‌ای و تجربه عملی در حوزه امنیت سایبری یا مدیریت ریسک بودند، در پژوهش مشارکت کردند.

فرآیند دلفی طی سه دور انجام شد. در دور نخست، خبرگان درباره مؤلفه‌های پیشنهادی اظهار نظر کردند. در دور دوم، پیشنهادهای اصلاحی بررسی و چارچوب بازنگری شد. در دور سوم، میزان

[1] Scopus
[2] Web of Science
[3] IEEE Xplore
[4] Springer
[5] ScienceDirect
[6] ACM Digital Library

توافق خبرگان درباره هر مؤلفه اندازه‌گیری شد و تنها مؤلفه‌هایی که میانگین امتیاز آن‌ها بیش از ۴ از ۵ بود در مدل نهایی باقی ماندند.

مرحله کمی پژوهش

در مرحله کمی، مدل مفهومی استخراج‌شده از مرحله کیفی از طریق پرسشنامه استاندارد محقق‌ساخته مورد ارزیابی قرار گرفت.

جامعه آماری شامل مدیران فناوری اطلاعات، مدیران امنیت اطلاعات، مدیران ریسک، کارشناسان امنیت سایبری و مدیران تحول دیجیتال سازمان‌های بزرگ، بانک‌ها، شرکت‌های بیمه، اپراتورهای مخابراتی و سازمان‌های دولتی ایران بود.

با توجه به تعداد متغیرهای پژوهش و استفاده از مدل‌یابی معادلات ساختاری، حجم نمونه بر اساس روش هیر و همکاران[1] در سال ۱۴۰۳ حداقل ۲۰۰ نفر تعیین شد. در نهایت ۲۲۸ پرسشنامه جمع‌آوری شد که پس از حذف پرسشنامه‌های ناقص، ۲۱۲ پرسشنامه برای تحلیل نهایی مورد استفاده قرار گرفت.

نمونه‌گیری به روش در دسترس همراه با قضاوتی انجام شد؛ زیرا جامعه متخصصان امنیت سایبری جامعه‌ای تخصصی و محدود است.

جدول ۲

مقایسه مشخصات جامعه آماری و نمونه پژوهش

مرحله پژوهش	جامعه آماری	روش نمونه‌گیری	حجم نمونه
کیفی	خبرگان امنیت سایبری، مدیریت ریسک و حاکمیت فناوری اطلاعات	هدفمند	۱۸ نفر
کمی	مدیران و کارشناسان امنیت اطلاعات، فناوری اطلاعات و مدیریت ریسک	در دسترس و قضاوتی	۲۱۲ نفر

[1] Hair et al

ابزار گردآوری داده‌ها

در مرحله کیفی، ابزار گردآوری اطلاعات شامل چک‌لیست استخراج مفاهیم از ادبیات پژوهش و پرسشنامه دلفی بود.

در مرحله کمی، پرسشنامه‌ای محقق‌ساخته بر اساس مؤلفه‌های استخراج‌شده طراحی شد. پرسشنامه شامل دو بخش بود:

- اطلاعات جمعیت‌شناختی پاسخ‌دهندگان
- گویه‌های مربوط به سازه‌های پژوهش

پاسخ‌ها بر اساس طیف پنج‌درجه‌ای لیکرت از «کاملاً مخالفم» تا «کاملاً موافقم» اندازه‌گیری شدند.

سازه‌های اصلی پرسشنامه عبارت بودند از:

- حاکمیت شرکتی
- حاکمیت سایبری
- مدیریت ریسک سایبری
- هوش مصنوعی
- تاب‌آوری سایبری

در مجموع ۳۴ گویه برای اندازه‌گیری متغیرهای پژوهش طراحی شد.

روایی و پایایی ابزار پژوهش

برای ارزیابی روایی محتوا، پرسشنامه در اختیار خبرگان قرار گرفت و پس از اعمال اصلاحات لازم، نسخه نهایی تهیه شد.

در مرحله کمی، روایی همگرا با استفاده از میانگین واریانس استخراج‌شده[1] و روایی واگرا با معیار فورنل و لارکر و نسبت هتروتریت ـ مونوتریت[2] بررسی شد.

پایایی ابزار نیز از طریق شاخص‌های زیر اندازه‌گیری شد:

- آلفای کرونباخ
- پایایی ترکیبی

[1] Average Variance Extracted (AVE)
[2] Heterotrait–Monotrait Ratio (HTMT)

- شاخص rho_A

مطابق معیارهای هیر و همکاران، مقادیر آلفای کرونباخ و پایایی ترکیبی بزرگ‌تر از ۰/۷ و مقدار میانگین بزرگ‌تر از ۰/۵ نشان‌دهنده مطلوب بودن ابزار اندازه‌گیری است.

روش تجزیه و تحلیل داده‌ها

داده‌های جمع‌آوری‌شده در دو سطح توصیفی و استنباطی تحلیل شدند.

در بخش توصیفی از شاخص‌هایی مانند فراوانی، درصد، میانگین و انحراف معیار استفاده شد.

در بخش استنباطی، برای آزمون مدل مفهومی پژوهش از مدل‌یابی معادلات ساختاری مبتنی بر حداقل مربعات جزئی[1] استفاده شد.

تحلیل مدل در دو مرحله انجام شد:

۱. ارزیابی مدل اندازه‌گیری شامل:

- پایایی
- روایی همگرا
- روایی واگرا

۲. ارزیابی مدل ساختاری شامل:

- ضرایب مسیر
- آماره t
- مقدار p
- ضریب تعیین (R^2)
- اندازه اثر (f^2)
- شاخص پیش‌بینی (Q^2)

برای تحلیل داده‌ها از نرم‌افزارهای اس‌پی‌اس‌اس[2] نسخه ۲۷ و نرم‌افزار اسمارت‌پی‌ال‌اس[3] نسخه ۴ استفاده شد.

---

[1] Partial Least Squares Structural Equation Modeling
[2] SPSS
[3] SmartPLS

متغیرهای پژوهش و تعریف عملیاتی آن‌ها

در پژوهش حاضر، تاب‌آوری سایبری سازمانی به‌عنوان متغیر وابسته در نظر گرفته شد و میزان توانایی سازمان در پیش‌بینی، مقاومت، پاسخ، بازیابی و یادگیری از رخدادهای سایبری را اندازه‌گیری می‌کند.

هوش مصنوعی و مدیریت ریسک سایبری به‌عنوان متغیرهای مستقل اصلی تعریف شدند و میزان استفاده سازمان از فناوری‌های هوشمند در شناسایی تهدیدها، تحلیل ریسک و تصمیم‌گیری امنیتی را می‌سنجند.

حاکمیت شرکتی و حاکمیت سایبری نیز به‌عنوان سازه‌های راهبردی مدل در نظر گرفته شدند که نقش آن‌ها در ایجاد ساختارهای تصمیم‌گیری، سیاست‌گذاری و نظارت بر امنیت سایبری ارزیابی می‌شود.

یافته‌های پژوهش

استخراج و پالایش مؤلفه‌های چارچوب پیشنهادی

در مرحله نخست پژوهش، با مرور نظام‌مند منابع علمی منتشرشده بین سال‌های ۲۰۲۰ تا ۲۰۲۵ و تحلیل چارچوب‌های معتبر بین‌المللی شامل چارچوب امنیت سایبری مؤسسه ملی استانداردها و فناوری ۲.۰، چارچوب مدیریت ریسک هوش مصنوعی مؤسسه ملی استانداردها و فناوری، اهداف حاکمیت و مدیریت فناوری اطلاعات ۲۰۱۹، استاندارد ایزو/آی‌ای‌سی ۲۷۰۰۱:۲۰۲۲، استاندارد ایزو ۳۱۰۰۰ و مدیریت ریسک سازمانی کمیته سازمان‌های حامی کمیسیون تردوی، مجموعه‌ای از مؤلفه‌های اولیه مرتبط با حاکمیت تاب‌آوری سایبری استخراج شد. این مؤلفه‌ها پس از حذف موارد تکراری و ادغام مفاهیم مشابه، در قالب پنج بُعد اصلی و بیست‌ویک مؤلفه فرعی سازمان‌دهی شدند.

در ادامه، مؤلفه‌های استخراج‌شده در اختیار خبرگان قرار گرفت و طی سه دور اجرای روش دلفی، میزان اهمیت، شفافیت مفهومی، قابلیت اجرا و ارتباط هر مؤلفه با هدف پژوهش ارزیابی شد. نتایج این مرحله نشان داد که تمامی ابعاد اصلی چارچوب از نظر خبرگان دارای اهمیت بالا بوده و میانگین امتیاز آن‌ها از حد آستانه تعیین‌شده فراتر است. همچنین برخی مؤلفه‌ها با نظر خبرگان ادغام یا بازتعریف شدند تا از همپوشانی مفهومی جلوگیری شود.

فرآیند پالایش نشان داد که تاب‌آوری سایبری تنها حاصل استقرار کنترل‌های امنیتی نیست، بلکه پیامد تعامل نظام‌مند میان ساختارهای حاکمیتی، فرآیندهای مدیریت ریسک، فناوری‌های هوش مصنوعی و سازوکارهای یادگیری سازمانی است. این یافته با نتایج پژوهش‌های اخیر در حوزه حاکمیت سایبری و مدیریت ریسک همسو است که بر ضرورت نگاه فرابخشی به امنیت سایبری تأکید دارند.

ابعاد اصلی چارچوب حاکمیت تاب‌آوری سایبری

بر اساس تحلیل داده‌های کیفی، چارچوب پیشنهادی از پنج بُعد اصلی تشکیل شده است که هر یک نقش مشخصی در ارتقای تاب‌آوری سایبری سازمان ایفا می‌کنند.

حاکمیت شرکتی به‌عنوان لایه راهبردی، مسئول تعیین سیاست‌های کلان، میزان ریسک‌پذیری، تخصیص منابع و نظارت بر عملکرد امنیت سایبری است. در این سطح، هیئت‌مدیره و کمیته‌های تخصصی مسئولیت اصلی هدایت و پایش ریسک‌های سایبری را بر عهده دارند.

حاکمیت سایبری لایه‌ای است که سیاست‌های کلان را به فرآیندهای اجرایی تبدیل می‌کند. این بُعد شامل مدیریت کنترل‌های امنیتی، پایش انطباق، مدیریت دارایی‌های اطلاعاتی، تعیین مسئولیت‌ها و نظارت بر اجرای الزامات امنیتی است.

مدیریت ریسک سایبری هسته تصمیم‌گیری چارچوب محسوب می‌شود. در این بخش، دارایی‌های حیاتی، تهدیدها، آسیب‌پذیری‌ها و پیامدهای بالقوه شناسایی و ارزیابی شده و اولویت اقدامات امنیتی مشخص می‌شود.

هوش مصنوعی نقش تصمیم‌یار را در چارچوب پیشنهادی ایفا می‌کند. سامانه‌های هوشمند با تحلیل داده‌های امنیتی، شناسایی الگوهای غیرعادی، پیش‌بینی حملات، اولویت‌بندی هشدارها و ارائه پیشنهادهای تصمیم‌گیری، سرعت و دقت مدیریت ریسک را افزایش می‌دهند.

در نهایت، یادگیری مستمر و بهبود مداوم به‌عنوان مؤلفه‌ای میان‌بخشی، نتایج حاصل از رخدادهای امنیتی، تحلیل‌های هوش مصنوعی و بازخوردهای مدیریتی را به چرخه حاکمیت بازمی‌گرداند تا سیاست‌ها، کنترل‌ها و مدل‌های تحلیلی به‌صورت مستمر بهبود یابند.

جدول ۳

ابعاد و مؤلفه‌های چارچوب پیشنهادی حاکمیت تاب‌آوری سایبری

بُعد اصلی	مؤلفه‌های کلیدی	نقش در چارچوب
حاکمیت شرکتی	سیاست‌گذاری، راهبری، نظارت، تعیین ریسک‌پذیری	تعیین جهت‌گیری راهبردی
حاکمیت سایبری	مدیریت کنترل‌ها، انطباق، تخصیص مسئولیت، پایش	اجرای سیاست‌های امنیتی
مدیریت ریسک سایبری	شناسایی، تحلیل، ارزیابی، پاسخ و پایش ریسک	اولویت‌بندی تصمیمات امنیتی
هوش مصنوعی	تحلیل داده، پیش‌بینی تهدید، تشخیص ناهنجاری، تصمیم‌یار	افزایش دقت و سرعت تصمیم‌گیری
یادگیری مستمر	بازخورد، بهبود کنترل‌ها، آموزش مدل‌ها، بازنگری سیاست‌ها	ارتقای مستمر تاب‌آوری

تحلیل تعامل میان ابعاد چارچوب

تحلیل خبرگان نشان داد که اثربخشی هر یک از ابعاد چارچوب وابسته به تعامل آن با سایر ابعاد است و هیچ‌یک از آن‌ها به‌تنهایی قادر به ایجاد تاب‌آوری سایبری پایدار نیست. برای مثال، استقرار سامانه‌های هوش مصنوعی بدون وجود سیاست‌های حاکمیتی و فرآیندهای نظام‌مند مدیریت ریسک، ممکن است به تصمیم‌های غیرشفاف یا ناهماهنگ منجر شود. همچنین مدیریت ریسک بدون بهره‌گیری از تحلیل‌های هوشمند، در مواجهه با حجم بالای داده‌های امنیتی و تهدیدهای پیچیده، کارایی لازم را نخواهد داشت.

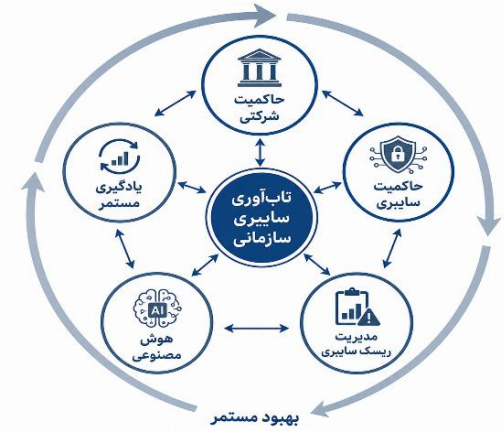
از سوی دیگر، خبرگان تأکید کردند که نقش هیئت‌مدیره در تعیین ریسک‌پذیری سازمان، تخصیص منابع و نظارت بر اجرای سیاست‌های امنیتی، عامل کلیدی موفقیت چارچوب است. این یافته با توصیه‌های سازمان همکاری و توسعه اقتصادی، انجمن حسابرسی و کنترل سامانه‌های اطلاعاتی و مؤسسه ملی استانداردها و فناوری ایالات متحده مبنی بر ضرورت مشارکت فعال هیئت‌مدیره در حاکمیت سایبری همخوانی دارد.

همچنین، به‌کارگیری هوش مصنوعی در چارچوب پیشنهادی صرفاً به اتوماسیون فرآیندها محدود نیست، بلکه به‌عنوان ابزاری برای ارتقای کیفیت تصمیم‌گیری مدیریتی، کاهش زمان کشف تهدید، افزایش دقت ارزیابی ریسک و تسهیل یادگیری سازمانی در نظر گرفته شده است. این موضوع یکی از وجوه تمایز چارچوب حاضر نسبت به بسیاری از مدل‌های موجود است که هوش مصنوعی را صرفاً در سطح عملیاتی بررسی کرده‌اند.

تبیین نوآوری چارچوب پیشنهادی

یافته‌های پژوهش نشان می‌دهد که نوآوری اصلی چارچوب پیشنهادی در یکپارچه‌سازی چهار حوزه راهبردی شامل حاکمیت شرکتی، حاکمیت سایبری، مدیریت ریسک و هوش مصنوعی در قالب یک چرخه یادگیرنده است. در این چارچوب، اطلاعات حاصل از پایش امنیتی و تحلیل‌های هوشمند، به‌صورت مستمر به فرآیندهای مدیریت ریسک و سطوح حاکمیتی بازخورد داده می‌شود و مبنای اصلاح سیاست‌ها و تصمیمات آینده قرار می‌گیرد.

این چرخه یادگیری موجب می‌شود که سازمان در برابر تغییرات محیط تهدید، فناوری‌های نوظهور و الگوهای جدید حملات، توان انطباق و بازآرایی خود را حفظ کند. به همین دلیل، چارچوب پیشنهادی تنها یک مدل مدیریتی نیست، بلکه یک سامانه حاکمیتی پویا برای ارتقای تاب‌آوری سایبری محسوب می‌شود.



شکل ۳. چرخه تعامل مؤلفه‌های چارچوب حاکمیت تاب‌آوری سایبری سازمانی

ارزیابی مدل اندازه‌گیری

پس از نهایی‌شدن چارچوب در مرحله کیفی و دلفی، مدل اندازه‌گیری با استفاده از روش حداقل مربعات جزئی ارزیابی شد. در این مرحله، پایایی سازه‌ها با استفاده از آلفای کرونباخ، rho_Aو پایایی ترکیبی و روایی همگرا با استفاده از میانگین واریانس استخراج‌شده بررسی شد. نتایج نشان داد که مقادیر شاخص‌های پایایی برای تمامی سازه‌ها در محدوده قابل قبول قرار دارد و مقادیر میانگین واریانس استخراج‌شده نیز از حداقل معیار قابل قبول ۵۰/۰ بالاتر است. بنابراین، سازه‌های مورد استفاده از پایایی درونی و روایی همگرای مطلوب برخوردارند.

جدول ٤

نتایج ارزیابی پایایی و روایی همگرای سازه‌ها

سازه	تعداد گویه	آلفای کرونباخ	rho_A	پایایی ترکیبی (CR)	AVE
حاکمیت شرکتی	۷	۰/۸۹۲	۰/۸۹۶	۰/۹۱۵	۰/۶۰۵
حاکمیت سایبری	۷	۰/۸۸۴	۰/۸۸۹	۰/۹۱۰	۰/۵۹۳
مدیریت ریسک سایبری	۷	۰/۹۰۱	۰/۹۰۵	۰/۹۲۲	۰/۶۲۹
هوش مصنوعی	۶	۰/۸۷۶	۰/۸۸۲	۰/۹۰۷	۰/۶۱۹
تاب‌آوری سایبری	۷	۰/۹۱۳	۰/۹۱۶	۰/۹۳۰	۰/۶۵۲

همان‌گونه که در جدول ۴ مشاهده می‌شود، مقدار آلفای کرونباخ سازه‌ها بین ۰/۸۷۶ و ۰/۹۱۳، مقدار rho_A بین ۰/۸۸۲ و ۰/۹۱۶ و مقدار پایایی ترکیبی بین ۰/۹۰۷ و ۰/۹۳۰ قرار دارد. همچنین مقدار میانگین واریانس استخراج‌شده تمامی سازه‌ها بیش از ۰/۵۰ است. بنابراین، پایایی درونی و روایی همگرای مدل اندازه‌گیری در سطح مطلوب ارزیابی می‌شود.

ارزیابی روایی واگرا

برای بررسی تمایز سازه‌های مدل از یکدیگر، روایی واگرا با استفاده از معیار فورنل–لارکر و نسبت هتروتریت – مونوتریت ارزیابی شد. نتایج نشان داد که جذر میانگین واریانس استخراج‌شده هر سازه از همبستگی آن سازه با سایر سازه‌ها بیشتر بوده و مقادیر هتروتریت –

مونوتریت نیز در محدوده قابل قبول قرار دارند. بنابراین، سازه‌های مدل از تمایز مفهومی و آماری مناسبی برخوردارند.

جدول ۵

نتایج معیار فورنل–لارکر

سازه	حاکمیت شرکتی	حاکمیت سایبری	مدیریت ریسک سایبری	هوش مصنوعی	تاب‌آوری سایبری
حاکمیت شرکتی	۰/۷۷۸	۰/۶۲۴	۰/۵۸۱	۰/۵۴۸	۰/۵۳۲
حاکمیت سایبری	۰/۶۲۴	۰/۷۷۰	۰/۶۷۱	۰/۶۰۲	۰/۵۸۷
مدیریت ریسک سایبری	۰/۵۸۱	۰/۶۷۱	۰/۷۹۳	۰/۷۸۷	۰/۷۱۱
هوش مصنوعی	۰/۵۴۸	۰/۶۰۲	۰/۶۴۸	۰/۷۸۷	۰/۷۱۱
تاب‌آوری سایبری	۰/۵۳۲	۰/۵۸۷	۰/۶۹۲	۰/۷۱۱	۰/۸۰۸

مقادیر قطری جدول نشان‌دهنده جذر میانگین واریانس استخراج‌شده هستند. همان‌طور که مشاهده می‌شود، مقدار جذر میانگین واریانس استخراج‌شده هر سازه از ضرایب همبستگی آن با سایر سازه‌ها بیشتر است؛ بنابراین شرط فورنل–لارکر برقرار است.

جدول ٦

نتایج آزمون هتروتریت ـ مونوتریت

رابطه سازه‌ها	هتروتریت ـ مونوتریت
حاکمیت شرکتی – حاکمیت سایبری	۰/۷۰۶
حاکمیت شرکتی – مدیریت ریسک سایبری	۰/۶۵۸
حاکمیت شرکتی – هوش مصنوعی	۰/۶۲۱
حاکمیت شرکتی – تاب‌آوری سایبری	۰/۶۰۳
حاکمیت سایبری – مدیریت ریسک سایبری	۰/۷۵۲
حاکمیت سایبری – هوش مصنوعی	۰/۶۹۱
حاکمیت سایبری – تاب‌آوری سایبری	۰/۶۷۴
مدیریت ریسک سایبری – هوش مصنوعی	۰/۷۳۱
مدیریت ریسک سایبری – تاب‌آوری سایبری	۰/۷۸۴
هوش مصنوعی – تاب‌آوری سایبری	۰/۸۱۲

بیشترین مقدار نسبت هتروتریت - مونوتریت مربوط به رابطه هوش مصنوعی و تاب‌آوری سایبری و برابر با ۰/۸۱۲ است که در محدوده قابل قبول قرار دارد. بنابراین، نتایج دو آزمون فورنل–لارکر و نسبت هتروتریت - مونوتریت ، روایی واگرای مدل اندازه‌گیری را تأیید می‌کنند.

ارزیابی مدل ساختاری و آزمون فرضیه‌ها

پس از تأیید مدل اندازه‌گیری، مدل ساختاری پژوهش مورد ارزیابی قرار گرفت. برای بررسی معناداری روابط، از ضرایب مسیر، آماره t و مقدار p استفاده شد. نتایج نشان داد که تمامی مسیرهای مستقیم پیشنهادی دارای اثر مثبت و معنادار هستند. همچنین، اثرهای غیرمستقیم مربوط به فرضیه‌های میانجی نیز مورد بررسی قرار گرفت.

جدول ۷

نتایج آزمون فرضیه‌های پژوهش

فرضیه	مسیر	β	t	p	نتیجه
H1	حاکمیت شرکتی ← حاکمیت سایبری	۰/۶۲۴	۱۰/۸۴۷	<۰/۰۰۱	تأیید
H2	حاکمیت سایبری ← مدیریت ریسک سایبری	۰/۶۷۱	۱۳/۱۲۶	<۰/۰۰۱	تأیید
H3	مدیریت ریسک سایبری ← هوش مصنوعی	۰/۶۴۸	۱۱/۹۳۲	<۰/۰۰۱	تأیید
H4	هوش مصنوعی ← تاب‌آوری سایبری	۰/۵۶۳	۹/۶۸۴	<۰/۰۰۱	تأیید
H5	مدیریت ریسک سایبری ← تاب‌آوری سایبری	۰/۳۲۸	۵/۴۱۷	<۰/۰۰۱	تأیید
H6	مدیریت ریسک سایبری ← هوش مصنوعی ← تاب‌آوری سایبری	۰/۳۶۵	۷/۱۲۶	<۰/۰۰۱	تأیید
H7	حاکمیت شرکتی ← حاکمیت سایبری ← مدیریت ریسک سایبری	۰/۴۱۹	۸/۵۰۳	<۰/۰۰۱	تأیید

نتایج جدول ۷ نشان می‌دهد که حاکمیت شرکتی تأثیر مثبت و معناداری بر حاکمیت سایبری دارد (ضریب مسیر: ۰/۶۲۴؛ آماره تی: ۱۰/۸۴۷؛ سطح معناداری: کمتر از ۰/۰۰۱). همچنین، حاکمیت سایبری تأثیر مثبت و معناداری بر مدیریت ریسک سایبری دارد (ضریب مسیر: ۰/۶۷۱؛ آماره تی: ۱۳/۱۲۶؛ سطح معناداری: کمتر از ۰/۰۰۱). تأثیر مدیریت ریسک سایبری بر به‌کارگیری هوش مصنوعی نیز مثبت و معنادار است (ضریب مسیر: ۰/۶۴۸؛ آماره تی: ۱۱/۹۳۲؛ سطح معناداری: کمتر از ۰/۰۰۱). افزون بر این، به‌کارگیری هوش مصنوعی تأثیر مثبت و معناداری بر تاب‌آوری سایبری دارد (ضریب مسیر: ۰/۵۶۳؛ آماره تی: ۹/۶۸۴؛ سطح معناداری: کمتر از ۰/۰۰۱). اثر مستقیم مدیریت ریسک سایبری بر تاب‌آوری سایبری نیز مثبت و معنادار است (ضریب مسیر: ۰/۳۲۸؛ آماره تی: ۵/۴۱۷؛ سطح معناداری: کمتر از ۰/۰۰۱).

بررسی اثرهای غیرمستقیم نشان می‌دهد که به‌کارگیری هوش مصنوعی در رابطه میان مدیریت ریسک سایبری و تاب‌آوری سایبری نقش میانجی معناداری دارد (ضریب اثر غیرمستقیم: ۰/۳۶۵؛ آماره تی: ۷/۱۲۶؛ سطح معناداری: کمتر از ۰/۰۰۱). همچنین، نقش میانجی حاکمیت سایبری در رابطه میان حاکمیت شرکتی و مدیریت ریسک سایبری معنادار است

(ضریب اثر غیرمستقیم: ۰/۴۱۹؛ آماره تی: ۸/۵۰۳؛ سطح معناداری: کمتر از ۰/۰۰۱). بر اساس نتایج گزارش‌شده، هر هفت فرضیه پژوهش تأیید شدند.

قدرت تبیین مدل

برای ارزیابی قدرت تبیین مدل ساختاری، ضریب تعیین (R^2) برای سازه‌های درون‌زا محاسبه شد. نتایج نشان می‌دهد که مدل پیشنهادی بخش قابل توجهی از تغییرات سازه‌های درون‌زا را تبیین می‌کند.

جدول ۸

شاخص‌های قدرت تبیین مدل ساختاری پژوهش

سازه درون‌زا	R^2	R^2 تعدیل‌شده
حاکمیت سایبری	۰/۳۹۰	۰/۳۸۷
مدیریت ریسک سایبری	۰/۴۵۰	۰/۴۴۷
هوش مصنوعی	۰/۴۲۰	۰/۴۱۷
تاب‌آوری سایبری	۰/۶۷۲	۰/۶۶۹

بیشترین قدرت تبیین مدل مربوط به سازه تاب‌آوری سایبری است که ضریب تعیین آن برابر با ۰/۶۷۲ به دست آمد؛ بنابراین، متغیرهای پیش‌بین این سازه در مدل، ۶۷/۲ درصد از واریانس آن را تبیین می‌کنند. همچنین، ضرایب تعیین حاکمیت سایبری، مدیریت ریسک سایبری و هوش مصنوعی به‌ترتیب برابر با ۰/۳۹۰، ۰/۴۵۰ و ۰/۴۲۰ است؛ به این معنا که متغیرهای پیش‌بین هر یک از این سازه‌ها، به‌ترتیب ۳۹، ۴۵ و ۴۲ درصد از واریانس آن‌ها را تبیین می‌کنند. ضرایب تعیین تعدیل‌شده نیز برای حاکمیت سایبری، مدیریت ریسک سایبری، هوش مصنوعی و تاب‌آوری سایبری به‌ترتیب برابر با ۰/۳۸۷، ۰/۴۴۷، ۰/۴۱۷ و ۰/۶۶۹ به دست آمد.

اندازه اثر و قدرت پیش‌بینی

در ادامه، اندازه اثر روابط با استفاده از شاخص f^2 و قدرت پیش‌بینی مدل با استفاده از شاخص Q^2 بررسی شد. نتایج نشان داد که مسیرهای اصلی مدل دارای اندازه اثر قابل قبول بوده و مقادیر Q^2 برای سازه‌های درون‌زا مثبت است؛ بنابراین، مدل علاوه بر قدرت تبیین، از قدرت پیش‌بینی قابل قبول نیز برخوردار است.

جدول ۹

شاخص‌های قدرت پیش‌بینی مدل ساختاری پژوهش

سازه درون‌زا	Q^2
حاکمیت سایبری	۰/۳۵۲
مدیریت ریسک سایبری	۰/۴۰۱
هوش مصنوعی	۰/۳۶۸
تاب‌آوری سایبری	۰/۵۱۷

و:

جدول ۱۰

اندازه اثر مسیرهای مدل ساختاری پژوهش

مسیر	f^2
حاکمیت شرکتی ← حاکمیت سایبری	۰/۶۳۷
حاکمیت سایبری ← مدیریت ریسک سایبری	۰/۸۱۸
مدیریت ریسک سایبری ← هوش مصنوعی	۰/۷۲۱
هوش مصنوعی ← تاب‌آوری سایبری	۰/۳۹۸
مدیریت ریسک سایبری ← تاب‌آوری سایبری	۰/۱۲۶

بحث و نتیجه‌گیری

تحول دیجیتال، گسترش زیرساخت‌های مبتنی بر فناوری اطلاعات و افزایش وابستگی سازمان‌ها به خدمات دیجیتال، موجب شده است که امنیت سایبری از یک مسئله صرفاً فنی به یکی از مهم‌ترین موضوعات راهبردی در حاکمیت سازمانی تبدیل شود. در چنین شرایطی،

سازمان‌ها علاوه بر حفاظت از دارایی‌های اطلاعاتی، باید توانایی حفظ تداوم فعالیت، پاسخ‌گویی مؤثر به رخدادهای سایبری و بازگشت سریع به وضعیت عادی را نیز داشته باشند. از این رو، مفهوم تاب‌آوری سایبری طی سال‌های اخیر به یکی از ارکان اصلی مدیریت ریسک سازمانی تبدیل شده است.

هدف اصلی پژوهش حاضر، طراحی چارچوبی جامع برای حاکمیت تاب‌آوری سایبری سازمانی مبتنی بر هوش مصنوعی و مدیریت ریسک بود. بر اساس مرور نظام‌مند ادبیات، تحلیل استانداردهای بین‌المللی و تلفیق دیدگاه‌های خبرگان، چارچوبی پنج‌بعدی شامل حاکمیت شرکتی، حاکمیت سایبری، مدیریت ریسک سایبری، هوش مصنوعی و یادگیری مستمر ارائه شد. این چارچوب با ایجاد ارتباط میان لایه‌های راهبردی، مدیریتی و عملیاتی، زمینه ارتقای توان سازمان در پیش‌بینی، پیشگیری، تشخیص، پاسخ، بازیابی و انطباق با تهدیدهای سایبری را فراهم می‌کند.

یافته‌های پژوهش نشان داد که حاکمیت شرکتی نقطه آغاز شکل‌گیری تاب‌آوری سایبری است. بدون مشارکت فعال هیئت‌مدیره، تعیین سطح ریسک‌پذیری، تصویب سیاست‌های امنیتی و تخصیص منابع، ایجاد سازوکارهای پایدار مدیریت ریسک و امنیت سایبری امکان‌پذیر نخواهد بود. این نتیجه با گزارش‌های سازمان همکاری و توسعه اقتصادی و چارچوب کوبیت ۲۰۱۹ همسو است که بر مسئولیت مستقیم هیئت‌مدیره در مدیریت ریسک‌های سایبری تأکید می‌کنند. همچنین یافته‌های پژوهش حاضر نشان می‌دهد که حاکمیت سایبری باید به‌عنوان حلقه واسط میان سیاست‌های کلان و فرآیندهای اجرایی عمل کند و از طریق نظارت مستمر، ارزیابی انطباق و مدیریت کنترل‌ها، تحقق اهداف امنیتی سازمان را تضمین نماید.

یکی دیگر از یافته‌های مهم پژوهش، نقش محوری مدیریت ریسک سایبری در چارچوب پیشنهادی است. برخلاف رویکردهای سنتی که مدیریت ریسک را فرآیندی دوره‌ای و عمدتاً مبتنی بر ارزیابی‌های دستی می‌دانند، چارچوب حاضر بر مدیریت ریسک پویا و داده‌محور تأکید دارد. در این رویکرد، اطلاعات حاصل از سامانه‌های پایش امنیتی، تحلیل‌های هوشمند و بازخوردهای عملیاتی به‌صورت مستمر در فرآیند ارزیابی ریسک وارد شده و موجب به‌روزرسانی اولویت‌های امنیتی سازمان می‌شود. این نتیجه با یافته‌های پژوهش‌های کور و

همکاران و شارما و همکاران همخوانی دارد که مدیریت ریسک پویا را یکی از پیش‌نیازهای تاب‌آوری سایبری معرفی کرده‌اند.

پژوهش حاضر همچنین نشان داد که هوش مصنوعی تنها یک ابزار فناورانه برای تشخیص نفوذ یا تحلیل داده نیست، بلکه می‌تواند به‌عنوان یک سامانه تصمیم‌یار مدیریتی در تمام مراحل چرخه مدیریت ریسک ایفای نقش کند. به‌کارگیری الگوریتم‌های یادگیری ماشین، تحلیل رفتار، کشف ناهنجاری، پیش‌بینی تهدید و اولویت‌بندی هشدارها، امکان تصمیم‌گیری سریع‌تر و دقیق‌تر را برای مدیران فراهم می‌کند. علاوه بر این، استفاده از تحلیل‌های هوشمند موجب کاهش زمان کشف حملات، بهبود کیفیت ارزیابی ریسک و افزایش سرعت پاسخ‌گویی به رخدادهای امنیتی می‌شود. این یافته با چارچوب چارچوب مدیریت ریسک هوش مصنوعی مؤسسه ملی استانداردها و فناوری و گزارش‌های اخیر آژانس اتحادیه اروپا برای امنیت سایبری در سال ۱۴۰۳ و مایکروسافت در سال ۱۴۰۴ مبنی بر نقش هوش مصنوعی در ارتقای امنیت سایبری سازگار است.

از مهم‌ترین نوآوری‌های چارچوب پیشنهادی، ایجاد چرخه یادگیری مستمر میان تمامی ابعاد مدل است. در بسیاری از چارچوب‌های موجود، فرآیند مدیریت ریسک به ارزیابی و پاسخ ختم می‌شود؛ اما در مدل حاضر، نتایج حاصل از هر رخداد سایبری، تحلیل‌های هوش مصنوعی و بازخوردهای مدیریتی، مجدداً وارد فرآیندهای حاکمیتی شده و مبنای اصلاح سیاست‌ها، بازنگری کنترل‌ها و آموزش مجدد مدل‌های هوش مصنوعی قرار می‌گیرد. این چرخه موجب افزایش توان انطباق سازمان در برابر تهدیدهای نوظهور و کاهش آسیب‌پذیری در بلندمدت می‌شود.

از منظر نظری، پژوهش حاضر با یکپارچه‌سازی مفاهیم حاکمیت شرکتی، مدیریت ریسک، امنیت سایبری، هوش مصنوعی و تاب‌آوری سازمانی، مدلی مفهومی ارائه می‌کند که می‌تواند مبنای توسعه پژوهش‌های آینده قرار گیرد. بسیاری از مطالعات پیشین این حوزه را به‌صورت مجزا بررسی کرده‌اند؛ در حالی که پژوهش حاضر ارتباط میان این مؤلفه‌ها را در قالب یک نظام حاکمیتی منسجم تبیین کرده است. از این رو، چارچوب پیشنهادی می‌تواند به غنای ادبیات پژوهش در حوزه حاکمیت سایبری و مدیریت ریسک فناوری اطلاعات کمک کند.

از منظر کاربردی، نتایج پژوهش برای سازمان‌هایی که با ریسک‌های سایبری گسترده مواجه هستند، از جمله بانک‌ها، شرکت‌های بیمه، اپراتورهای مخابراتی، سازمان‌های دولتی، شرکت‌های زیرساختی و صنایع حیاتی، قابل استفاده است. استقرار چارچوب پیشنهادی می‌تواند به مدیران ارشد در تعیین سیاست‌های امنیتی، تخصیص بهینه منابع، اولویت‌بندی سرمایه‌گذاری‌های امنیتی، ارتقای هماهنگی میان واحدهای سازمانی و افزایش آمادگی در برابر رخدادهای سایبری کمک کند. همچنین، استفاده از هوش مصنوعی در فرآیندهای مدیریت ریسک می‌تواند موجب کاهش هزینه‌های ناشی از رخدادهای امنیتی، افزایش سرعت بازیابی خدمات و بهبود کیفیت تصمیم‌گیری مدیریتی شود.

با وجود دستاوردهای پژوهش، محدودیت‌هایی نیز وجود دارد. نخست، چارچوب پیشنهادی بر پایه مرور ادبیات، استانداردهای بین‌المللی و دیدگاه خبرگان تدوین شده و برای تعمیم نتایج به تمامی سازمان‌ها، لازم است در محیط‌های عملیاتی مختلف اعتبارسنجی شود. دوم، سرعت بالای تحول فناوری‌های هوش مصنوعی و ظهور تهدیدهای جدید سایبری ممکن است در آینده نیازمند بازنگری و به‌روزرسانی برخی مؤلفه‌های چارچوب باشد. سوم، تفاوت در ساختار حاکمیتی، الزامات قانونی و سطح بلوغ امنیت سایبری سازمان‌ها می‌تواند بر نحوه استقرار و اثربخشی چارچوب تأثیرگذار باشد.

بر این اساس، پیشنهاد می‌شود در پژوهش‌های آینده، چارچوب ارائه‌شده در صنایع مختلف از جمله بانکداری، سلامت، انرژی، حمل‌ونقل و خدمات دولت الکترونیک به‌صورت تجربی اعتبارسنجی شود. همچنین بررسی نقش فناوری‌های نوظهوری مانند سامانه‌های چندعاملی هوش مصنوعی، هوش مصنوعی مولد، رایانش لبه، معماری اعتماد صفر و رایانش کوانتومی در توسعه تاب‌آوری سایبری می‌تواند زمینه‌های ارزشمندی برای پژوهش‌های آینده فراهم آورد. علاوه بر این، توسعه شاخص‌های بلوغ حاکمیت تاب‌آوری سایبری و طراحی مدل‌های ارزیابی عملکرد مبتنی بر هوش مصنوعی نیز از دیگر حوزه‌های پژوهشی قابل پیشنهاد است.

در مجموع، نتایج این پژوهش نشان می‌دهد که دستیابی به تاب‌آوری سایبری پایدار مستلزم عبور از رویکردهای سنتی امنیت اطلاعات و حرکت به سمت نظام‌های هوشمند حاکمیتی است. چارچوب پیشنهادی با تلفیق اصول حاکمیت شرکتی، مدیریت ریسک، هوش

مصنوعی و یادگیری مستمر، زمینه ایجاد سازمان‌هایی را فراهم می‌کند که نه‌تنها توانایی مقابله با تهدیدهای سایبری را دارند، بلکه قادرند از رخدادهای امنیتی بیاموزند، خود را با شرایط جدید تطبیق دهند و در بلندمدت مزیت رقابتی پایدارتری در فضای دیجیتال کسب کنند.

ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنابر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

تعهد کپی رایت: طبق تعهد نویسندگان حق کپی رایت رعایت شده‌است.

منابع

احمدی، م.، و رضایی، ع. (۱۴۰۲). ارائه چارچوب مدیریت ریسک امنیت سایبری در سازمان‌های مالی ایران. *فصلنامه مدیریت فناوری اطلاعات*، ۱۵(۳)، ۵۵–۷۸.

جعفری، س.، محمدی، ع.، و کریمی، ح. (۱۴۰۱). ارزیابی بلوغ امنیت سایبری در سازمان‌های ایرانی با رویکرد COBIT 2019. *پژوهش‌های مدیریت فناوری اطلاعات*، ۱۴(۲)، ۹۱–۱۱۲.

حسینی، م.، و همکاران. (۱۴۰۳). نقش هوش مصنوعی در مدیریت ریسک امنیت اطلاعات. *فصلنامه پژوهش‌های فناوری اطلاعات*، ۱۸(۱)، ۲۵–۴۸.

References

Ahmadi, M., & Rezaei, A. (2023). A framework for cybersecurity risk management in Iranian financial organizations. *Journal of Information Technology Management*, 15(3), 55–78. (in Persian).

Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). A survey on cyber resilience: Key strategies, research challenges, and future directions. *ACM Computing Surveys*, *56*(8), 196, 1–48. https://doi.org/10.1145/3649218

Committee of Sponsoring Organizations of the Treadway Commission (COSO), & World Business Council for Sustainable Development (WBCSD). (2018). *Enterprise risk management: Applying enterprise risk management to environmental, social and governance-related risks*.

Creswell, J. W., & Plano Clark, V. L. (2021). *Designing and conducting mixed methods research* (3rd ed.). SAGE.

Deloitte. (2024). *Global Future of Cyber Survey 2024*. Deloitte.

ENISA. (2023). *Artificial intelligence and cybersecurity: Challenges and opportunities*. European Union Agency for Cybersecurity.

ENISA. (2024). *ENISA Threat Landscape 2024*. European Union Agency for Cybersecurity. https://doi.org/10.2824/0710888

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). SAGE.

Hosseini, M., et al. (2024). Artificial intelligence in information security risk management. *Information Technology Research Journal, 18*(1), 25–48. (in Persian).

IBM. (2024). *Cost of a data breach report 2024*. IBM Security.

ISACA. (2020). *COBIT 2019 framework: Governance and management objectives*. ISACA.

ISACA. (2023). *State of Cybersecurity 2023*. ISACA.

ISO. (2018). *ISO 31000:2018 Risk management—Guidelines*. International Organization for Standardization.

ISO. (2019). *ISO 22301:2019 Security and resilience—Business continuity management systems—Requirements*. International Organization for Standardization.

ISO. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. International Organization for Standardization.

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management, 8*(2), 100063. https://doi.org/10.1016/j.dim.2023.100063

Jafari, S., Mohammadi, A., & Karimi, H. (2022). Cybersecurity maturity assessment in Iranian organizations based on COBIT 2019. *Information Technology Management Studies, 14*(2), 91–112. (in Persian).

McIntosh, T. R., Susnjak, T., Liu, T., Watters, P. A., Xu, D., Liu, D., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. *Computers & Security*, *144*, 103964. https://doi.org/10.1016/j.cose.2024.103964

Microsoft. (2024). *Microsoft Digital Defense Report 2024*. Microsoft.

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)*. NIST AI 100-1. https://doi.org/10.6028/NIST.AI.100-1

Organisation for Economic Co-operation and Development (OECD). (2023). *G20/OECD principles of corporate governance*. OECD Publishing.

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Paper 29. https://doi.org/10.6028/NIST.CSWP.29

World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. World Economic Forum.

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025*. World Economic Forum.

COPYRIGHT

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.