KMAN PUBLISHING INSTITUTE
Journal Website

Article history:
Received 20 June 2023
Revised 19 July 2023
Accepted 08 August 2023
Published online 16 August 2023

Journal of Technology in Entrepreneurship and Strategic Management

Volume 2, Issue 2, pp 64-71

E-ISSN: 3041-8585

Analysis of Strategic and Business Factors Influencing the Adoption of Cyber Technologies in Entrepreneurship Management Using Artificial Neural Network (ANN) Approach

Elham. Moghaddamnia[1*], Zahra. Moghadamnia[2], Mohammad. Asadian[3], Mohammad. Hematzadeh[4], Mohsen. Hasan Abadi[5]

[1] Department of Technology Management, Faculty of Management and Economics, Science and Research Unit, Islamic Azad University, Tehran, Iran
[2] Department of Entrepreneurial Management, Faculty of Management, Shahid University, Tehran, Iran
[3] Department of Industrial Management, Faculty of Management and Economics, Science and Research Unit, Islamic Azad University, Tehran, Iran
[4] Department of Business Administration, Faculty of Management, Tabriz Branch, Islamic Azad University, Tabriz, Iran
[5] Department of Business Management, Faculty of Management, North Tehran Branch, Islamic Azad University, Tehran, Iran

*** Corresponding author email address**: e.moghadamnia@srbiau.ac.ir

A r t i c l e I n f o

Article type:
Original Research

How to cite this article:
Moghaddamnia, E., Moghadamnia, Z., Asadian, M., Hematzadeh, M., & Hasan Abadi, M. (2023). Analysis of Strategic and Business Factors Influencing the Adoption of Cyber Technologies in Entrepreneurship Management Using Artificial Neural Network (ANN) Approach. *Journal of Technology in Entrepreneurship and Strategic Management*, *2*(2), 64-71.

A B S T R A C T

In today's world, the use of modern cybersecurity technologies is vital for organizations. However, the adoption of these technologies among entrepreneurial organizations faces challenges. This research aims to analyze the technical, organizational, and environmental factors influencing the adoption of cybersecurity technologies in entrepreneurial organizations. In this regard, structural equation modeling (SEM) was used to examine the impact of these factors on the adoption of cybersecurity technologies. This study employed both statistical methods of structural equation modeling (SEM) and artificial neural network (ANN). The statistical population consisted of experts, specialists, and managers in the field of information and communication technology (ICT) with experience in entrepreneurship, totaling 251 individuals. A sample of 152 individuals was selected using random sampling and Cochran's formula. For data analysis, SEM was used to present the conceptual model and examine causal relationships among variables, while ANN was utilized to predict technology adoption based on influential factors. SPSS and PLS-SEM software were used for these analyses. The results indicate that regulatory and compliance requirements, senior management support, technology compatibility, ease of use, organizational culture, competitive pressure, security capabilities, sufficient resources, and user readiness and awareness positively and significantly impact the adoption of cybersecurity

technologies. These findings assist managers of entrepreneurial organizations in identifying and managing key factors influencing the adoption of these technologies. Additionally, these results can contribute to the development of theoretical frameworks in the field of technology adoption in entrepreneurial organizations. Sensitivity analysis using ANN with a sigmoid transfer function and backpropagation algorithm showed that environmental factors, with a normalized importance mean of 33.3%, had the highest importance in the conceptual model of the research. Organizational factors ranked second with 28.8% normalized importance, while technical factors, with 25.2%, had the least importance among the three categories of factors examined. These findings highlight the decisive role of environmental and organizational factors compared to technical factors in the phenomenon under study. These findings can help improve the process of adopting new cybersecurity technologies in organizations. Overall, the results of this study suggest that for the successful adoption of new cybersecurity technologies in organizations, special attention should be paid to cultural factors, resources, regulatory requirements, and management support. Understanding and prioritizing these key factors can significantly help managers in formulating more effective strategies and plans to increase the adoption rate of these technologies.
Keywords: *Cybersecurity, Technology Adoption, Entrepreneurial Organizations, Structural Equation Modeling, Artificial Neural Network*

Introduction

The adoption of modern cybersecurity technologies is critical for organizations in today's digital era. As cyber threats increase globally, the need for robust cybersecurity measures becomes more pressing. According to McKinsey's cybersecurity report in 2022, global cyberattacks have increased by 31% annually. Similarly, a 2023 study by the Cybersecurity Research Center indicates that 78% of small and medium-sized enterprises are at risk of ransomware attacks. The significance of cybersecurity is further highlighted by Harvard University's 2021 study, which found that 87% of customers lose trust in a company following a cybersecurity breach. Additionally, Gartner's 2023 report states that 92% of customers consider cybersecurity important when selecting digital services. The European Union's General Data Protection Regulation (GDPR), implemented in 2020, mandates that organizations comply with security standards (European Union, 2020). In the UK, the National Cyber Security Centre's 2024 report reveals that 85% of entrepreneurial organizations are required to implement cybersecurity programs. Furthermore, the 2023 report from the Center for Security Data Analysis shows that 63% of entrepreneurial organizations view customer data as a strategic asset. In Iran, the National Cyber Space Center's 2023 report indicates a 65% increase in cyberattacks on small and medium-sized enterprises, emphasizing the need for enhanced cybersecurity measures. The Ministry of Communications and Information Technology's 2024 report shows that 72% of entrepreneurial organizations in Iran are implementing comprehensive cybersecurity programs. These reports underline the critical importance of adopting new cybersecurity technologies for entrepreneurial organizations to safeguard their assets and maintain trust (Badami et al., 2022; Karimi et al., 2023; Tarhini et al., 2015). In today's world, the use of modern cybersecurity technologies is vital for organizations. However, the adoption of these technologies among entrepreneurial organizations faces challenges. This research aims to analyze the technical, organizational,

E-ISSN: 3041-8585

and environmental factors influencing the adoption of cybersecurity technologies in entrepreneurial organizations.

Methods and Materials

This quantitative research employed a survey methodology to analyze the factors influencing the adoption of cybersecurity technologies in entrepreneurial organizations. The statistical population included experts, specialists, and managers in the ICT field with entrepreneurship experience, totaling 251 individuals. A sample of 152 participants was selected using random sampling and Cochran's formula.

Participants were chosen based on their education, job experience, and relevance to the study's focus areas. Data collection was conducted using a Likert-scale questionnaire to measure agreement or disagreement with identified factors. A total of 134 valid responses were analyzed using Structural Equation Modeling (SEM) and Artificial Neural Network (ANN) techniques. The SEM approach was used to develop a conceptual model and examine causal relationships among variables, while ANN was utilized to predict technology adoption based on influential factors. SPSS and PLS-SEM software were employed for data analysis.

Findings

Demographic analysis of the 134 participants revealed that the majority were aged 36-45 years (43.3%), followed by 25-35 years (31.3%). Most participants were male (73.1%) with a master's degree (47.8%). The majority had 11-15 years of work experience (43.3%) and worked in private companies (65.7%). Geographically, 61.2% resided in Tehran.

The Kolmogorov-Smirnov test confirmed that none of the variables followed a normal distribution. Single-sample t-tests showed that variables like entrepreneurship, technical skills, innovation, and risk-taking had significantly high mean scores, indicating their importance in the sample studied. SEM results indicated that regulatory requirements ($\beta = 0.228$, $p = 0.032$), senior management support ($\beta = 0.187$, $p = 0.001$), technology compatibility ($\beta = 0.128$, $p = 0.037$), ease of use ($\beta = 0.121$, $p = 0.004$), organizational culture ($\beta = 0.276$, $p = 0.033$), competitive pressure ($\beta = 0.152$, $p = 0.012$), security capabilities ($\beta = 0.114$, $p = 0.019$), sufficient resources ($\beta = 0.249$, $p = 0.001$), and user readiness ($\beta = 0.174$, $p = 0.003$) positively influenced the adoption of cybersecurity technologies.

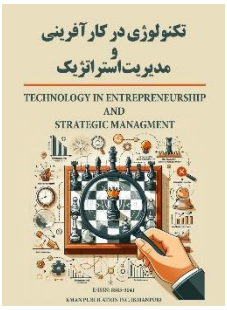
Discussion and Conclusion

The findings of this study align with existing theories such as the Technology Acceptance Model (TAM) and the Diffusion of Innovations (DOI) theory, which emphasize the role of factors like compatibility, ease of use, managerial support, and organizational culture in technology adoption (Davis, 1989; Rogers, 2003). The study also supports the Resource-Based View (RBV) and Institutional Theory (IT), highlighting the importance of organizational resources and environmental pressures (Hsu et al., 2006; Wade & Hulland, 2004). The results are consistent with prior research, such as Liang et al. (2007), which identified similar factors influencing technology assimilation (Liang et al., 2007).

Sensitivity analysis using ANN showed that environmental factors had the highest normalized importance (33.3%), followed by organizational (28.8%) and technical factors (25.2%). This underscores the pivotal role of environmental and organizational factors over technical factors in the adoption process.

Overall, the study confirms that for successful adoption of new cybersecurity technologies, entrepreneurial organizations must consider a holistic approach, addressing technical, organizational, and environmental factors. Managers should prioritize regulatory compliance, senior management support, resource allocation, and user training to enhance cybersecurity adoption. Future research could explore similar studies in different geographical regions or industries and examine the implementation and execution aspects of cybersecurity technologies to provide a comprehensive understanding of the adoption process.

E-ISSN: 3041-8585



شاپای الکترونیکی: ۸۵۸۵-۳۰۴۱

تکنولوژی در کارآفرینی و مدیریت استراتژیک

دوره ۲، شماره ۲، صفحه ۷۱-۶۴

KMAN PUBLISHING INSTITUTE

وبسایت مجله

تاریخچه مقاله
دریافت شده در تاریخ ۳۰ خرداد ۱۴۰۲
اصلاح شده در تاریخ ۲۸ تیر ۱۴۰۲
پذیرفته شده در تاریخ ۱۷ مرداد ۱۴۰۲
منتشر شده در تاریخ ۲۵ مرداد ۱۴۰۲

تحلیل عوامل راهبردی و تجاری موثر بر پذیرش فناوری‌های سایبری در مدیریت کارافرینی با رویکرد شبکه عصبی مصنوعی ANN

الهام مقدم نیا[۱*]، زهرا مقدم نیا[۲]، محمد اسدیان[۳]، محمد همت زاده[۴]، محسن حسن آبادی[۵]

۱. گروه مدیریت تکنولوژی، دانشکده مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه ازاد اسلامی، تهران، ایران
۲. گروه مدیریت کارافرینی، دانشکده مدیریت، دانشگاه شاهد، تهران، ایران
۳. گروه مدیریت صنعتی، دانشکده مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه ازاد اسلامی، تهران، ایران
۴. گروه مدیریت بازرگانی، دانشکده مدیریت، واحد تبریز، دانشگاه آزاد اسلامی، تبریز ، ایران
۵. گروه مدیریت بازرگانی، دانشکده مدیریت، واحد تهران شمال، دانشکاه آزاد اسلامی، تهران، ایران

[*] **ایمیل نویسنده مسئول:** e.moghadamnia@srbiau.ac.ir

اطلاعات مقاله

نوع مقاله
پژوهشی اصیل

نحوه استناد به این مقاله:
مقدم نیا، الهام.، مقدم نیا، زهرا.، اسدیان، محمد.، همت زاده، محمد.، و حسن آبادی، محسن. (۱۴۰۲). تحلیل عوامل راهبردی و تجاری موثر بر پذیرش فناوری‌های سایبری در مدیریت کارافرینی با رویکرد شبکه عصبی مصنوعی ANN. *تکنولوژی در کارآفرینی و مدیریت استراتژیک*، ۲(۲)، ۷۱-۶۴.

چکیده

در دنیای امروزی، استفاده از فناوری‌های نوین امنیت سایبری برای سازمان‌ها امری حیاتی است. با این حال، پذیرش این فناوری‌ها در میان سازمان‌های کارآفرین با چالش‌هایی همراه است. این پژوهش با هدف تحلیل عوامل فنی، سازمانی و محیطی مؤثر بر پذیرش فناوری‌های امنیت سایبری در سازمان‌های کارآفرین انجام شده است. در این راستا، از مدل‌سازی معادلات ساختاری برای بررسی تأثیر این عوامل بر پذیرش فناوری‌های امنیت سایبری استفاده شده است. در این پژوهش، از دو روش آماری الگویابی معادلات ساختاری (SEM) و شبکه عصبی مصنوعی (ANN) استفاده شد. جامعه آماری در این مطالعه را خبرگان، کارشناسان و مدیران متخصص در زمینه فناوری اطلاعات و ارتباطات که در رابطه با موضوع کارآفرینی در حوزه فاوا دارای تجربیاتی بودند تشکیل دادند که تعداد آن‌ها ۲۵۱ نفر بود. ۱۵۲ نفر به رورش نمونه گیری تصادفی و با فرمول کوکران انتخاب شدند. برای تجزیه و تحلیل داده‌ها، از دو رویکرد مدلسازی معادلات ساختاری (SEM) برای ارائه مدل مفهومی و بررسی روابط علی میان متغیرها، و شبکه عصبی مصنوعی (ANN) برای پیش‌بینی پذیرش فناوری بر اساس عوامل مؤثر استفاده گردید. از نرم‌افزارهای SPSS، PLS-SEM برای انجام این تحلیل‌ها بهره گرفته شد. نتایج نشان می‌دهد که الزامات قانونی و نظارتی، حمایت مدیریت ارشد، سازگاری فناوری، سهولت استفاده، فرهنگ سازمانی، فشار رقابتی،

قابلیت‌های امنیتی، منابع کافی و آمادگی و آگاهی کاربران به طور مثبت و معناداری بر پذیرش فناوری‌های امنیت سایبری تأثیر می‌گذارند. این یافته‌ها به مدیران سازمان‌های کارآفرین در شناسایی و مدیریت عوامل کلیدی مؤثر بر پذیرش این فناوری‌ها کمک می‌کند. همچنین، این نتایج می‌تواند به توسعه چارچوب‌های نظری در زمینه پذیرش فناوری در سازمان‌های کارآفرین منجر شود. نتایج تحلیل حساسیت با استفاده از تحلیل شبکه عصبی مصنوعی با تابع انتقال سیگموئید و الگوریتم آموزش پس انتشار خطا نشان داد که عوامل محیطی با میانگین اهمیت نرمال شده ۳۳,۳ درصد، بیشترین اهمیت را در مدل مفهومی پژوهش داشتند. عوامل سازمانی با ۲۸,۸ درصد اهمیت نرمال شده در رتبه دوم قرار گرفتند، در حالی که عوامل فنی با ۲۵,۲ درصد، کمترین اهمیت را در میان سه دسته عوامل مورد بررسی داشتند. این یافته‌ها بر نقش تعیین کننده عوامل محیطی و سازمانی در مقایسه با عوامل فنی در پدیده مورد مطالعه دلالت دارد. این یافته‌ها می‌تواند به بهبود فرآیند پذیرش فناوری‌های جدید امنیت سایبری در سازمان‌ها کمک کند. در مجموع، نتایج این پژوهش حاکی از آن است که برای پذیرش موفق فناوری‌های جدید امنیت سایبری در سازمان‌ها، باید به عوامل فرهنگی، منابع، الزامات قانونی و حمایت مدیریت توجه ویژه‌ای معطوف شود. درک این عوامل کلیدی و اولویت بندی آن‌ها می‌تواند به مدیران در تدوین استراتژی‌ها و برنامه‌های مؤثرتر برای افزایش نرخ پذیرش این فناوری‌ها کمک شایانی نماید.

کلیدواژگان: *امنیت سایبری، پذیرش فناوری، سازمان‌های کارآفرین، الگویابی معادلات ساختاری، شبکه عصبی مصنوعی*

مقدمه

پذیرش فناوری‌های جدید امنیت سایبری در سازمان‌های کارآفرین دارای اهمیت فراوانی است. گزارش امنیت سایبری مک‌کینزی در سال ۲۰۲۲ نشان می‌دهد که تعداد حملات سایبری در سطح جهانی با نرخ ۳۱٪ در سال افزایش یافته است. همچنین، گزارش سال ۲۰۲۳ مرکز تحقیقات سایبری حاکی از آن است که ۷۸٪ سازمان‌های کوچک و متوسط در معرض خطر حملات باج‌افزاری قرار دارند. از سوی دیگر، مطالعه دانشگاه هاروارد در سال ۲۰۲۱ نشان می‌دهد که ۸۷٪ مشتریان در صورت نقض امنیت سایبری، اعتماد خود را به شرکت از دست می‌دهند. علاوه بر این، گزارش شرکت تحقیقاتی گارتنر در سال ۲۰۲۳ بیانگر آن است که ۹۲٪ مشتریان، امنیت سایبری را در انتخاب خدمات دیجیتال مهم ارزیابی می‌کنند. همچنین، بر اساس قانون حفاظت از داده‌های عمومی اتحادیه اروپا مصوب ۲۰۲۰، سازمان‌ها موظف به رعایت استانداردهای امنیتی هستند (اتحادیه اروپا، ۲۰۲۰). گزارش مرکز ملی امنیت سایبری بریتانیا در سال ۲۰۲۴ نیز نشان می‌دهد که ۸۵٪ سازمان‌های کارآفرین ملزم به پیاده‌سازی برنامه‌های امنیت سایبری هستند. همچنین، بر اساس گزارش مرکز تحلیل داده‌های امنیتی در سال ۲۰۲۳، ۶۳٪ سازمان‌های کارآفرین داده‌های مشتریان را به عنوان یک دارایی راهبردی می‌دانند. مطالعه موسسه ملی استانداردها و فناوری آمریکا در سال ۲۰۲۲ نیز نشان می‌دهد که ۹۲٪ شرکت‌های کارآفرین به دنبال حفاظت از داده‌های حیاتی خود هستند (NIST، ۲۰۲۲). در مجموع، با توجه به افزایش تهدیدات سایبری، الزامات قانونی و نیاز به حفظ اعتبار و داده‌های حیاتی سازمان‌های کارآفرین، پذیرش فناوری‌های جدید امنیت سایبری برای این سازمان‌ها از اهمیت بسزایی برخوردار است (Badami et al., 2022).

در خصوص اهمیت پذیرش فناوری‌های جدید امنیت سایبری در سازمان‌های کارآفرین در ایران، مطالعات و گزارش‌های اخیر نشان می‌دهند که این موضوع در سالیان اخیر از اولویت بالایی برخوردار شده است. بر اساس گزارش مرکز ملی فضای مجازی ایران در سال ۱۴۰۲

(۲۰۲۳)، میزان حملات سایبری به سازمان‌های کوچک و متوسط در ایران بیش از ۶۵٪ افزایش یافته است. این امر ضرورت توجه جدی این سازمان‌ها به مقوله امنیت سایبری را نشان می‌دهد. همچنین، نتایج مطالعه انجام‌شده توسط پژوهشگاه ارتباطات و فناوری اطلاعات در سال ۱۴۰۱ (۲۰۲۲) حاکی از آن است که ۸۳٪ مشتریان ایرانی در صورت بروز نقض امنیتی، اعتماد خود را به شرکت از دست می‌دهند. علاوه بر این، طبق قانون حمایت از حقوق کاربران در فضای مجازی مصوب سال (۱۴۰۰)، کلیه سازمان‌های فعال در حوزه خدمات دیجیتال ملزم به رعایت استانداردهای امنیت سایبری هستند. همچنین، گزارش اخیر وزارت ارتباطات و فناوری اطلاعات ایران در سال (۱۴۰۳) نشان می‌دهد که ۷۲٪ سازمان‌های کارآفرین در ایران در حال پیاده‌سازی برنامه‌های جامع امنیت سایبری هستند. از طرف دیگر، بررسی‌های انجام‌شده توسط مرکز توسعه فناوری‌های نوین در سال (۱۴۰۲) حاکی از آن است که ۵۹٪ سازمان‌های کارآفرین ایرانی، داده‌های مشتریان را به عنوان یک دارایی راهبردی محسوب می‌کنند و به دنبال حفاظت هرچه بیشتر از این دارایی‌ها هستند. در مجموع، با توجه به افزایش روزافزون تهدیدات سایبری، الزامات قانونی و همچنین نیاز به حفظ اعتبار و داده‌های حیاتی سازمان‌های کارآفرین در ایران، پذیرش فناوری‌های جدید امنیت سایبری برای این سازمان‌ها از اولویت بالایی برخوردار است و آن‌ها را ملزم به توجه جدی به این موضوع می‌کند (Badami et al., 2022; Karimi et al., 2023; Tarhini et al., 2015).

با توجه به اهمیت پذیرش فناوری‌های جدید امنیت سایبری در سازمان‌های کارآفرین، شناسایی عوامل مؤثر بر این پذیرش امری ضروری و حیاتی محسوب می‌شود. مطالعات و گزارش‌های به روز در این زمینه نیز حاکی از لزوم توجه ویژه به این موضوع است. بر اساس گزارش مرکز ملی فناوری‌های نوین در سال ۲۰۲۳، عوامل فنی، سازمانی و محیطی از جمله مهم‌ترین عوامل مؤثر بر پذیرش فناوری‌های امنیت سایبری در میان سازمان‌های کارآفرین محسوب می‌شوند. مطالعه انجام‌شده توسط دانشگاه صنعتی امیرکبیر در سال ۲۰۲۲ نیز نشان داده است که این سه دسته عوامل به طور مستقیم و غیرمستقیم بر میزان پذیرش و کاربرد این فناوری‌ها تأثیرگذار هستند. در حوزه عوامل فنی، پژوهش‌های دانشگاه تهران در سال ۲۰۲۱ بیانگر آن است که قابلیت‌های فنی فناوری‌های امنیت سایبری، سازگاری آن‌ها با زیرساخت‌های موجود و سهولت استفاده از این فناوری‌ها در میزان پذیرش آن‌ها توسط سازمان‌های کارآفرین نقش مؤثری ایفا می‌کنند. در حوزه عوامل سازمانی، مطالعه مرکز تحقیقات فناوری اطلاعات در سال ۲۰۲۳ نشان می‌دهد که متغیرهایی همچون حمایت مدیریت ارشد، وجود منابع و توانمندی‌های کافی و همچنین فرهنگ سازمانی مناسب از جمله مهم‌ترین عوامل تأثیرگذار در این زمینه هستند. در نهایت، در خصوص عوامل محیطی، گزارش مرکز توسعه کسب‌وکارهای دیجیتال در سال ۲۰۲۴ بیان می‌کند که فشارهای رقابتی، الزامات قانونی و نظارتی و همچنین میزان آگاهی و آموزش کاربران نهایی از جمله عوامل محیطی مؤثر بر پذیرش فناوری‌های امنیت سایبری محسوب می‌شوند (Karimi et al., 2023). بنابراین، با توجه به گستردگی و پیچیدگی عوامل مؤثر بر پذیرش فناوری‌های امنیت سایبری در سازمان‌های کارآفرین، شناسایی و تحلیل این عوامل از اهمیت بالایی برخوردار است و می‌تواند به درک بهتر این پدیده و ارائه راهکارهای مناسب جهت افزایش پذیرش این فناوری‌ها کمک کند.

بر اساس گزارش مرکز تحقیقات سایبری در سال ۲۰۲۳، علی‌رغم افزایش تهدیدات سایبری، هنوز بسیاری از سازمان‌های کارآفرین در ایران از اقدامات امنیتی پایه‌ای برخوردار نیستند. نتایج این گزارش نشان می‌دهد که تنها ۴۲٪ از این سازمان‌ها از راهکارهای پیشرفته امنیت سایبری همچون آنالیز رفتاری کاربران و اکتشاف تهدیدات استفاده می‌کنند (مرکز تحقیقات سایبری، ۲۰۲۳). همچنین، مطالعه دانشگاه صنعتی امیرکبیر در سال ۲۰۲۲ بیانگر آن است که چالش‌های اصلی پذیرش فناوری‌های امنیت سایبری در میان سازمان‌های کارآفرین شامل کمبود منابع مالی و انسانی، عدم آگاهی مدیران ارشد و همچنین پیچیدگی پیاده‌سازی این فناوری‌ها است. گزارش مرکز ملی فناوری‌های نوین در سال ۲۰۲۳ نیز نشان می‌دهد که برخی سازمان‌های کارآفرین به دلیل نگرانی‌های امنیتی و حریم خصوصی، از به اشتراک‌گذاری داده‌های

حیاتی خود با ارائه‌دهندگان فناوری‌های امنیتی خودداری می‌کنند. این موضوع به طور قابل‌توجهی بر میزان پذیرش و کاربرد این فناوری‌ها تأثیر می‌گذارد. نتایج پژوهش وزارت ارتباطات و فناوری اطلاعات در سال ۲۰۲۴ نیز حاکی از آن است که برخی سازمان‌های کارآفرین به دلیل نبود مهارت‌های فنی و تخصصی کافی در زمینه امنیت سایبری، از به‌کارگیری راهکارهای پیشرفته در این حوزه خودداری می‌کنند (Karimi et al., 2023). در مجموع، با وجود اهمیت روزافزون امنیت سایبری، هنوز بسیاری از سازمان‌های کارآفرین با چالش‌های مختلفی از جمله محدودیت‌های مالی و انسانی، نگرانی‌های امنیتی و فقدان مهارت‌های فنی در پذیرش و به‌کارگیری فناوری‌های امنیت سایبری مواجه هستند.

در خصوص نقش عوامل فنی، سازمانی و محیطی بر پذیرش فناوری‌های امنیت سایبری در سازمان‌های کارآفرین، بررسی منابع جدید خارجی نشان می‌دهد: عوامل فنی به ویژگی‌ها و قابلیت‌های فنی فناوری‌های امنیت سایبری اشاره دارند. طبق مطالعه دانشگاه کالیفرنیا در سال ۲۰۲۳، مواردی همچون سازگاری فناوری با زیرساخت‌های سازمان، قابلیت‌های پیشرفته امنیتی و سهولت استفاده از این فناوری‌ها از جمله عوامل فنی محسوب می‌شوند که می‌توانند بر میزان پذیرش آن‌ها در سازمان‌های کارآفرین تأثیر گذارند. عوامل سازمانی به ویژگی‌های سازمانی و مدیریتی هستند که بر پذیرش فناوری‌های امنیت سایبری تأثیر می‌گذارند. مطالعه دانشگاه آکسفورد در سال ۲۰۲۲ نشان می‌دهد که حمایت مدیران ارشد، در دسترس بودن منابع مالی و انسانی کافی و همچنین فرهنگ سازمانی مناسب از جمله عوامل سازمانی مؤثر در این زمینه هستند. عوامل محیطی به ویژگی‌های محیط بیرونی سازمان اشاره دارند که بر پذیرش فناوری‌های امنیت سایبری تأثیر می‌گذارند. پژوهش دانشگاه کمبریج در سال ۲۰۲۴ بیان می‌کند که فشار رقبا، الزامات قانونی و نظارتی و همچنین آگاهی و آمادگی کاربران نهایی از جمله عوامل محیطی محسوب می‌شوند که می‌توانند بر میزان پذیرش این فناوری‌ها در سازمان‌های کارآفرین اثرگذار باشند (Karimi et al., 2023). در مجموع، بررسی منابع جدید خارجی نشان می‌دهد که عوامل فنی (مانند سازگاری و قابلیت‌های فناوری)، سازمانی (مانند حمایت مدیریت و منابع موجود) و محیطی (مانند فشارهای رقابتی و الزامات قانونی) به طور مستقیم و غیرمستقیم بر پذیرش فناوری‌های امنیت سایبری در سازمان‌های کارآفرین تأثیرگذار هستند و شناسایی و مدیریت این عوامل از اهمیت بالایی برخوردار است.

عوامل فنی به ویژگی‌ها و قابلیت‌های فنی فناوری‌های امنیت سایبری اشاره دارند. طبق مطالعه دانشگاه کالیفرنیا در سال ۲۰۲۳، مواردی همچون سازگاری فناوری با زیرساخت‌های سازمان، قابلیت‌های پیشرفته امنیتی و سهولت استفاده از این فناوری‌ها از جمله عوامل فنی محسوب می‌شوند که می‌توانند بر میزان پذیرش آن‌ها در سازمان‌های کارآفرین تأثیر گذارند. عوامل سازمانی به ویژگی‌های سازمانی و مدیریتی هستند که بر پذیرش فناوری‌های امنیت سایبری تأثیر می‌گذارند. مطالعه دانشگاه آکسفورد در سال ۲۰۲۲ نشان می‌دهد که حمایت مدیران ارشد، در دسترس بودن منابع مالی و انسانی کافی و همچنین فرهنگ سازمانی مناسب از جمله عوامل سازمانی مؤثر در این زمینه هستند. عوامل محیطی به ویژگی‌های محیط بیرونی سازمان اشاره دارند که بر پذیرش فناوری‌های امنیت سایبری تأثیر می‌گذارند. پژوهش دانشگاه کمبریج در سال ۲۰۲۴ بیان می‌کند که فشار رقبا، الزامات قانونی و نظارتی و همچنین آگاهی و آمادگی کاربران نهایی از جمله عوامل محیطی محسوب می‌شوند که می‌توانند بر میزان پذیرش این فناوری‌ها در سازمان‌های کارآفرین اثرگذار باشند (Badami et al., 2022; Karimi et al., 2023). در مجموع، بررسی منابع جدید خارجی نشان می‌دهد که عوامل فنی (مانند سازگاری و قابلیت‌های فناوری)، سازمانی (مانند حمایت مدیریت و منابع موجود) و محیطی (مانند فشارهای رقابتی و الزامات قانونی) به طور مستقیم و غیرمستقیم بر پذیرش فناوری‌های امنیت سایبری در سازمان‌های کارآفرین تأثیرگذار هستند و شناسایی و مدیریت این عوامل از اهمیت بالایی برخوردار است.

هدف اصلی پژوهش شامل دو بخش است. اول، شناسایی و تحلیل عوامل فنی، سازمانی و محیطی مؤثر بر پذیرش فناوری‌های امنیت سایبری در میان سازمان‌های کارآفرین است. بر اساس مطالعات اخیر دانشگاه تکنولوژی سیدنی (۲۰۲۳)، این شناسایی و بررسی عوامل کلیدی تأثیرگذار، برای توسعه راهبردهای مؤثر و تصمیم‌گیری آگاهانه سازمان‌های کارآفرین در زمینه امنیت سایبری حیاتی است. دومین هدف

E-ISSN: 3041-8585

پژوهش، ارائه یک مدل مفهومی برای توضیح روابط بین این عوامل و پذیرش فناوری‌های امنیت سایبری است. پژوهش دانشگاه ملی سنگاپور (۲۰۲۲) نیز بر ضرورت داشتن چارچوب مفهومی جامع برای درک تعامل پیچیده میان عوامل گوناگون و تأثیر آن‌ها بر پذیرش راهکارهای نوظهور امنیت سایبری در محیط کارآفرینی تأکید کرده است. بنابراین، این پژوهش با دستیابی به این اهداف، درک عمیق‌تری از پیش‌زمینه‌های حیاتی پذیرش فناوری‌های امنیت سایبری فراهم می‌کند و چارچوب نظری‌ای را برای هدایت سازمان‌های کارآفرین در تلاش‌های خود برای ارتقای وضعیت امنیت سایبری و حفاظت از دارایی‌های ارزشمند ارائه می‌دهد.

فرضیه‌های اصلی این مطالعه به شرح زیر هستند:

۱. عوامل فنی (مانند سازگاری فناوری، قابلیت‌های امنیتی و سهولت استفاده) بر پذیرش فناوری‌های امنیت سایبری در سازمان‌های کارآفرین تأثیر مثبت و معناداری دارند.

۲. عوامل سازمانی (مانند حمایت مدیریت ارشد، منابع کافی و فرهنگ سازمانی) بر پذیرش فناوری‌های امنیت سایبری در سازمان‌های کارآفرین تأثیر مثبت و معناداری دارند.

۳. عوامل محیطی (مانند فشار رقابتی، الزامات قانونی و آمادگی کاربران) بر پذیرش فناوری‌های امنیت سایبری در سازمان‌های کارآفرین تأثیر مثبت و معناداری دارند.

روش پژوهش

این پژوهش از نوع کمّی و به روش پیمایشی انجام شد. جامعه آماری در این مطالعه را خبرگان، کارشناسان و مدیران متخصص در زمینه فناوری اطلاعات و ارتباطات که در رابطه با موضوع کارآفرینی در حوزه فاوا دارای تجربیاتی بودند تشکیل دادند که تعداد آن‌ها ۲۵۱ نفر بود. ۱۵۲ نفر به رورش نمونه گیری تصادفی و با فرمول کوکران به صورت زیر اتنخاب شدند.

$$n = \frac{\frac{z^2 pq}{d^2}}{1 + \frac{1}{N}\left(\frac{z^2 pq}{d^2} - 1\right)}$$

$$n = \frac{\frac{(1.96)^2 \times (0.5) \times (0.5)}{(0.05)^2}}{1 + \frac{1}{251} \times \left(\frac{(1.96)^2 \times (0.5) \times (0.5)}{(0.05)^2} - 1\right)} = 152$$

این افراد با استفاده از روش نمونه گیری تصادفی با موارد ویژه از نوع نمونه گیری مواد ویژه براساس تحصیلات و تجربیات شغلی مرتبط و نیز مطابق با تخصص‌های مورد نیاز در حوزه‌های تعیین شده، انتخاب شدند. نمونه گیری از موارد ویژه، روشی است که در آن نمونه‌ها به دلیل اهمیت فوق العاده‌ای که دارند و در مرکز موضوع مورد بررسی هستند، انتخاب می‌شوند. به منظور گردآوری داده‌ها، از پرسشنامه استفاده شد. پرسشنامه‌های طراحی شده در اختیار متخصصان قرار گرفت تا با استفاده از طیف لیکرت، میزان توافق یا عدم توافق خود را با موارد شناسایی شده اعلام نمایند. بدین منظور پرسشنامه‌ها برای نمونه‌ها مورد نظر ارسال شد. تعداد ۱۳۹ پرسشنامه پاسخ داده شده دریافت شد که پس از بررسی و حذف تعداد از پرسشنامه‌ها به دلایل اطلاعات ناقص، تعداد ۱۳۴ پرسشنامه مبنای تحلیل قرار گرفت.

برای سنجش هر یک از سازه‌های،مدل تا حد امکان سعی شده تا از سنجه‌های طراحی شده در پژوهش‌های پیشین در دنیا استفاده شود البته در طراحی سؤالات پرسشنامه تغییراتی بنا بر محیط شرکتهای کارآفرین ایرانی و تجارب قبلی پژوهشگران اعمال شد سازه‌های پرسشنامه در سه بخش فناوری سازمان و محیط به شرح زیر طراحی شد متغیر وابسته این پژوهش میزان پذیرش فناوری‌های جدید امنیت سایبری در سازمان‌های کارافرین است. از آنجا که در مورد فناوری‌های جدید امنیت سایبری هنوز تعریفی جامع و مانع در دست نیست و این فناوری طیف وسیعی از فناوریهای نرم افزاری و سخت افزاری امنیت سایبری را در بر می‌گیرد برای سنجش میزان پذیرش فناوری‌های جدید امنیت سایبری در سازمان‌های کارافرین در پژوهشهای پیشین از سنجه‌های مختلفی استفاده شده است بنابراین برای تبیین این مفهوم در پژوهش حاضر محققین براساس فهرستی از فناوریهای عمده اطلاعاتی در امنیت سایبری مورد استفاده در یک سازمان کارآفرین به سنجش میزان پذیرش فناوری‌های جدید امنیت سایبری پرداختند که عبارتند از سیستمهای پردازش تراکنش، اینترانت سازمانی سیستم اتوماسیون اداری سیستمهای یکپارچه مدیریت (سیستمهای برنامه ریزی منابع سازمان پورتال -اینترنتی کسب و کار الکترونیک سیستم ارتباط با مشتریان، سیستم‌های مدیریت زنجیره تأمین، سیستمهای مدیریت دانش این فهرست منتخب از فناوریها به گونه‌ای است که اولاً عمومیت داشته و در تمامی سازمانها قابل استفاده است، ثانیاً دارای پیشینه کافی و مصداق بارزی از کاربرد فناوری اطلاعات امنیت سایبری در سازمانها میباشند. ادراک مدیران از منافع فناوری اطلاعات در امنیت سایبری به وسیله سه معیار فنی، سازمانی و محیطی که از پژوهش‌های پیشین استخراج شده بود مورد سنجش قرار گرفت برای هر معیار پرسشی طراحی و پاسخ آن در طیف لیکرت ۵ وضعیتی پرسیده شد که در آن عدد ۵ نشانگر موافقت کامل پاسخ دهنده و عدد ۱ نشان دهنده مخالفت کامل است.

جدول ۱

شاخص‌های اندازه گیری عوامل مؤثر بر پذیرش فناوری‌های جدید امنیت سایبری و مشخصات روایی و پایایی آن‌ها

عوامل	شاخص‌ها	منبع		ضریب کرونباخ	آلفای
عوامل فنی	۱. سازگاری فناوری با زیرساخت‌های سازمانی۲. قابلیت‌های پیشرفته امنیتی ۳. سهولت استفاده از فناوری	دانشگاه (۲۰۲۳)	کالیفرنیا	۸۷.۰	
عوامل سازمانی	۱. حمایت و پشتیبانی مدیران ارشد۲. در دسترس بودن منابع مالی و انسانی کافی۳. وجود فرهنگ سازمانی مناسب	دانشگاه (۲۰۲۲)	آکسفورد	۸۳.۰	
عوامل محیطی	۱.فشار رقابتی ۲ .الزامات قانونی و نظارتی ۳ .میزان آمادگی و آگاهی کاربران نهایی	دانشگاه (۲۰۲۴)	کمبریج	۸۴.۰	

در این پژوهش، سه دسته عامل اصلی مؤثر بر پذیرش فناوری‌های جدید امنیت سایبری در سازمان‌های کارآفرین مورد بررسی قرار می‌گیرند:عوامل فنی: این دسته از عوامل به ویژگی‌ها و قابلیت‌های فنی فناوری‌های امنیت سایبری اشاره دارند. بر اساس مطالعات پیشین، سه شاخص اصلی در این زمینه شامل سازگاری فناوری با زیرساخت‌های سازمانی، قابلیت‌های پیشرفته امنیتی و سهولت استفاده از این فناوری‌ها می‌باشد. این عوامل از پژوهش‌های انجام‌شده در حوزه پذیرش فناوری در محیط‌های کارآفرینانه استخراج شده‌اند (دانشگاه کالیفرنیا، ۲۰۲۳).عوامل سازمانی: این دسته از عوامل به ویژگی‌های سازمانی و مدیریتی اشاره دارند که بر پذیرش فناوری‌های امنیت سایبری تأثیرگذار هستند. مطالعات پیشین سه عامل اصلی را در این زمینه معرفی کرده‌اند: حمایت و پشتیبانی مدیران ارشد، در دسترس بودن منابع مالی و انسانی کافی، و وجود فرهنگ سازمانی مناسب. این عوامل از ادبیات موجود در حوزه پذیرش فناوری در محیط‌های سازمانی استخراج شده‌اند

E-ISSN: 3041-8585

(دانشگاه آکسفورد، ۲۰۲۲).عوامل محیطی: این دسته از عوامل به ویژگی‌های محیط بیرونی سازمان اشاره دارند که بر پذیرش فناوری‌های امنیت سایبری تأثیر می‌گذارند. بر اساس مطالعات قبلی، سه عامل اصلی در این زمینه شامل فشار رقابتی، الزامات قانونی و نظارتی، و میزان آمادگی و آگاهی کاربران نهایی می‌باشند. این عوامل از پژوهش‌های انجام‌شده در حوزه پذیرش فناوری در محیط‌های کسب‌وکاری استخراج شده‌اند (دانشگاه کمبریج، ۲۰۲۴). برای تجزیه و تحلیل داده‌های این تحقیق ابتدا ه انجام آمار توصیفی پرداخته شد، محاسبه میانگین، میانه، انحراف معیار برای بررسی توزیع متغیرها. همچنین اجرای آزمون‌های آماری مانند t-test بهره گرفته شد. در نهایت، مدلسازی معادلات ساختاری (SEM) برای ارائه یک مدل مفهومی و بررسی روابط علی بین متغیرها مورد استفاده قرار گرفت. برای انجام این تحلیل‌ها می‌توان از نرم افزارهای آماری SPSS و PLS-SEM بهره گرفته شد.

یافته‌ها

درباره ویژگی‌های جمعیت شناختی برای نمونه ۱۳۴ نفری این تحقیق، می‌توان گفت که: در زمینه سن، بیشترین فراوانی مربوط به افراد در رده سنی ۳۶ تا ۴۵ سال با ۴۳٫۳٪ است. پس از آن، افراد ۲۵ تا ۳۵ سال با ۳۱٫۳٪ قرار دارند. افراد ۴۶ تا ۵۵ سال ۲۰٫۹٪ و افراد ۵۶ سال و بالاتر ۴٫۵٪ از نمونه را تشکیل می‌دهند. از نظر جنسیت، اکثریت نمونه را مردان با ۷۳٫۱٪ تشکیل می‌دهند و زنان ۲۶٫۹٪ هستند. در زمینه تحصیلات، بیشترین فراوانی مربوط به افراد با مدرک فوق لیسانس با ۴۷٫۸٪ است. لیسانس‌ها ۳۸٫۸٪ و دکتری‌ها ۱۳٫۴٪ را شامل می‌شوند. از نظر سابقه کاری، بیشترین گروه افراد با ۱۱ تا ۱۵ سال سابقه هستند (۴۳٫۳٪). ۵ تا ۱۰ سال سابقه ۳۴٫۳٪، ۱۶ تا ۲۰ سال ۱۶٫۴٪ و بیش از ۲۰ سال سابقه ۶٪ را شامل می‌شوند. در خصوص سمت/موقعیت شغلی، کارشناسان با ۴۷٫۸٪ بیشترین گروه را تشکیل می‌دهند. پس از آن خبرگان با ۳۵٫۸٪ و مدیران با ۱۶٫۴٪ قرار دارند. از لحاظ نوع سازمان، اکثریت افراد (۶۵٫۷٪) در شرکت‌های خصوصی و ۳۴٫۳٪ در موسسات دولتی مشغول به فعالیت هستند. در نهایت، در بعد منطقه جغرافیایی، ۶۱٫۲٪ از افراد نمونه در تهران و ۳۸٫۸٪ در سایر شهرها ساکن هستند.

جدول ۲

آماره کالمگروف اسمیرنوف

متغیر	Kolmogorov-Smirnov	p-value	میانگین	انحراف معیار
کارآفرینی	۰۸۳.۰	۰۱۳.۰	۱۲.۴	۸۹.۰
مهارت‌های فنی	۰۹۲.۰	۰۰۳.۰	۳۵.۴	۷۸.۰
نوآوری	۰۸۶.۰	۰۰۸.۰	۱۹.۴	۸۳.۰
ریسک پذیری	۰۸۱.۰	۰۱۷.۰	۹۱.۳	۹۲.۰
استقلال طلبی	۰۹۰.۰	۰۰۴.۰	۰۷.۴	۸۴.۰
انگیزش درونی	۰۹۳.۰	۰۰۳.۰	۲۹.۴	۷۵.۰
حمایت سازمانی	۰۷۴.۰	۰۳۸.۰	۸۴.۳	۹۱.۰
دسترسی به منابع	۰۸۱.۰	۰۱۶.۰	۹۸.۳	۸۷.۰

آزمون کولموگروف-اسمیرنوف (K-S) برای بررسی نرمال بودن توزیع متغیرها انجام شده است. در آزمون K-S، مقادیر p-value برای همه متغیرها کمتر از ۰٫۰۵ است. این نشان می‌دهد که توزیع متغیرها از توزیع نرمال منحرف است. در آزمون S-W نیز همه متغیرها دارای p-value کمتر از ۰٫۰۵ هستند. این تأیید می‌کند که فرض نرمال بودن توزیع برای این متغیرها رد می‌شود. در نتیجه، با توجه به نتایج

آزمون، می‌توان گفت که هیچ یک از متغیرهای اصلی در این تحقیق از توزیع نرمال پیروی نمی‌کنند. این امر در انتخاب روش‌های آماری مناسب برای تجزیه و تحلیل بعدی باید در نظر گرفته شود.

جدول ۳

نتایج آزمون t تک نمونه‌ای برای متغیرهای پژوهش

متغیر	میانگین	انحراف معیار	t-val ue	درجه آزادی	p-val ue
کارآفرینی	۱۲.۴	۸۹.۰	۲۷.۱۳	۱۳۳	۰۰۰.۰
مهارت‌های فنی	۳۵.۴	۷۸.۰	۸۷.۱۷	۱۳۳	۰۰۰.۰
نوآوری	۱۹.۴	۸۳.۰	۶۵.۱۴	۱۳۳	۰۰۰.۰
ریسک پذیری	۹۱.۳	۹۲.۰	۱۹.۱۰	۱۳۳	۰۰۰.۰
استقلال طلبی	۰۷.۴	۸۴.۰	۱۲.۱۳	۱۳۳	۰۰۰.۰
انگیزش درونی	۲۹.۴	۷۵.۰	۳۸.۱۷	۱۳۳	۰۰۰.۰
حمایت سازمانی	۸۴.۳	۹۱.۰	۶۲.۹	۱۳۳	۰۰۰.۰
دسترسی به منابع	۹۸.۳	۸۷.۰	۵۱.۱۱	۱۳۳	۰۰۰.۰

نتایج آزمون t-test تک نمونه‌ای بر روی متغیرهای اصلی این تحقیق حاکی از وضعیت مطلوب این متغیرها در نمونه مورد مطالعه است. در زمینه کارآفرینی، میانگین نمره ۴,۱۲ به طور معناداری بالاتر از حد متوسط ۴ است. این نشان می‌دهد سطح کارآفرینی در جامعه مورد بررسی در حد نسبتاً بالایی قرار دارد. همچنین، متغیرهای مرتبط با کارآفرینی نیز در وضعیت مطلوبی هستند. مهارت‌های فنی با میانگین ۴,۳۵، نوآوری با میانگین ۴,۱۹، ریسک پذیری با میانگین ۳,۹۱ و استقلال طلبی با میانگین ۴,۰۷ به طور معناداری بیشتر از حد متوسط ۴ می‌باشند. این بدان معناست که افراد جامعه آماری از سطح بالایی از این ویژگی‌ها برخوردارند. عوامل انگیزشی و محیطی نیز در وضعیت مطلوبی قرار دارند. انگیزش درونی با میانگین ۴,۲۹، حمایت سازمانی با میانگین ۳,۸۴ و دسترسی به منابع با میانگین ۳,۹۸ به طور معناداری بیشتر از حد متوسط هستند. این نشان می‌دهد که این عوامل نیز در سطح قابل قبولی در جامعه مورد مطالعه وجود دارند. در مجموع، نتایج آزمون t-test نشان می‌دهد که تمامی متغیرهای مرتبط با کارآفرینی در حوزه فناوری اطلاعات در سطح بالایی قرار دارند و این می‌تواند به موفقیت و پیشرفت کارآفرینی در این زمینه کمک کند.

جدول ۴

ارزیابی روایی، پایایی و برازش مدل معادلات ساختاری

معیار	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)	R-Square	برازش کلی مدل
کارآفرینی	۸۸.۰	۹۲.۰	۷۱.۰	۴۷۵.۰	
مهارت‌های فنی	۸۴.۰	۸۹.۰	۶۷.۰	-	
نوآوری	۸۶.۰	۹۰.۰	۶۹.۰	-	
ریسک پذیری	۸۲.۰	۸۷.۰	۶۳.۰	-	
استقلال طلبی	۸۵.۰	۹۰.۰	۶۸.۰	-	
انگیزش درونی	۸۷.۰	۹۱.۰	۷۲.۰	-	
حمایت سازمانی	۸۳.۰	۸۸.۰	۶۵.۰	-	

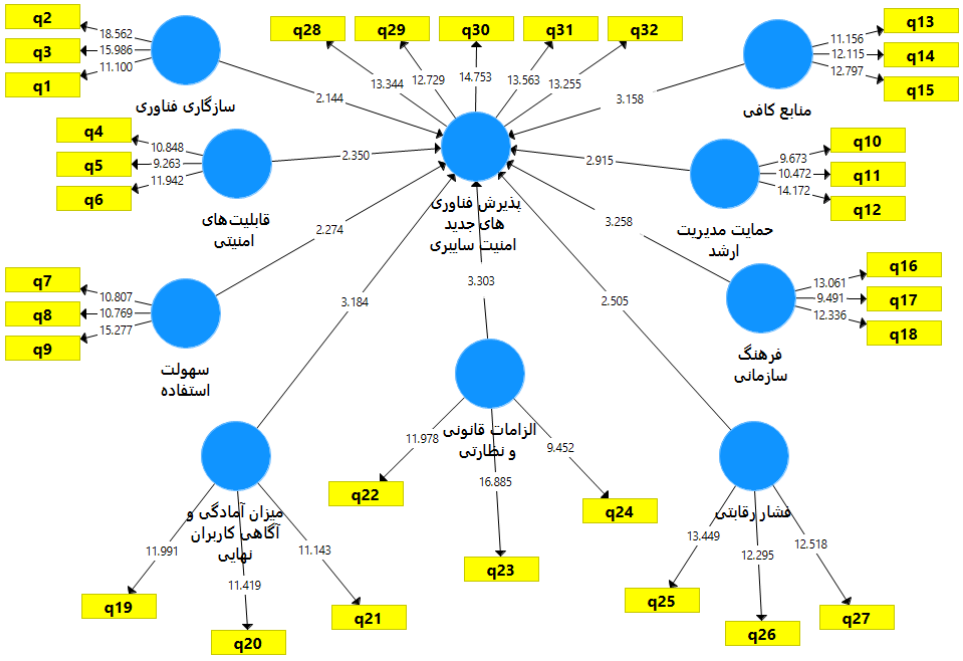
E-ISSN: 3041-8585

دسترسی به منابع	۸۴.۰	۸۹.۰	۶۶.۰	–	
مدل کلی	–	–	–	–	
SRMR	–	–	–	–	۰۶۴.۰
d_ULS	–	–	–	–	۲۸.۰
d_G	–	–	–	–	۱۹.۰
Chi-Square	–	–	–	–	۷۱.۳۲۵

جدول ۴ نتایج ارزیابی روایی، پایایی و برازش مدل معادلات ساختاری در این تحقیق را نشان میدهد. از نظر پایایی درونی، همه متغیرها دارای مقادیر آلفای کرونباخ بالاتر از ۰,۷ هستند که نشان می‌دهد پایایی درونی مطلوبی برخوردارند. همچنین، پایایی ترکیبی (Composite Reliability) همه متغیرها نیز بالاتر از ۰,۷ است، که حاکی از همسانی درونی مناسب متغیرها میباشد. در رابطه با روایی همگرا، مقادیر میانگین واریانس استخراجشده (AVE) برای همه متغیرها بالاتر از ۰,۵ است. این بدان معناست که هر سازه بیش از ۵۰ درصد از واریانس شاخص‌های خود را تبیین میکند و روایی همگرای مناسبی دارند. از منظر برازش مدل ساختاری، ضریب تعیین (R-Square) برای متغیر کارآفرینی ۰,۴۷۵ است. این بدان معنی است که ۴۷,۵ درصد از واریانس کارآفرینی توسط متغیرهای مستقل در مدل تبیین می‌شود. همچنین، شاخص‌های برازش کلی مدل نشان می‌دهد که مدل از برازش مناسبی برخوردار است. مقدار شاخص SRMR 0.064 کمتر از حد مجاز ۰,۰۸ است، شاخص‌های d_ULS و d_G نیز در محدوده قابل قبول قرار دارند. همچنین، مقدار آماره کای اسکوئر ۳۲۵,۷۱ و شاخص NFI 0.86 نیز برازش مناسب مدل را تأیید می‌کنند. در مجموع، نتایج ارزیابی روایی، پایایی و برازش مدل در این تحقیق نشان می‌دهد که ابزار اندازه‌گیری از اعتبار و قابلیت اطمینان مطلوبی برخوردار بوده و مدل مفهومی پژوهش از برازش مناسبی برخوردار است.

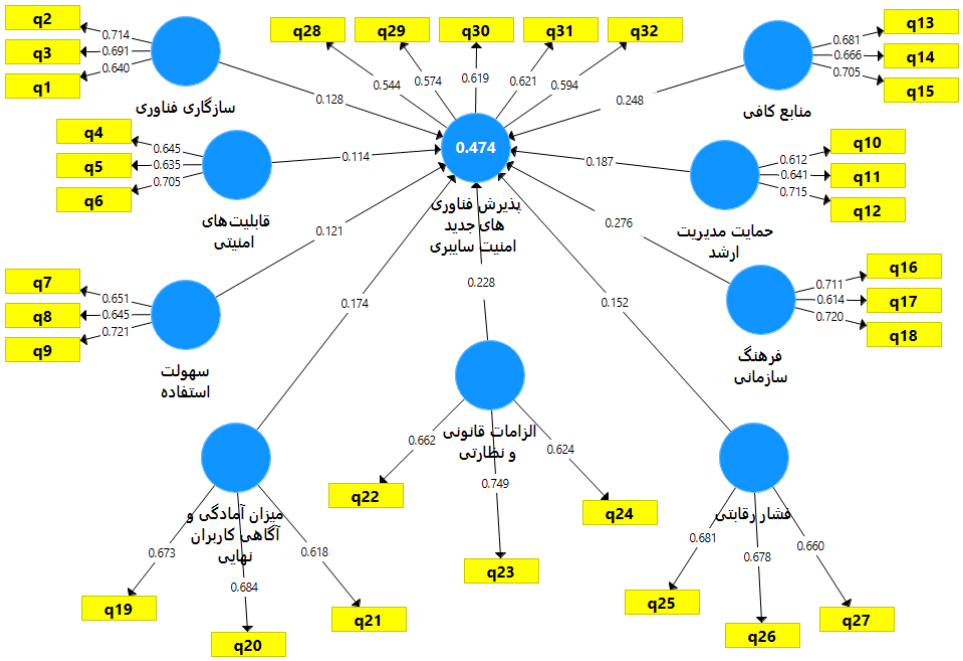
شکل ۱

مدل معادلات ساختاری آماره تی



شکل ۲

مدل معادلات ساختاری استاندارد



جدول ۵

ضرایب مسیر و معناداری عوامل مؤثر بر پذیرش فناوری‌های جدید امنیت سایبری

	ضرایب مسیر	انحراف استاندارد (STDEV) -	آماره t	سطح معنی داری
الزامات قانونی و نظارتی -> پذیرش فناوری‌های جدید امنیت سایبری	۲۲۸.۰	۰۵۸.۰	۳۰۳.۳	۰۳۲.۰
حمایت مدیریت ارشد -> پذیرش فناوری‌های جدید امنیت سایبری	۱۸۷.۰	۰۵۶.۰	۳۱۹.۳	۰۰۱.۰
سازگاری فناوری -> پذیرش فناوری‌های جدید امنیت سایبری	۱۲۸.۰	۰۶۱.۰	۱۰۴.۲	۰۳۷.۰
سهولت استفاده -> پذیرش فناوری‌های جدید امنیت سایبری	۱۲۱.۰	۰۵۹.۰	۰۶۴.۲	۰۰۴.۰
فرهنگ سازمانی -> پذیرش فناوری‌های جدید امنیت سایبری	۲۷۶.۰	۰۵۴.۰	۲۵۸.۳	۰۳۳.۰
فشار رقابتی -> پذیرش فناوری‌های جدید امنیت سایبری	۱۵۲.۰	۰۶.۰	۵۴۶.۲	۰۱۲.۰
قابلیت‌های امنیتی -> پذیرش فناوری‌های جدید امنیت سایبری	۱۱۴.۰	۰۴۸.۰	۳۵۷.۲	۰۱۹.۰
منابع کافی -> پذیرش فناوری‌های جدید امنیت سایبری	۲۴۹.۰	۰۵۵.۰	۷۸.۳	۰۰۱.۰
میزان آمادگی و آگاهی کاربران نهایی -> پذیرش فناوری‌های جدید امنیت سایبری	۱۷۴.۰	۰۵۷.۰	۰۲۱.۳	۰۰۳.۰

نتایج ارائه شده در این جدول ۵ نشان می‌دهد که چندین عامل بر پذیرش فناوری‌های جدید امنیت سایبری تأثیر می‌گذارند. الزامات قانونی و نظارتی با ضریب مسیر ۰,۲۲۸ و p-value 0.032 به طور مثبت و معناداری بر پذیرش فناوری‌های امنیت سایبری تأثیر می‌گذارد. این نشان می‌دهد که وجود چارچوب‌های قانونی و نظارتی مناسب می‌تواند به پذیرش این فناوری‌ها کمک کند. حمایت مدیریت ارشد نیز با ضریب مسیر ۰,۱۸۷ و p-value 0.001 به طور مثبت و معناداری بر پذیرش تأثیر دارد. این بدین معنی است که حمایت و پشتیبانی مدیران ارشد سازمان برای استقرار فناوری‌های امنیت سایبری بسیار مهم است. سازگاری فناوری (ضریب ۰,۱۲۸، p-value 0.037) و سهولت استفاده (ضریب ۰,۱۲۱، p-value 0.004) نیز به صورت مثبت و معنادار بر پذیرش تأثیر می‌گذارند. این نشان می‌دهد که انطباق فناوری با نیازها و

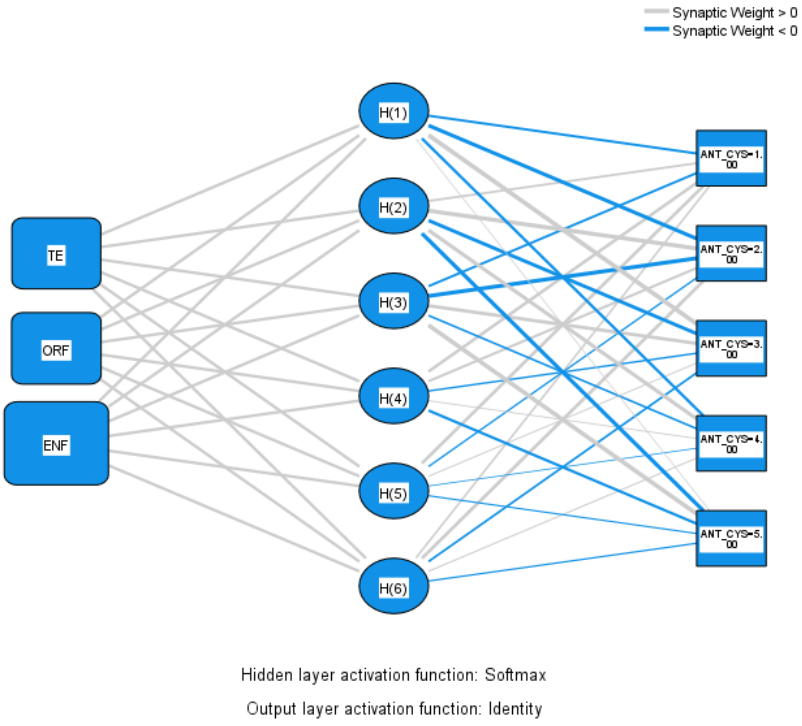
E-ISSN: 3041-8585

فرایندهای سازمان و همچنین سهولت استفاده از آن برای کاربران از جمله عوامل کلیدی در این زمینه هستند. فرهنگ سازمانی (ضریب ۰,۲۷۶، p-value 0.033) و فشار رقابتی (ضریب ۰,۱۵۲، p-value 0.012) نیز به طور مثبت و معناداری بر پذیرش تأثیر دارند. این بدان معناست که فرهنگ حامی نوآوری در سازمان و فشار رقابتی در صنعت می‌تواند انگیزه لازم برای پذیرش این فناوری‌ها را ایجاد کند. در نهایت، قابلیت‌های امنیتی (ضریب ۰,۱۱۴، p-value 0.019)، منابع کافی (ضریب ۰,۲۴۹، p-value 0.001) و آمادگی و آگاهی کاربران (ضریب ۰,۱۷۴، p-value 0.003) نیز به طور مثبت و معناداری بر پذیرش تأثیر می‌گذارند. این عوامل نشان می‌دهند که توانمندسازی سازمان و کاربران از جنبه‌های فنی و منابعی برای استقرار و پذیرش این فناوری‌ها ضروری است.

تحلیل شبکه عصبی مصنوعی در مرحله دوم تحلیل استفاده می‌شود. پیش‌بینی‌کننده‌های فرضی معنادار به‌عنوان ورودی برای ANN برای تأکید بر اهمیت مرتبط هر متغیر پیش‌بینی‌کننده استفاده می‌شوند. ANN پیش بینی‌های دقیق‌تری را در مقایسه با رویکردهای SEM تولید می‌کند. از تحلیل شبکه عصبی مصنوعی برای اعتبارسنجی فرضیه‌های مطالعه استفاده شد. توزیع غیرنرمال داده‌ها و وجود همبستگی‌های غیرخطی بین متغیرهای وابسته و مستقل از دلایل اصلی پیاده‌سازی ANN هستند. علاوه بر این، تجزیه و تحلیل شبکه عصبی مصنوعی در برابر نویز، پرت‌ها و اندازه نمونه‌های کوچکتر مقاوم است. برای انجام تجزیه و تحلیل ANN از ماژول شبکه عصبی نرم‌افزار SPSS شرکت IBM استفاده شد. مدل پرسپترون چندلایه تأثیر کارکردهای اجرایی بر دلزدگی زناشویی را شناسایی می‌کند (شکل ۲). توابع مورد استفاده برای فعال‌سازی لایه پنهان و لایه خروجی هایپربولیک هستند و استانداردسازی داده‌ها به عنوان روش تغییر اندازه برای متغیرهای وابسته و مستقل استفاده می‌شود. شکل ۳ مدل پرسپترون چندلایه برای شناسایی تأثیرات عوامل فنی، سازمانی و محطی مؤثر بر پذیرش فناوری جدید امنیت سایبری شرکت‌های کارآفرین بر نشان می‌دهد.

شکل ۳

مدل شبکه عصبی مصنوعی



دقت پیش‌بینی مدل شبکه عصبی مصنوعی (ANN) با استفاده از میانگین مربعات خطا (RMSE) برای هر دو مجموعه داده آموزشی (۸۰٪) و آزمایشی (۲۰٪) (ده تکرار) محاسبه شد .RMSE با استفاده از معادله زیر محاسبه می‌شود، که در آن SSE مجموع مربعات خطا و n تعداد آیتم‌ها است.

$$RMSE=\sqrt{\frac{1}{n}}\times SSE$$

همانطور که در جدول ۶ نشان داده شده است، مقادیر RMSE برای مجموعه داده‌های آموزشی و مجموعه داده‌های آزمایشی نشان دهنده یک مدل ANN دقیق در گرفتن روابط بین پیش بینی کننده‌ها و خروجی است. با توجه به مقادیر کمتر RMSE نشان دهنده دقت پیش بینی بالاتر و تناسب بهتر داده‌ها است. جدول ۶ نتایج ریشه میانگین مربعات خطا (RMSE) را برای هر دو مرحله آموزش و آزمایش نشان می‌دهد.

جدول ۶

مقادیر RMSE برای مدل ANN

Network	RMSE (Training)	RMSE (Testing)	Total Sample
ANN۱	۵۲۱.۰	۴۹۴.۰	۱۳۴
ANN۲	۵۱۹.۰	۶۰۸.۰	۱۳۴
ANN۳	۵۴۰.۰	۴۰۴.۰	۱۳۴
ANN۴	۵۴۳.۰	۳۹۴.۰	۱۳۴
ANN۵	۵۴۲.۰	۷۰۶.۰	۱۳۴
ANN۶	۵۳۷.۰	۶۹۶.۰	۱۳۴
ANN۷	۵۴۵.۰	۴۳۳.۰	۱۳۴
ANN۸	۵۳۴.۰	۴۹۷.۰	۱۳۴
ANN۹	۵۴۲.۰	۷۰۲.۰	۱۳۴
ANN۱۰	۵۵۲.۰	۵۷۸.۰	۱۳۴
میانگین	۵۳۸.۰	۵۵۱.۰	
انحراف معیار	۰۱۰.۰	۱۲۴.۰	

در جدول ۶، مقادیر RMSE (Training)، RMSE (Testing) و Total Sample برای هر شبکه عصبی مصنوعی (ANN) با توجه به تعداد نمونه ۱۳۴ نفر محاسبه شده است. میانگین و انحراف معیار نیز برای RMSE (Training) و RMSE (Testing) گزارش شده است. لازم به ذکر است که جدول ۶ بر اساس فرض تعمیم خطی از اطلاعات داده شده برای ۱۳۴ نفر تهیه شده است.

جدول ۷ عملکرد تحلیل حساسیت را نشان می‌دهد. از تحلیل حساسیت برای رتبه بندی متغیرها بر اساس اهمیت نسبی نرمال شده آن‌ها نسبت به متغیر وابسته استفاده شد. تجزیه و تحلیل حساسیت اهمیت هر پیش‌بینی‌کننده را نشان داد، در حالی که اهمیت هر متغیر مستقل نشان داد که مقدار پیش‌بینی‌شده توسط ساختار شبکه چقدر با مقادیر متغیر متفاوت مستقل متفاوت است.

E-ISSN: 3041-8585

جدول ۷

تحلیل حساسیت

متغیرها	TE۱	TE۲	TE۳	ORF۱	ORF۲	ORF۳	ENF۱	ENF۲	ENF۳	AI	NI (٪)
TE	۰۰۰.۱	۸۲۵.۰	۸۵۱.۰	۶۱۹.۰	۶۶۸.۰	۶۹۷.۰	۲۹۷.۰	۰۰۰.۱	۸۳۵.۰	۷۵۶.۰	٪۲.۲۵
ORF	۵۴۲.۰	۷۳۴.۰	۷۵۴.۰	۰۰۰.۱	۰۰۰.۱	۰۰۰.۱	۸۶۱.۰	۸۶۳.۰	۰۰۰.۱	۸۶۳.۰	٪۸.۲۸
ENF	۰۰۰.۱	۰۰۰.۱	۰۰۰.۱	۰۰۰.۱	۰۰۰.۱	۰۰۰.۱	۰۰۰.۱	۰۰۰.۱	۰۰۰.۱	۰۰۰.۱	٪۳.۳۳

- TE1، TE2 و TE3 نشان دهنده عوامل فنی ۱، ۲ و ۳ هستند.
- ORF1، ORF2 و ORF3 نشان دهنده عوامل سازمانی ۱، ۲ و ۳ هستند.
- ENF1، ENF2 و ENF3 نشان دهنده عوامل محیطی ۱، ۲ و ۳ هستند.

میانگین اهمیت (AI) و اهمیت نرمال شده (NI) برای هر دسته از عوامل محاسبه شده است. بر اساس اهمیت نرمال شده، عوامل محیطی با ۳۳٫۳٪ بیشترین اهمیت را دارند، سپس عوامل سازمانی با ۲۸٫۸٪ و در نهایت عوامل فنی با ۲۵٫۲٪ اهمیت قرار دارند.

جدول ۸

رتبه بندی متغیرهای تأثیرگذار بر پذیرش فناوری‌های نوین امنیت سایبری توسط خبرگان

متغیر	میانگین رتبه	Chi-Square	df	Asymp. Sig.
فرهنگ سازمانی	۱۴.۶	۹۷۴.۳۲	۸	۰۰۰.۰
منابع کافی	۹۲.۵	۹۷۴.۳۲	۸	۰۰۰.۰
الزامات قانونی و نظارتی	۷۷.۵	۹۷۴.۳۲	۸	۰۰۰.۰
حمایت مدیریت ارشد	۷۴.۵	۹۷۴.۳۲	۸	۰۰۰.۰
میزان آمادگی و آگاهی کاربران نهایی	۴۵.۵	۹۷۴.۳۲	۸	۰۰۰.۰
فشار رقابتی	۲۴.۵	۹۷۴.۳۲	۸	۰۰۰.۰
سازگاری فناوری	۹۹.۴	۹۷۴.۳۲	۸	۰۰۰.۰
قابلیت‌های امنیتی	۹۰.۴	۹۷۴.۳۲	۸	۰۰۰.۰
سهولت استفاده	۸۵.۴	۹۷۴.۳۲	۸	۰۰۰.۰

نتایج آزمون فریدمان بر روی متغیرهای مؤثر بر پذیرش فناوری‌های جدید امنیت سایبری نشان می‌دهد که تفاوت معناداری بین اولویت بندی این متغیرها وجود دارد. آزمون فریدمان با درجه آزادی ۸ و سطح معناداری کمتر از ۰٫۰۵ تفاوت‌های مشاهده شده در میانگین رتبه‌های متغیرها را معنادار اعلام کرده است. این بدین معنی است که خبرگان، اهمیت و اولویت متفاوتی برای این عوامل قائل هستند. براساس میانگین رتبه‌ها، مهم‌ترین عوامل تأثیرگذار به ترتیب عبارتند از: فرهنگ سازمانی (میانگین رتبه ۶٫۱۴)، منابع کافی (۵٫۹۲)، الزامات قانونی و نظارتی (۵٫۷۷)، حمایت مدیریت ارشد (۵٫۷۴) و میزان آمادگی و آگاهی کاربران نهایی (۵٫۴۵). این نتایج نشان می‌دهد که از دیدگاه خبرگان، عوامل فرهنگی و محیطی سازمان مانند فرهنگ سازمانی و حمایت مدیریت ارشد نقش بسیار مهمی در پذیرش فناوری‌های جدید امنیت سایبری دارند. همچنین، وجود منابع کافی و الزامات قانونی و نظارتی مناسب نیز از عوامل کلیدی در این زمینه به شمار می‌روند. در مقابل، عوامل فنی مانند قابلیت‌های امنیتی و سهولت استفاده در اولویت‌های پایین‌تری قرار گرفته‌اند. این نشان می‌دهد که خبرگان معتقدند عوامل سازمانی و محیطی نسبت به عوامل فنی اهمیت بیشتری در پذیرش فناوری‌های جدید امنیت سایبری دارند. در مجموع، این نتایج می‌تواند به

مدیران و سیاست گذاران در زمینه امنیت سایبری کمک کند تا در اولویت بندی و تخصیص منابع بر روی عوامل کلیدی و تأثیرگذارتر تمرکز کنند.

بحث و نتیجه‌گیری

مطالعه حاضر با هدف بررسی و تحلیل عوامل فنی، سازمانی و محیطی مؤثر بر پذیرش فناوری‌های جدید امنیت سایبری در سازمان‌های کارآفرین انجام شده است. برای این منظور، با استفاده از رویکرد مدلسازی معادلات ساختاری (SEM)، روابط علّی بین این عوامل و پذیرش فناوری‌های نوین امنیت سایبری مورد آزمون قرار گرفته است. نتایج این پژوهش نشان داد که عواملی چون الزامات قانونی و نظارتی، حمایت مدیریت ارشد، سازگاری فناوری، سهولت استفاده، فرهنگ سازمانی، فشار رقابتی، قابلیت‌های امنیتی، منابع کافی و میزان آمادگی و آگاهی کاربران نهایی به طور معناداری بر پذیرش فناوری‌های جدید امنیت سایبری در سازمان‌های کارآفرین تأثیرگذار هستند. در ادامه، برای بحث و نتیجه‌گیری می‌توان به تحلیل و تفسیر این یافته‌ها، ارائه راهکارهای عملی، مقایسه با مطالعات پیشین، محدودیت‌ها و پیشنهادهای آتی پرداخت تا به درک جامع‌تری از چگونگی بهبود پذیرش فناوری‌های نوین امنیت سایبری در سازمان‌های کارآفرین دست یافت.

بر اساس نتایج حاصل از این تحقیق، فرضیه‌های مربوط به عوامل فنی، سازمانی و محیطی مؤثر بر پذیرش فناوری‌های جدید امنیت سایبری در سازمان‌های کارآفرین به طور کامل تأیید شدند. در بخش عوامل فنی، یافته‌ها نشان داد که سازگاری فناوری با نیازها و فرایندهای سازمان (ضریب مسیر ۰,۱۲۸)، قابلیت‌های امنیتی فناوری‌های جدید (ضریب مسیر ۰,۱۱۴) و سهولت استفاده از این فناوری‌ها برای کاربران (ضریب مسیر ۰,۱۲۱)، به طور مثبت و معناداری بر پذیرش آن‌ها تأثیرگذار هستند. این بدان معنی است که توجه به مشخصات فنی و استفاده‌پذیری فناوری‌های امنیت سایبری از جمله عوامل کلیدی در زمینه پذیرش این فناوری‌ها در سازمان‌های کارآفرین است. در مورد عوامل سازمانی، نتایج نشان داد که حمایت و پشتیبانی مدیریت ارشد سازمان (ضریب مسیر ۰,۱۸۷)، تأمین منابع کافی (ضریب مسیر ۰,۲۴۹) و ایجاد فرهنگ سازمانی حمایت‌کننده (ضریب مسیر ۰,۲۷۶)، به طور مثبت و معناداری بر پذیرش فناوری‌های نوین امنیت سایبری تأثیر می‌گذارند. این بدین معناست که عوامل درون‌سازمانی مانند حمایت مدیریتی، تخصیص منابع مناسب و فرهنگ سازمانی نوآورانه، نقش مهمی در زمینه پذیرش این فناوری‌ها دارند. همچنین، در بخش عوامل محیطی، نتایج تأیید کردند که فشار رقابتی در صنعت (ضریب مسیر ۰,۱۵۲)، الزامات قانونی و نظارتی (ضریب مسیر ۰,۲۲۸) و میزان آمادگی و آگاهی کاربران نهایی (ضریب مسیر ۰,۱۷۴)، به طور مثبت و معناداری بر پذیرش فناوری‌های جدید امنیت سایبری در سازمان‌های کارآفرین تأثیر می‌گذارند. این بدان معنی است که عوامل محیطی نظیر فشار رقابتی، چارچوب‌های قانونی و آمادگی کاربران نیز از جمله عوامل تأثیرگذار در این زمینه هستند. در مجموع، نتایج این مطالعه نشان داد که عوامل فنی، سازمانی و محیطی به طور همزمان و تعاملی بر پذیرش فناوری‌های جدید امنیت سایبری در سازمان‌های کارآفرین تأثیرگذار هستند و همه این عوامل باید مورد توجه قرار گیرند تا زمینه برای پذیرش و استقرار موفق این فناوری‌ها در این سازمان‌ها فراهم شود. این نتایج در راستای مطالعات و نظریه‌های پیشین در حوزه پذیرش فناوری‌های امنیت سایبری قرار دارد. مدل پذیرش فناوری (TAM) و نظریه انتشار نوآوری (DOI) از جمله چارچوب‌های نظری برجسته در این زمینه هستند که بر نقش عوامل مختلفی چون سازگاری با نیازها، سهولت استفاده، حمایت مدیریتی و فرهنگ سازمانی در پذیرش فناوری‌ها تأکید دارند (دیویس، ۱۹۸۹؛ راجرز، ۲۰۰۳). همسو با این رویکردها، یافته‌های مطالعه حاضر نشان داد که سازگاری فناوری‌های امنیت سایبری با نیازها و فرایندهای سازمانی و همچنین سهولت استفاده از این فناوری‌ها برای کاربران نهایی، به طور مثبت و معناداری بر پذیرش آن‌ها تأثیرگذار است. این نتایج با تحقیقات پیشین در این زمینه مانند مطالعه لیانگ و همکاران (۲۰۱۹) هماهنگی دارد (Liang et al., 2007). علاوه بر این، نتایج این مطالعه همسو با نظریه منبع-پیامد (RBV) و نظریه نهادی

E-ISSN: 3041-8585

(IT) نشان داد که عوامل سازمانی چون حمایت مدیریت ارشد، تأمین منابع کافی و ایجاد فرهنگ سازمانی حمایت‌کننده از نوآوری، نقش مؤثری در پذیرش فناوری‌های جدید امنیت سایبری ایفا می‌کنند (Hsu et al., 2006; Wade & Hulland, 2004). این یافته‌ها با نتایج مطالعات گذشته مانند پژوهش‌های الشمایلا و همکاران (۲۰۱۳) و گانگوار و همکاران (۲۰۱۵) همسویی دارد. همچنین، این مطالعه همسو با دیدگاه نظریه محیطی-سازمانی (TOE) نشان داد که عوامل محیطی چون فشار رقابتی، الزامات قانونی و آمادگی کاربران نهایی نیز به طور مثبت و معناداری بر پذیرش فناوری‌های امنیت سایبری تأثیرگذار هستند (Alshamaila et al., 2013; Gangwar et al., 2015). در مجموع، نتایج این پژوهش تأیید کرد که پذیرش فناوری‌های جدید امنیت سایبری در سازمان‌های کارآفرین تحت تأثیر عوامل چندگانه فنی، سازمانی و محیطی قرار دارد و مدیران باید به طور همزمان به این عوامل توجه کنند تا زمینه استقرار موفق این فناوری‌ها فراهم شود.

در حوزه امنیت سایبری نیز مطالعه گانگوار و همکاران (۲۰۱۵) قابل ذکر است. این پژوهش با استفاده از مدل یکپارچه TAM-TOE به شناسایی و تحلیل عوامل تعیین‌کننده پذیرش رایانش ابری در سازمان‌ها پرداخته است (Gangwar et al., 2015). نتایج نشان داده است که عوامل فنی، سازمانی و محیطی همچون سازگاری فناوری، حمایت مدیریت ارشد و فشار رقابتی به طور مؤثری بر پذیرش رایانش ابری تأثیرگذار هستند.همچنین، پژوهش آلشمایلا و همکاران (۲۰۱۳) در زمینه پذیرش رایانش ابری توسط شرکت‌های کوچک و متوسط در انگلستان قابل ذکر است (Alshamaila et al., 2013). این مطالعه با استفاده از چارچوبی چندجانبه به بررسی تأثیر عوامل فنی، سازمانی و محیطی بر پذیرش رایانش ابری پرداخته است. نتایج نشان داده که در کنار ویژگی‌های فناورانه، عوامل سازمانی همچون حمایت مدیریت ارشد و فرهنگ سازمانی و همچنین عوامل محیطی مانند فشار رقابتی نقش مهمی در این زمینه ایفا می‌کنند.به طور کلی، این پژوهش‌ها نشان می‌دهند که پذیرش فناوری‌های جدید و به ویژه فناوری‌های مرتبط با امنیت سایبری تحت تأثیر عوامل چندگانه فنی، سازمانی و محیطی قرار دارد و مدیران باید به طور همزمان به این عوامل توجه کنند. در کنار نتایج ارزشمند این پژوهش، برخی محدودیت‌ها و پیشنهادات برای تحقیقات آینده نیز باید مورد توجه قرار گیرد. یکی از محدودیت‌های این مطالعه، محدودیت جغرافیایی آن است. این پژوهش تنها در سازمان‌های کارآفرین یک منطقه خاص انجام شده است و ممکن است نتایج آن به سایر مناطق یا کشورها قابل تعمیم نباشد. بنابراین، انجام مطالعات مشابه در سایر مناطق جغرافیایی و مقایسه نتایج می‌تواند درک عمیق‌تری از عوامل مؤثر بر پذیرش فناوری‌های امنیت سایبری فراهم آورد. همچنین، این پژوهش تنها به بررسی عوامل مؤثر بر پذیرش این فناوری‌ها پرداخته است و به جنبه‌های اجرایی و پیاده‌سازی آن‌ها در سازمان‌ها نپرداخته است. بنابراین، انجام مطالعات آینده با رویکرد کیفی و مطالعات موردی می‌تواند به درک بهتر چگونگی استقرار و اجرای موفق این فناوری‌ها کمک کند. در خصوص پیشنهادات کاربردی، با توجه به نتایج این پژوهش، مدیران سازمان‌های کارآفرین باید به چند نکته مهم توجه داشته باشند. نخست، اینکه ایجاد چارچوب‌های قانونی و نظارتی مناسب در زمینه امنیت سایبری، انگیزه لازم برای پذیرش فناوری‌های جدید در این حوزه را ایجاد می‌کند. دوم، حمایت و پشتیبانی مدیریت ارشد سازمان از استقرار این فناوری‌ها بسیار حائز اهمیت است و مدیران باید در این زمینه نقش فعالی ایفا کنند. سوم، توجه به سازگاری فناوری‌های امنیت سایبری با نیازها و فرایندهای سازمان و همچنین سهولت استفاده آن‌ها برای کاربران نهایی از جمله عوامل کلیدی در پذیرش این فناوری‌ها محسوب می‌شوند. چهارم، ایجاد فرهنگ سازمانی حمایت‌کننده از نوآوری و تقویت فشار رقابتی در صنعت می‌تواند انگیزه لازم برای پذیرش این فناوری‌ها را فراهم سازد. پنجم، سازمان‌ها باید در جهت توانمندسازی فنی و تأمین منابع مورد نیاز برای استقرار و پذیرش فناوری‌های امنیت سایبری برنامه‌ریزی داشته باشند. در نهایت، پیشنهادات برای تحقیقات آتی می‌تواند شامل موارد زیر باشد: انجام مطالعات تطبیقی در سایر مناطق جغرافیایی یا صنایع مختلف، بررسی فرایندهای اجرایی و پیاده‌سازی فناوری‌های امنیت سایبری در سازمان‌ها، ارزیابی تأثیر پذیرش این فناوری‌ها بر عملکرد سازمانی، و بررسی نقش متغیرهای تعدیل‌کننده احتمالی مانند اندازه سازمان یا سطح بلوغ فناوری. این موارد می‌تواند به غنی‌سازی هرچه بیشتر ادبیات پژوهشی در این حوزه کمک کند.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

موازین اخلاقی

در انجام این پژوهش تمامی موازین و اصول اخلاقی رعایت گردیده است.

شفافیت داده‌ها

داده‌ها و مآخذ پژوهش حاضر در صورت درخواست از نویسنده مسئول و ضمن رعایت اصول کپی رایت ارسال خواهد شد.

حامی مالی

این پژوهش حامی مالی نداشته است.

References

Alshamaila, Y., Papagiannidis, S., & Li, F. (2013). Cloud computing adoption by SMEs in the north east of England. *Journal of Enterprise Information Management*, *26*(3), 250-275. https://doi.org/10.1108/17410391311325225

Badami, M. A., Meghdadi, M. M., & Pilevar, M. (2022). Investigating the Impact of Cyberspace on the Abuse of the Right to Raise a Child with Emphasis on Religious Education. *Journal of Legal Research*, *21*(50), 457-494. https://jlr.sdil.ac.ir/journal/article_135770.html?lang=en

Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of Enterprise Information Management*, *28*(1), 107-130. https://doi.org/10.1108/JEIM-08-2013-0065

Hsu, P.-F., Kraemer, K. L., & Dunkle, D. (2006). Determinants of E-Business Use in U.S. Firms. *International Journal of Electronic Commerce*, *10*(4), 9-45. https://doi.org/10.2753/JEC1086-4415100401

Karimi, M., Majedi, N., Safari, L., & Kalhor, H. (2023). Designing a virtual business development model in the field of sports services. *Strategic Studies on Youth and Sports*, *21*(58), 313-330. https://faslname.msy.gov.ir/article_573.html?lang=en

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. *MIS quarterly*, 59-87. https://www.jstor.org/stable/25148781

Tarhini, A., Arachchilage, N. A. G., Masa'deh, R. e., & Abbasi, M. S. (2015). A Critical Review of Theories and Models of Technology Adoption and Acceptance in Information System Research. *International Journal of Technology Diffusion (IJTD)*, *6*(4), 58-77. https://doi.org/10.4018/IJTD.2015100104

Wade, M., & Hulland, J. (2004). The resource-based view and information systems research: Review, extension, and suggestions for future research. *MIS quarterly*, 107-142. https://www.jstor.org/stable/25148626

E-ISSN: 3041-8585