Journal of Islamic Art Studies
www.sysislamicartjournal.ir

Implementing a Structural-Interpretive Model for Information Security Management in Iranian Governmental Organizations: An Art-Islamic Approach

Hojat Talebi [1], **Hamid Taboli** [*2]

[1] PhD Student, Department of Public Administration, Chalous Branch, Islamic Azad University, Chalous, Iran, hojattalebi2021@yahoo.com
[*2] (Corresponding author) Associate Professor, Department of Public Administration, Payame Noor University, Tehran, Iran, hamidtaboli1400@yahoo.com

Article Info

Research Article
Issue 56
Volume 21
Page 331 to 348

Submission Date: 2021/05/20
Review Date: 2021/07/21
Acceptance Date: 2021/09/25
Publication Date: 2024/12/21

Keywords

Information Security Management,
Structural-Interpretive Model,
Islamic Approach,
Art Approach.

Cite this article

Talebi, H. and Taboli, H. (2024). Implementing a Structural-Interpretive Model for Information Security Management in Iranian Governmental Organizations: An Art-Islamic Approach. *Islamic Art Studies*, *21*(56), 331-348.

dorl.net/dor/20.1001.1.******.****.**.**.*.*/

dx.doi.org/10.22034/IAS.2021.300790.1696

ABSTRACT

In the modern era, information serves as a primary driver of power, making information dominance a critical form of control. Information Security Management (ISM) offers a model designed to protect an organization's information assets, thereby minimizing the likelihood of unauthorized access to sensitive data. Implementing robust ISM policies and programs can contribute to enhanced employee work ethic; conversely, improvements in work ethic can strengthen ISM within the organization. Despite its recognized importance, ISM has not been effectively implemented in many Iranian governmental organizations due to various factors. This research aims to address this gap by developing a "Structural-Interpretive Model for Information Security Management in Iranian Governmental Organizations with an Art-Islamic Approach."

Using a grounded theory research methodology, data were collected through theoretical and snowball sampling, achieving theoretical saturation after 17 interviews. Initial themes were identified through open coding, from which categories were extracted. Axial coding was then employed to link these categories within a coding paradigm, delineating causal conditions, a core category, strategies, context, intervening conditions, and consequences. Following the qualitative phase, a questionnaire based on the developed model was administered to 384 managers and experts familiar with ISM in Iranian governmental organizations. The collected responses were analyzed, and the results largely validated the model derived from the qualitative data, leading to specific recommendations.

Research Objectives:

1. Examine the Art and Islamic approach in organizational information security management.
2. Investigate the framework and interpretive structure of information security in Iranian organizations.

Research Questions:

1. How does the Art-Islamic approach influence organizational information security management?
2. What should be the framework and interpretive structure of information security in Iranian organizations?

Introduction

Information constitutes a critical asset for organizations and individuals alike. Its loss or compromise can necessitate significant time, resources, and labor to remediate, potentially threatening an organization's operational integrity and even its existence (Mousavi, 2015). Organizational viability is closely linked to its information systems (Tajfar, 2014), an importance so significant that some liken them to the lifeblood of the organization (Muscal et al., 2015). Since organizations derive resources and advantages from their environment, a failure to protect the information security of the organization and its stakeholders can erode its position and credibility. The human dimension and human behavior are crucial in information security, as individuals use systems and information and can, intentionally or unintentionally, compromise security (Salehi, 2017).

Information security management encompasses both technical and managerial dimensions; integrating these aspects is essential for ensuring effective information security (Young, 2014). However, some researchers argue that information security is no longer primarily a technical issue but rather a management concern (Naderi, 2017). The human factor has been identified as a critical vulnerability in information security (Bhattacharya, 2011). The success of information security increasingly depends on the effective behavior of employees and managers (Hagen, 2011). Today, information is the primary means of gaining power, and true dominance lies in information control. The conflict between wealthy and poor nations is, in reality, an information war, with dominant countries seeking to perpetuate their exploitation of resources and wealth in less-developed countries, showing little interest in fostering information infrastructures in those nations (Jahromi, 2017).

Mohammadi et al. (2019) compared patient-centered algorithms for health information security in health social networks and cloud environments, selecting articles from 2009 to 2019. This study identified 29 articles addressing user revocation and 7 addressing access control, suggesting encryption before sharing to maintain patient confidentiality. The identified solution presents a user revocation problem, and various methods have been proposed to address it. These solutions differ in aspects such as the shortness of revocation time, updating the encrypted text, the freedom of the cloud environment, the frequency of key updates, and immediate revocation. Moreover, methods have been developed for controlling patient access to information. Concerns regarding health information security lead patients to hesitate before sending their sensitive health information and sharing it with healthcare providers. This research compared algorithms and methods for health information security. The findings revealed that most

user revocation solutions require re-encryption, and access control solutions lack the necessary flexibility; therefore, better methods should be developed in the future.

Amini et al. (2019) identified factors influencing information security management in libraries and information centers at Hamadan University of Medical Sciences. The study found that the executive construct ranked highest, while human resources ranked lowest in impact on information security management. According to the results, the executive construct, with an average of 4.46, ranked first and exerted the most influence on the information security management system, while the human resource construct, with an average of 3.56, ranked seventh and had the least impact. To improve information security, senior managers must specify the security goals related to the organization, create comprehensive and integrated management, strive to comply with security rules and standards, maintain sufficient resources and budget, and create motivation among librarians and information providers. A suitable platform should be provided to facilitate improved services and take an effective step toward increasing academic scientific productivity.

Hadadi Harandi et al. (2019) examined information security management in smart business, using literature review and the Business Intelligence Maturity Model. In this research, a model was developed using the research literature and the Business Intelligence Maturity Model. A questionnaire was designed and completed by 305 managers, knowledge workers, and experts in the government transportation sector. Confirmatory factor analysis and path analysis were used to examine the model's constructs, and the data collected were analyzed using AMOS software. The results indicate that information security, with a regression coefficient of 0.38, has a direct impact on information security. In other words, information security, with the aim of ensuring continuity and minimizing cyber damages and threats, preserves and promotes business and maximizes investment opportunities through the development of new markets.

Dehghani et al. (2019) assessed the awareness, attitudes, and performance of Iranian hospital health information management staff regarding health information security. This descriptive-analytical study was conducted in 2018 on 367 employees of the health information management department in Iranian hospitals. The average scores for participants' awareness, attitude, and performance in information security management were 0.67, 3.53, and 1.47, respectively. A direct and significant relationship was found between the scores obtained in each of these three dimensions and age, work experience, education level, and field of study. Considering the awareness, attitude, and performance of employees, hospitals can improve health information security by holding educational and in-service courses.

Rezvani (2018) concluded that organizational systems, architectures, and auditing contribute significantly to information security systems in digital libraries. Laying the foundation for research on organizational systems and various architectures is a necessary requirement, and researchers need to take basic steps in this direction. Implementing well-defined optimal systems, building trust in organizations, and providing research resources to organizations will be effective in accepting this architecture.

Rezaei et al. (2018) found that management role, awareness of information security systems, compliance with training, business information security, and risk assessment affect the effectiveness of information security management systems.

Park et al. (2017) examined the role of information security education and individual factors in the disclosure of patient health information. Given the increasing importance of employees in the healthcare industry complying with information security regulations and policies, discussing information security in medical centers has become more important. The findings of this research also showed that information security and personal values play an interesting role in nursing education and the healthcare industry's efforts to protect patients' health information. Veiga and Martins (2017) studied the improvement of information security culture through monitoring and implementation measures conducted among 512 employees in South Africa. The study concluded that information security culture assessment tools can successfully influence the information security culture in organizations. Information security training and awareness are also important factors in positively influencing the information security culture. They demonstrated that the dominant information security culture and subcultures improved to a more positive state over time after implementing targeted interventions. Parsons et al. (2014), in their research conducted on 552 Australian employees, showed that knowledge-based methods and policies had a stronger influence than individuals' definitions of their behavior. These findings indicate that education can, much more than expected, create the right knowledge for using information and security systems.

Conclusion

While various information security management standards exist globally, compelling organizations to implement them, even symbolically, are achievable. However, operationalizing the practical guidelines within these standards requires a specific model. Accepting information security management necessitates identifying its barriers and challenges, and, ultimately, identifying strategies for adoption and implementation.

To achieve these goals and answer the research questions, a qualitative research strategy based on grounded theory was used to design and explain an information security management model for Iranian governmental organizations with an Islamic approach and its components. In grounded theory, the answer to the research question is the derived model and its elements. The research findings are the categories and components expressed in the model (Danaeefard & Emami, 2007). Because a new theory emerges in grounded theory, not all findings can be compared with existing literature and must be further investigated and evaluated in future research. The information security management model has various benefits, including improved organizational trust, strengthened national security, societal excellence, and physical security. This is possible only if information security management is accepted. The most important point is that the human dimension and human behavior are vital, as people use systems and information and can, intentionally or unintentionally, compromise information security. It should be noted that absolute and complete security cannot exist in today's world. Both the real and virtual worlds are like a glass prison, in which there will always be the possibility of unintended and unauthorized publication and dissemination of information. However, adhering to certain practices can significantly reduce the probability of such events. As stated before, the information security management system is recognized as a comprehensive management and technical solution for dealing with security risks; however, its implementation requires a comprehensive model (Naghiyan Fesharki, 2014).

References

Amini, M., Vakili Mofrad, H., & Saberi, M. (2019). Identifying Factors Affecting Information Security Management of Libraries and Information Centers of Hamadan University of Medical Sciences. Academic Librarianship and Information Research, 3, 53. [In Persian]

Aram, Mohammadreza. (2009). Investigating and Assessing the Factors Affecting Information Security Management of Pars South Gas Company. Master's Thesis, Shahid Beheshti University. [In Persian]

Ashouri Zadeh, S. (2012). The Relationship between Organizational Culture and Information Security Management in the National Bank of Iran. Master's Thesis, Allameh Tabataba'i University. [In Persian]

Boritz, J. E. (2004). Managing enterprise information integrity: security, control, and audit issues. Isaca.

Chang, E. (2007). An Investigation of Organizational Culture on Information Security Management. Academy of Management Journal, 35, 421-438.

Chathoth, P. K., Mak, B., Sim, J., Jauhari, V., & Manaktola, K. (2011). Assessing dimensions of organizational trust across cultures: A comparative analysis of US and Indian full service hotels. International Journal of Hospitality Management, 30(2), 233-242.

Danaeefard, H., Abdali, R., & Mahmoudi Kouchaksaraei, A. A. (2020). Research on Corruption and Administrative Health in Iran: A Scoping Review. Knowledge of Auditing, 20(79), 201-218. [In Persian]

Danaeefard, H., Rajabzadeh, A., & Hasiri, A. (2009). Promoting Intra-Organizational Trust in the Public Sector: Examining the Role of Managers' Managerial Competence. Management Research, 4, 59-90. [In Persian]

Dehghani, M., Rahmatpasand Fotideh, Z., Arasteh, Z., Shokrizadeh Bazanjani, K., & Awareness, K. (2019). Attitude and performance of employees of the health information management department of Iranian hospitals regarding health information security. Journal of Health Information Management, 1, 3-9. [In Persian]

Hadadi Harandi, A. A., Valmohammadi, C., & Salehi Sedghiani, J. (2019). Information security management in smart business. Scientific Research of Crisis Management, 8(Special Issue of Smartization), 25-33. [In Persian]

Hagen, J. M. (2011). Information security culture: an exploratory study. Information Management & Computer Security.

Hansche, S. (2001). Designing a security awareness program: Part 1. Information Systems Security, 9(6), 1-9.

Heidari, S., & Mohammadi, S. (2012). A New Model for Information Security Management in Service-Oriented Enterprise Architecture. American Journal of Scientific Research, (76), 114-132.

Ho, S. M. (2008). A Framework of Coordinated Defense. In Proceedings of the Second International Conference on Computational Cultural Dynamics (pp. 39-44).

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. Information Management & Computer Security.

Kadam, A. W. (2007). Information security policy development and implementation. Information Systems Security, 16(5), 246-256.

Kambwiri, L. (2012). An Appraisal of Information Security Management at Chancellor College, University of Malawi.

Kauspadiene, L., Cenys, A., Goranin, N., Tjoa, S., & Ramanauskaite, S. (2017). High-level self-sustaining information security management framework. Baltic Journal of Modern Computing, 5(1), 107.

Kim, S., Kim, S., & Lee, G. (2009). Structure design and test of enterprise security management system with advanced internal security. Future Generation Computer Systems, 25(3), 358-363.

Kline, R. B. (2011). Principles and practice of structural equation modeling. Guilford press.

Mitchell, R. C., Marcella, R., & Baxter, G. (1999). Corporate information security management. New Library World.

Mivald, E. (2006). Basics of Network Security. Translation: Information Technology Research Group of Jihad University of Sharif University of Technology. Tehran: Institute Is Iran Publications. [In Persian]

Mohammadi, M., Sheikh Zaheri, A., & Kermani, F. (2019). Comparison of Patient-Oriented Algorithms for Health Information Security in Health Social Networks and Cloud Environment. Journal of Modern Medical Information, 5(2), 68-79. [In Persian]

Park, E. H., Kim, J., & Park, Y. S. (2017). The role of information security learning and individual factors in disclosing patients' health information. Computers & Security, 65, 64-76.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & Security, 42, 165-176.

Shams, Shahab al-Din; Esfandiari Moghaddam, Amir. (2015). The Relationship between Different Dimensions of Organizational Trust and Employees' Job Satisfaction. Management Studies (Improvement and Transformation), 77, 171-185. [In Persian]

Veiga, A. & Martins, N. (2017) “Defining and Identifying Dominant Information Security Cultures and Subcultures.” Computers & Security, 70: 72-94.

Vermeulen, C., & Von Solms, R. (2002). The information security management toolbox–taking the pain out of security management. Information Management & Computer Security.

Whitener, E. M. (2001). Do “high commitment” human resource practices affect employee commitment? A cross-level analysis using hierarchical linear modeling. Journal of Management, 27(5), 515-535.

نشریه مطالعات هنر اسلامی
www.sysislamicartjournal.ir

کاربست الگوی ساختاری - تفسیری مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با رویکرد هنری-اسلامی

حجت طالبی [۱]، حمید تابلی [۲*]

[۱] دانشجوی دکتری مدیریت دولتی، واحد چالوس، دانشگاه آزاد اسلامی، چالوس، ایران، Talebist۹۵@gmail.com
[۲*] (نویسنده مسئول) دانشیار گروه مدیریت دولتی، دانشگاه پیام نور، تهران، ایران، htaboli@pnu.ac.ir

اطلاعات مقاله

مقاله پژوهشی
شماره ۵۶
دوره ۲۱
صفحه ۳۳۱ الی ۳۴۸

تاریخ ارسال مقاله: ۱۴۰۰/۰۲/۳۰
تاریخ داوری: ۱۴۰۰/۰۴/۳۰
تاریخ صدور پذیرش: ۱۴۰۰/۰۷/۰۳
تاریخ انتشار: ۱۴۰۳/۱۰/۰۱

کلمات کلیدی
مدیریت امنیت اطلاعات،
الگوی ساختاری-تفسیری،
رویکرد اسلامی،
رویکرد هنری.

ارجاع به این مقاله
طالبی, حجت و تابلی, حمید . (۱۴۰۳). کاربست الگوی ساختاری - تفسیری مدیریت امنیت اطلاعات در سازمان های دولتی ایران با رویکرد هنری - اسلامی. *مطالعات هنر اسلامی*, ۲۱(۵۶), ۳۳۱-۳۴۸.

dorl.net/dor/20.1001.1.*
******.****.**.**.*.*/

dx.doi.org/10.22034/IAS
.۲۰۲۱.۳۰۰۷۹۰.۱۶۹۶

چکیده

امروزه اطلاعات، عامل اصلی کسب قدرت است و تسلط واقعی، تسلط اطلاعاتی است. مدیریت امنیت اطاعات مدلی را به‌منظور حفاظت از دارایی‌های اطلاعاتی سازمان ارائه می‌کند که در نتیجهٔ آن احتمال دسترسی غیرمجاز به این دارایی‌های حساس به حداقل می‌رسد. اجرای سیاست‌ها و برنامه‌های مدیریت امنیت اطلاعات می‌تواند در جهت بالابردن اخلاق کاری کارکنان کمک کند و همچنین با افزایش رعایت اخلاق کاری می‌توان مدیریت امنیت اطلاعات را در سازمان افزایش داد. مدیریت امنیت اطلاعات بنابه دلایلی که در این پژوهش در پی شناسایی آن هستیم تاکنون به‌درستی محقق نشده است، پژوهش حاضر با هدف غایی«کاربست الگوی ساختاری - تفسیری مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با رویکرد هنری- اسلامی» و با استفاده از روش تحقیق نظریه داده‌بنیاد، روش جمع‌آوری داده مصاحبه، نمونه‌گیری نظری و گلوله برفی انجام و با ۱۷ مصاحبه اشباع نظری آن حاصل شد. مجموعه‌ای از مضامین اولیه طی فرآیند کدگذاری باز، گردآوری و از دل آن‌ها مقوله‌هایی استخراج گردید. سپس در مرحله کدگذاری محوری، پیوند میان این مقوله‌ها ذیل عناوین شرایط علی، مقوله محوری، راهبردها، بستر، شرایط مداخله‌گر و پیامدها در قالب پارادایم کدگذاری تعیین شدند. بعد از پژوهش کیفی براساس مدل به‌دست آمده، پرسش‌نامه‌ای تنظیم و از ۳۸۴ نفر از مدیران و کارشناسان آشنا و مرتبط با حوزه مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران، پاسخ‌ها جمع‌آوری و مورد تجزیه‌وتحلیل قرار گرفت. نتایج به‌دست آمده از تجزیه‌وتحلیل داده‌ها کلیات مدل استخراج شده از داده‌های کیفی را مورد تأیید قرار داد و براساس آن پیشنهاداتی ارائه گردید.

اهداف پژوهش:

۱. بررسی رویکرد هنری و اسلامی در مدیریت امنیت اطلاعات سازمانی.

۲. بررسی چارچوب و ساختار تفسیری امنیت اطلاعات سازمان‌های ایران.

سؤالات پژوهش:

۱. رویکرد هنری- اسلامی در مدیریت امنیت اطلاعات سازمانی چه تأثیری دارد؟

۲. چارچوب و ساختار تفسیری امنیت اطلاعات سازمان‌های ایران به چه شکل باشد؟

مقدمه

اطلاعات مهم‌ترین گنجینه سازمان‌ها و اشخاص می‌باشد که از بین رفتن و حتی کوچک‌ترین آسیب به آن، نیازمند صرف زمان، هزینه و نیروی کار تصورناپذیری برای جبران است و در برخی مواقع اصول کاری و موجودیت یک سازمان را تهدید می‌کند (موسوی، ۱۳۹۴). حیات سازمان‌ها ارتباط نزدیکی با سیستم اطلاعاتی آن‌ها دارد (تاج‌فر، ۱۳۹۳) و این اهمیت تا جایی است که عده‌ای آن را به خونی در رگ‌های سازمان تشبیه کرده و آن را عامل حیات‌بخش سازمان می‌دانند (مسکل[۱] و همکاران، ۲۰۱۵). چون سازمان‌ها، بسیاری از منابع و امتیازاتشان را از محیط اطراف کسب می‌کنند، چنانچه نتوانند امنیت اطلاعات سازمان و یا افراد مرتبط با سازمان را حفظ نمایند به تدریج جایگاه و اعتبارشان را از دست داده و دیگر نمی‌توانند موفق باشند. مهم‌ترین مطلبی که در مورد امنیت باید موردتوجه قرار گیرد این است که بُعد انسانی و رفتار انسانی در این مقوله مهم و حیاتی می‌باشد، زیرا این انسان‌ها هستند که از سیستم‌ها و اطلاعات استفاده کرده و می‌توانند خواسته یا ناخواسته امنیت اطلاعات را زیر سوال ببرند (صالحی، ۱۳۹۶).

مدیریت امنیت اطلاعات به دو بخش عمده فنی و مدیریتی تقسیم می‌شود که ادغام این دو جنبه کارایی امنیت اطلاعات را تضمین خواهد کرد (یانگ[۲]، ۲۰۱۴)؛ لیکن برخی از پژوهشگران حوزه امنیت معتقدند طی سال‌های اخیر مسلم شده است که امنیت اطلاعات دیگر یک موضوع فنی نیست، بلکه مسئله‌ای مدیریتی محسوب می‌شود (نادری، ۱۳۹۶). در یکی از تحقیقات (بهاتاچاریا[۳]، ۲۰۱۱) عامل انسانی به‌عنوان پاشنه آشیل امنیت اطلاعات معرفی شده است. امروزه به‌نظر می‌رسد موفقیت امنیت اطلاعات تا حد زیادی به رفتار اثربخش کارکنان و مدیران وابسته است (هاگن، ۲۰۱۱). امروزه اطلاعات عامل اصلی کسب قدرت است و تسلط واقعی، تسلط اطلاعاتی است. جنگ میان کشورهای غنی و فقیر درواقع جنگ اطلاعاتی است و کشورهای سلطه‌گر که خواستار استمرار بهره‌جویی خود از منابع و ثروت کشورهای عقب مانده هستند، علاقه‌ای به ایجاد زیربناهای اطلاعاتی در این کشورها ندارند (جهرمی، ۱۳۹۶).

محمدی و همکاران (۱۳۹۸)، به مقایسه الگوریتم‌های بیمار محور برای امنیت اطلاعات سلامت در شبکه‌های اجتماعی سلامت و محیط ابر پرداختند. در این پژوهش، جست‌وجو مقالات در فاصلهٔ زمانی ۲۰۰۹-۲۰۱۹ انتخاب شده‌اند. ۲۹ مقاله برای حل مسئله لغو کاربر و ۷ مقاله برای حل مسئله کنترل دسترسی انتخاب شده است. به‌منظور حفظ محرمانگی اطلاعات بیماران، روش رمزنگاری قبل از به اشتراک‌گذاری پیشنهاد شده است. این راه حل مشکل لغو کاربر را دارد. برای حل این مشکل روش‌های مختلفی ارائه شده است. این راه‌حل‌ها از جنبه‌های مختلف کوتاه بودن زمان لغو، به‌روزرسانی متن رمز شده، آزادبودن محیط ابر، تناوب در به‌روزرسانی کلید و لغو فوری متفاوت هستند. همچنین روش‌هایی برای کنترل دسترسی اطلاعات توسط بیمار ارائه شده است. مسائل مربوط به امنیت اطلاعات سلامت باعث می‌شود بیماران نسبت به ارسال اطلاعات حساس لامت خود و اشتراک آن با ارائه‌دهندگان خدمات سلامت مردد باشند. در این پژوهش، الگوریتم‌ها و روش‌های امنیت اطلاعات سلامت مقایسه شده‌اند. اکثر راه‌حل‌های لغو کاربر به رمزنگاری

---
[۱] Meskel
[۲] Yang
[۳] Bhattacharya

مجدد نیاز دارند. همچنین راه‌حل‌های کنترل دسترسی انعطاف‌پذیری لازم ندارند. از این‌رو در آینده باید روش‌های بهتری ارائه شوند.

امینی و همکاران (۱۳۹۸)، در پژوهشی به شناسایی عوامل مؤثر بر مدیریت امنیت اطلاعات کتابخانه‌ها و مراکز اطلاع رسانی دانشگاه علوم پزشکب همدان پرداختند. براساس نتایج مطالعه، سازه اجرایی با میانگین ۴۶/۴ در رتبه اول و با بیشترین اثرگذاری در سیستم مدیریت امنیت اطلاعات و سازه نیروی‌انسانی با میانگین ۵۶/۳ در رتبه هفتم و با کم‌ترین اثرگذاری شناسایی شد. برای ارتقاء سطح امنیت اطلاعات ضروری است که مدیران ارشد با مشخص‌نمودن اهداف امنیتی مرتبط با سازمان، ایجاد مدیریتی جامع و یکپارچه، تلاش برای رعایت قوانین و استانداردهای امنیتی، در دست داشتن منابع و بودجه کافی و ایجاد انگیزه در بین کتابداران و اطلاع‌رسانان، بستر مناسبی را فراهم آورند تا ارائه خدمات مطلوب‌تر گردد و همچنین بتوانند گامی مؤثر در جهت افزایش تولیدات علمی دانشگاهی داشته باشند. حدادی هرندی و همکاران (۱۳۹۸) به بررسی مدیریت امنیت اطلاعات در کسب و کار هوشمند پرداختند. در این پژوهش با استفاده از ادبیات تحقیق و مدل بلوغ سیستم‌های هوشمند کسب و کار، مدلی تبیین و پرسش‌نامه‌ای طراحی و توسط ۳۰۵ نفر از مدیران، کارکنان دانشی و کارشناسان بخش حمل‌ونقل دولتی تکمیل شده است. با استفاده از تحلیل عاملی تأییدی و تجزیه‌وتحلیل مسیر، سازه‌های مدل بررسی و داده‌های جمع‌آوری شده توسط نرم‌افزار AMOS تحلیل شدند. نتایج نشان می‌دهد که امنیت اطلاعات با ضریب رگرسیونی ۰/۳۸ تأثیر مستقیم بر امنیت اطلاعات درد. به عبارت دیگر، امنیت اطلاعات با هدف تضمین تداوم و به حداقل رساندن آسیب‌ها و تهدیدات سایبری، باعث حفظ و ارتقاء کسب و کار و به حداکثر رساندن فرصت‌های سرمایه‌گذاری از طریق توسعه بازارهای جدید می‌شود.

دهقانی و همکاران (۱۳۹۸) به بررسی آگاهی، نگرش و عملکرد کارکنان بخش مدیریت اطلاعات سلامت بیمارستان‌های ایران نسبت به امنیت اطلاعات سلامت پرداختند. این مطالعه توصیفی- تحلیلی در سال ۱۳۹۷ برروی ۳۶۷ نفر از کارکنان بخش مدیریت اطلاعات سلامت بیمارستان‌های ایران انجام شده است. میانگین امتیازات آگاهی، نگرش و عملکرد شرکت‌کنندگان در زمینهٔ مدیریت امنیت اطلاعات به ترتیب ۰/۶۷ ، ۳/۵۳ و ۱/۴۷ به‌دست آمده است. همچنین رابطهٔ مستقیم و معناداری بین نمره کسب شده در هر یک از این سه بعد با سن، سابقه کار، مقطع تحصیلی و رشته تحصیلی وجود دارد. باتوجه‌به وضعیت آگاهی، نگرش و عملکرد کارکنان، می‌توان با برگزاری دوره‌های آموزشی و ضمن خدمت، وضعیت امنیت اطلاعات سلامت در بیمارستان‌ها را ارتقا داد.

رضوانی، شهلا (۱۳۹۷) در پژوهشی با عنوان «طراحی الگوی مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتالی» دریافت که سیستم‌ها و معماری‌های سازمانی و ممیزی کمک شایانی به استقرار سیستم‌های امنیت در سازمان‌ها خواهند نمود. پایه‌ریزی تحقیقات دربارهٔ سیستم‌های سازمانی و معماری‌های مختلف، یکی از نیازمندی‌های ضروری محسوب می‌شود و لازم است محققان قدم‌های اساسی در این جهت بردارند. پیاده‌سازی سیستم‌های بهینه تعریف شده، نیاز اعتمادسازی در سازمان‌ها و ارائه منابع تحقیقات به سازمان‌ها، در پذیرش این معماری تأثیرگذار خواهند بود.

رضایی، علی و همکاران (۱۳۹۷) در پژوهشی با عنوان «عوامل مؤثر بر اثربخشی سیستم مدیریت امنیت اطلاعات» دریافتند که شاخص‌های نقش مدیریت، آگاهی از سیستم امنیت اطلاعات و انطباق با آموزش، امنیت سیستم اطلاعات کسب و کار و ارزیابی ریسک امنیت سیستم اطلاعات بر اثربخشی سیستم مدیریت امنیت اطلاعات تأثیرگذار می‌باشد.

پارک[۴] و همکاران (۲۰۱۷)، نقش آموزش امنیت اطلاعات و عوامل فردی در افشای اطلاعات سلامت بیماران را بر گسترش امنیت اطلاعات بررسی کردند. باتوجه‌به بیشتر شدن اهمیت اجابت مقررات و سیاست‌های امنیت اطلاعات به‌وسیلهٔ کارکنانی که در صنعت مراقبت‌های بهداشتی کار می‌کنند، بحث امنیت اطلاعات در مراکز درمانی از اهمیت بیشتری برخوردار شده است. همچنین یافته‌های این پژوهش نشان دادند امنیت اطلاعات و ارزش‌های شخصی در آموزش پرستاری و تلاش صنعت مراقبت‌های بهداشتی برای حفاظت از اطلاعات سلامت بیماران نقش جالب توجهی دارند.

وایگا و مارتینز[۵] (۲۰۱۷)، در پژوهش بهبود فرهنگ امنیتی اطلاعات از طریق اقدامات نظارت و پیاده‌سازی که بین ۵۱۲ نفر از کارکنان در آفریقای جنوبی انجام دادند، به این نتیجه رسیدند که ابزار ارزیابی فرهنگ امنیت اطلاعات می‌تواند در سازمان‌ها به‌طور موفقیت‌آمیزی بر فرهنگ امنیت اطلاعات تأثیر بگذارد. همچنین آموزش امنیت اطلاعات و آگاهی عاملی مهم در تأثیرگذاری مثبت بر فرهنگ امنیت اطلاعات است. آن‌ها نشان دادند فرهنگ و خرده‌فرهنگ‌های امنیتی اطلاعات غالب در طول زمان پس از اجرای مداخلات هدفمند به یک فرهنگ امنیتی اطلاعاتی مثبت‌تر بهبود یافته است. پارسونز[۶] و همکاران (۲۰۱۴)، در پژوهش خود که بر روی ۵۵۲ کارمند استرالیایی انجام شده است، نشان دادند که روش‌ها و سیاست‌های دانشی نفوذ قوی‌تری نسبت به تعریف افراد از رفتار خود داشته است. این یافته‌ها بیانگر این است که آموزش و پرورش خیلی بیشتر از آنچه انتظار می‌رود می‌تواند در ایجاد دانش مناسب برای استفاده از سیستم‌های اطلاعاتی و امنیت سیستم‌ها، نگرش ایجاد نماید.

۱. مدیریت امنیت اطلاعات

برای کاربست الگوی ساختاری - تفسیری مدیریت امنیت اطلاعات، لازم است ابتدا مفهوم امنیت اطلاعات و مدیریت آن به‌درستی درک شده و عوامل مؤثر بر امنیت اطلاعات شناسایی شوند.

۱/۱. امنیت اطلاعات

اندرس[۷] (۲۰۱۴) امنیت اطلاعات را به‌عنوان محافظت از سیستم‌های اطلاعاتی و اطلاعات در برابر دسترسی غیرمجاز، استفاده، افشا، اختلال، اصلاح و تخریب تعریف می‌کند.

---

[۴] - Park
[۵] Veiga. & Martins
[۶] Parsons
[۷] Andress

ویتمن و ماتورد[۸] (۲۰۱۱) امنیت را به‌عنوان عاری‌بودن از خطر تعریف می‌کنند و امنیت اطلاعات را تنها یکی از چندین لایه امنیتی موردنیاز مانند امنیتی فیزیکی، امنیت کارکنان، امنیت عملیات، امنیت ارتباطات و امنیت شبکه می‌دانند.

محققان بر این باور هستند که امنیت اطلاعات دارای سه ویژگی است که باید به آن‌ها توجه کرد. این سه ویژگی عبارت‌اند از:

۱- امنیت اطلاعات یک مشکل فنی نیست بلکه یک مسئله مدیریتی و کسب و کاری است (چانگ[۹] و همکاران، ۲۰۰۶).

۲- امنیت اطلاعات یک فرایند مدیریتی چرخشی تحت عنوان سیستم مدیریت امنیت اطلاعات است. در این فرایند مخاطرات به‌صورت پیوسته توسط کنترل‌های مناسب مدیریت می‌شوند. تا احتمال نتایج مخاطرات ناخواسته کاهش یابد (آرام، ۱۳۸۸).

۳- امنیت اطلاعات بر مبنای مدیریت مخاطرات بنا می‌شود. ازآنجایی‌که به‌دست‌آوردن امنیت کامل، غیرقابل دسترس است همیشه یک سطح مخاطره برای امنیت اطلاعات باید درنظر گرفته شود. مخاطرات با کاهش احتمال وقوع آن‌ها یا با کاهش نتایج آن‌ها، تقلیل داده می‌شود (آرام، ۱۳۸۸).

محققان ویژگی‌های متفاوتی را برای اطلاعات درنظر می‌گیرند. به‌عنوان مثال، ویتمن و ماتورد (۲۰۱۳) محرمانه‌بودن[۱۰]، یکپارچگی[۱۱]، سودمندی[۱۲] و مالکیت[۱۳] را به‌عنوان ویژگی‌های مهم اطلاعات درنظر می‌گیرند؛ درحالی‌که اندرس (۲۰۱۴) محرمانه‌بودن، یکپارچگی و در دسترس بودن[۱۴] را به‌عنوان مثلث CIA می‌پذیرد و مالکیت، اصالت (اعتبار)[۱۵] و و سودمندی را به آن اضافه می‌کند.

مؤلفه‌های مثلث CIA به‌صورت زیر تعریف می‌شوند.

الف- محرمانه‌بودن: محرمانگی یعنی جلوگیری از افشای اطلاعات به افراد غیرمجاز یا جلوگیری از دست دادن آن‌ها (هومفریز[۱۶]و همکاران، ۱۹۹۸). به‌عنوان مثال، برای خرید با کارت‌های اعتباری بر روی اینترنت نیاز به ارسال شماره کارت اعتباری از خریدار به فروشنده و سپس به مرکز پردازش معامله است. در این مورد، شماره کارت و دیگر اطلاعات مربوط به خریدار و کارت اعتباری او باید محرمانه بماند و در اختیار افراد غیرمجاز قرار نگیرد. در این مورد برای محرمانه نگهداشتن اطلاعات، شماره کارت رمزنگاری می‌شود و در طی انتقال یا مکان‌هایی که ممکن است ذخیره شود (در پایگاه‌های داده، فایل‌های ثبت وقایع سیستم، پشتیبان‌گیری، چاپ رسید و غیره) رمز شده باقی می‌ماند. همچنین

[۸] Whitman & Mattord,
[۹] Chang
[۱۰] Confidentiality
[۱۱] Confidentiality
[۱۲] Utility
[۱۳] Possession
[۱۴] Availability
[۱۵] Authenticity
[۱۶] Humphreys

دسترسی به اطلاعات و سیستم‌ها نیز محدود می‌شود. اگر فردی غیرمجاز به شماره کارت به هر نحوی دست یابد، نقض محرمانگی رخ داده است (عاشوری‌زاده، ۱۳۹۱).

ب-یکپارچگی: یکپارچه‌بودن یعنی جلوگیری از تغییر داده‌ها به‌طور غیرمجاز و تشخیص تغییر در صورت دستکاری غیرمجاز اطلاعات. یکپارچگی وقتی نقض می‌شود که اطلاعات در حین انتقال به‌صورت غیرمجاز تغییر داده می‌شود (عاشوری‌زاده، ۱۳۹۱). سرویس یکپارچگی درست‌بودن اطلاعات را ارائه می‌کند. هنگامی که از یکپارچگی به‌خوبی استفاده شود، به کاربران اجازه می‌دهد که این اعتماد را داشته باشند که اطلاعات درست است و توسط فرد غیرمجازی تغییر نکرده است (میوالد، ۱۳۸۵). رخنه در صحت اطلاعات می‌تواند ناشی از تغییر غیرمجاز، غیرمنتظره و غیرعامدانه باشد. یکپارچگی اطلاعات زمانی رخ می‌دهد که درستی، تمامیت، به هنگامی، اعتبار و روش‌های پردازش اطلاعات ایمن تأمین گردند (بورتیز[۱۷]، ۲۰۰۴).

پ- در دسترس بودن: اطلاعات باید زمانی که موردنیاز افراد مجاز هستند، در دسترس باشند. این ویژگی از آن رو مهم است که بدون آن فعالیت‌های معمول شرکت ادامه نمی‌یابد و تصمیمات به موقع گرفته نمی‌شود (گربر و وان سولمز[۱۸]،۲۰۰۱). در دسترس بودن به کاربران اجازه می‌دهد که به سیستم‌های رایانه‌ای، اطلاعات روی این سیستم‌ها و برنامه کاربردی که عملیات را بر روی اطلاعات اجرا می‌کند، دسترسی داشته باشند (کیم[۱۹]و همکاران، ۲۰۰۹). همچنین در دسترس بودن، برای سیستم‌های ارتباطی، انتقال اطلاعات بین محل‌ها یا سیستم‌های رایانه‌ای را فراهم می‌کند. هنگامی که دربارهٔ در دسترس بودن صحبت می‌شود، اغلب این اطلاعات و قابلیت‌ها همگی به شکل الکترونیک در ذهن می‌آیند. با این حال، در دسترس بودن پرونده‌های کاغذی اطلاعات نیز باید محافظت شود.

به‌منظور حفظ امنیت اطلاعات، استانداردهای بین‌المللی وجود دارند که محرمانگی، یکپارچگی و در دسترس بودن اطلاعات را تضمین می‌کنند. این استانداردها در ذیل آورده شده‌اند.

۱/۲. استانداردهای امنیت اطلاعات

پور[۲۰](۲۰۰۱) اظهار داشت که بدون استانداردهایی که معیارهای عینی را برای انتخاب امنیت اطلاعات فراهم کنند، مدیران ممکن است تصمیماتی را براساس فاکتورهای غیراصولی که ممکن است براساس سوگیری، محدودیت‌های درک شده و انگیزه‌های شخصی باشد، اتخاذ نماید؛ بنابراین استانداردهای بین‌المللی به‌وجود آمدند که جنبه‌های مختلف مدیریت اطلاعات را مورد بررسی قرار می‌دهند. در جدول شماره (۱) این استانداردها شرح داده شده‌اند.

[۱۷] Boritz
[۱۸] Gerber & Von Solms
[۱۹] Kim
[۲۰] Poore

جدول۱. استانداردهای امنیت اطلاعات (کامویری[۲۱]،۲۰۱۲)

ردیف	استاندارد	توصیف	توضیح مختصر
۱	ISO/IEC ۲۷۰۰۲: ۲۰۰۵	کد عمل برای مدیریت امنیت اطلاعات	مشخصات: سیاست امنیتی، سازماندهی امنیت اطلاعات، مدیریت دارایی، امنیت منابع انسانی، امنیت فیزیکی و محیط‌زیست، مدیریت ارتباطات و عملیات، کنترل دسترسی، دستیابی به سیستم‌های اطلاعاتی، توسعه و نگهداری، مدیریت حوادث امنیتی اطلاعات، مدیریت پیوستگی تجارت، انطباق.
۲	SO/IEC ۲۷۰۰۱:۲۰۰۵	الزامات سیستم مدیریت امنیت اطلاعات	الزامات مربوط به ایجاد، اجرا، بهره‌برداری، نظارت، بررسی، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات را به طور مستند مشخص می‌کند. یک مدل چرخه‌ای معروف به «برنامه-اجرا-چک-اقدام» را معرفی می‌کند. اغلب همراه با ISO / IEC ۲۷۰۰۲: ۲۰۰۵ اجرا می‌شود.
۳	ISO/IEC ۱۵٤۰۸	معیارهای ارزیابی امنیت IT (معیارهای مشترک)	شامل سه بخش است که عبارتند از: معرفی و مدل کلی (۱۵۴۰۸-۱: ۲۰۰۵)، الزامات عملکردی امنیتی (۱۵۴۰۸-۲: ۲۰۰۵) و الزامات تضمین امنیتی (۱۵۴۰۸ ۳:۲۰۰۵). به ارزیابی، اعتبارسنجی و تأیید تضمین امنیت یک محصول فناوری در برابر عوامل مختلف کمک می‌کند. سخت‌افزار و نرم‌افزار را می‌توان در برابر این استاندارد ارزیابی کرد.
۴	صنعت کارت‌های پرداخت / PCI DSS	صنعت کارت پرداخت استاندارد امنیت داده‌ها	برای امنیت تراکنش با کارت اعتباری به صورت آنلاین
۵	COBIT	اهداف کنترلی برای اطلاعات و فناوری‌های مرتبط	چارچوبی که ابتکار عمل IT را با الزامات تجاری پیوند داده و شکاف بین الزامات کنترل، مسائل فنی و ریسک‌های تجاری را مشخص می‌کند.

در هر حال باید توجه شود که هر استانداردی که انتخاب می‌شود باید برای آن سازمان، قابل پذیرش و کاربردی باشد.

۱/۳. نقش عوامل انسانی در مدیریت امنیت اطلاعات

کارکنان نقش مهم در امنیت کلی اطلاعات در سازمان دارند. بدون درنظر گرفتن عامل انسانی، حتی ترفندهای فناوری نیز نمی‌تواند امنیت اطلاعات را تضمین نماید. سازمان‌ها به‌طور فزاینده از فناوری‌های امنیتی برای حفاظت از اطلاعات

[۲۱] Kambwiri

استفاده می‌کنند، اما امنیت اطلاعات تنها با استفاده از این فناوری‌ها حاصل نمی‌شود (هراث و رائو[۲۲]،۲۰۰۹). امنیت اطلاعات مؤثر در سازمان‌ها به سه مؤلفه بستگی دارد: کارکنان، فرایندها و فناوری.

سازمان جهانی استاندارد (ISO) در سال ۲۰۱۴، رتبه ایران از نظر تعداد گواهینامه‌های اخذ شده در سیستم مدیریت امنیت اطلاعات را جایگاه ششم از میان چهارده کشور خاورمیانه اعلام نمود. آمار ارائه شده، نشان‌دهندهٔ عدم توجه کافی در کشور به حوزهٔ مدیریت امنیت اطلاعات می باشد که به‌نظر می‌رسد نبود الگوی مناسب با دیدگاه همه‌جانبه نسبت به امنیت اطلاعات، توجه بیشتر به توسعهٔ فنی این حوزه و عدم در نظر گرفتن جنبهٔ مدیریتی آن سبب بروز این مشکل می‌باشد (عبدی، ۱۳۹۵). به همین دلیل با وجود توسعه و ایجاد راه‌کارها و تکنیک‌های پیچیدهٔ امنیتی شاهد وخیم‌تر شدن وضعیت امنیت اطلاعات در سازمان‌ها هستیم (عیدی، ۱۳۹۷) و از طرفی با وجود برخی استانداردهای خارجی در حوزه مدیریت امنیت اطلاعات ازجمله (NIST[۲۳]، COBIT[۲۴] و ISO۲۷۰۰۰[۲۵])، حرکت براساس سیستم مدیریت امنیت اطلاعات منطبق بر استانداردهای اروپایی که تطابق کمی با شرایط زیرساختی سازمان‌های ایرانی دارند دشوار به‌نظر می‌رسد (تقوا، ۱۳۹۶). استفاده از یک الگوی جامع امنیتی در سازمان می‌تواند ضمن محافظت از اطلاعات یک سیستم، موجب بالابردن قابلیت اطمینان تصمیم‌گیری، ایجاد اطمینان نزد مشتریان، امکان رقابت بهتر با سایر سازمان‌ها و ... شود. در طول سال‌ها سازمان‌ها، ضرر و زیان‌های متعددی که تأثیر مستقیمی بر اطلاعاتشان داشته تجربه کرده‌اند. در محیط اطلاعاتی امروز، ماهیت خطرات و تهدیدات نیز تغییر پیدا کرده است، مرزهای سازمانی حذف شده‌اند، در نتیجه، چالش برای امنیت اطلاعات افزایش یافته است. برای پرداختن به این خطرات امنیتی یک سازمان باید استراتژی امنیت اطلاعات را از طریق ایجاد یک چارچوب جامع پیاده‌سازی کند.

۲. روش پژوهش

الگو مفهومی از رویکرد کیفی (روش تئوری داده بنیاد) و در فاز تبیین الگو از رویکرد کمّی بهره برده است. به‌طور کلی روش گردآوری داده‌ها در تحقیق حاضر به دو دسته کلی قابل تقسیم‌بندی می‌باشد:

- روش کتابخانه‌ای و اینترنتی به‌منظور آشنایی با ادبیات و پیشینه تحقیق
- روش میدانی (و مشخصاً مصاحبه و پرسش‌نامه) به‌منظور جمع‌آوری داده‌های موردنیاز از جامعه آماری. بدین‌نحو که در فاز طراحی الگو، از روش مصاحبه عمیق، و در فاز برازش الگو، از روش پرسش‌نامه بسته استفاده شد. گفتنی است که در این تحقیق، ابزارهای اصلی تحقیق براساس فازهای مختلف، به‌صورت زیر خواهند بود:

[۲۲] Herath and Rao
[۲۳] National Institute of Standard and Technology (NIST)
[۲۴] Control Objective for Information and related Technology (CObIT)
[۲۵] International Standard Organization (ISO)

جدول۲. ابزارهای گردآوری اطلاعات به تفکیک هر فاز

فاز	ابزار اصلی جمع‌آوری داده
مطالعه ادبیات و پیشینه تحقیق	بانک‌های اطلاعاتی و فیش‌برداری
دستیابی به الگوی اولیه تحقیق براساس روش گراندد تئوری(رویکرد کیفی)	مصاحبه عمیق
برازش الگوی تحقیق و دستیابی به الگوی نهایی (رویکرد کمّی)	پرسشنامه بسته

با استفاده از روش تحقیق نظریه داده‌بنیاد، روش جمع‌آوری داده مصاحبه، نمونه‌گیری نظری و گلوله برفی انجام و با ۱۷ مصاحبه اشباع نظری آن حاصل شد. مجموعه‌ای از مضامین اولیه طی فرآیند کدگذاری باز، گردآوری شد و از دل آن‌ها مقوله‌هایی استخراج گردید. سپس در مرحله کدگذاری محوری، پیوند میان این مقوله‌ها ذیل عناوین شرایط علی، مقوله محوری، راهبردها، بستر، شرایط مداخله‌گر و پیامدها در قالب پارادایم کدگذاری تعیین شدند. در ادامه و در مرحله کدگذاری گزینشی، یکایک اجزای پارادایم کدگذاری تشریح، سیر فعالیت ترسیم و الگو خلق شد. بعد از پژوهش کیفی براساس مدل به‌دست آمده، پرسش‌نامه‌ای تنظیم و از ۳۸۴ نفر از مدیران و کارشناسان آشنا و مرتبط با حوزه مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران، پاسخ‌ها جمع‌آوری و مورد تجزیه‌وتحلیل قرار گرفت.

۳. روش تجزیه‌وتحلیل داده‌ها

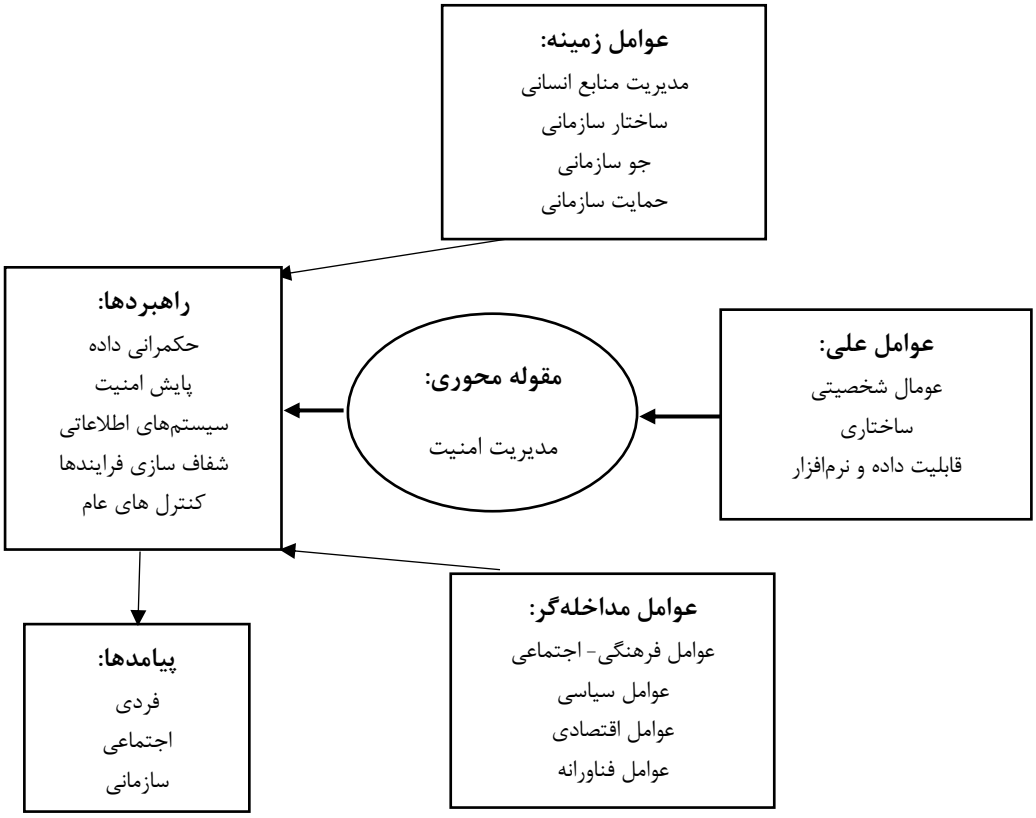
تجزیه‌وتحلیل داده‌های پژوهش در سطح آمار توصیفی (فراوانی، میانگین، انحراف استاندارد، کم‌ترین، بیشترین، جدول و نمودار، کجی و کشیدگی، آزمون مهالانوبیس) با استفاده از نرم‌افزار SPSS[۲۶]۲۳ و روش الگویابی معادلات ساختاری با استفاده از نرم‌افزار AMOS[۲۷]۲۳ انجام گرفت. به‌منظور ارزیابی الگوی پیشنهادی، رویکرد دومرحله‌ای آندرسون و گربینگ[۲۸] (۱۹۸۸) مورد استفاده قرار گرفت. در مرحله اول الگوی اندازه‌گیری و در مرحله دوم بخش ساختاری الگو بر پایه نتایج مرحله اول و با استفاده از الگویابی معادلات ساختاری[۲۹](SEM) برآورد شدند. مدل‌یابی معادلات ساختاری یک تکنیک تحلیل چندمؤلفه‌ای بسیار کلی و نیرومند از خانواده رگرسیون چندمؤلفه‌ای و به بیان دقیق‌تر بسط «مدل خطی کلی» است. مدل‌یابی معادله ساختاری یک رویکرد جامع برای آزمون فرضیه‌هایی دربارهٔ روابط مؤلفه‌های مشاهده شده و مکنون است که گاه تحلیل ساختاری کوواریانس، مدل‌یابی علّی نامیده شده است اما اصطلاح غالب در این روزها، مدل‌یابی معادله ساختاری یا به‌گونهٔ خلاصه SEM است (هومن، ۱۳۸۸: ۱۱). شاخص‌ها عبارت‌اند از: مقدار کای‌دو، شاخص هنجارشدهٔ مجذور کای دو (نسبت مجذور کای بر درجات آزادی)، شاخص نیکویی برازش[۳۰] (GFI)،

۱. statistical package for social science
۲. Alpha Micro Operating System
۳ . Anderson & Gerbing
٤. Structural Equaion Modeling
۱۱. Adjusted goodness -of-fit index

شاخص نیکویی برازش تعدیل‌یافته[۳۱](AGfI)، شاخص برازندگی هنجارشده[۳۲] (NFI)، شاخص برازندگی تطبیقی[۳۳](CFI)، شاخص برازندگی افزایشی[۳۴](IFI)، شاخص تاکر- لویس[۳۵](TLI) و جذر میانگین مجذورات خطای تقریب[۱۶] (RMSEA).

٤. یافته‌های پژوهش

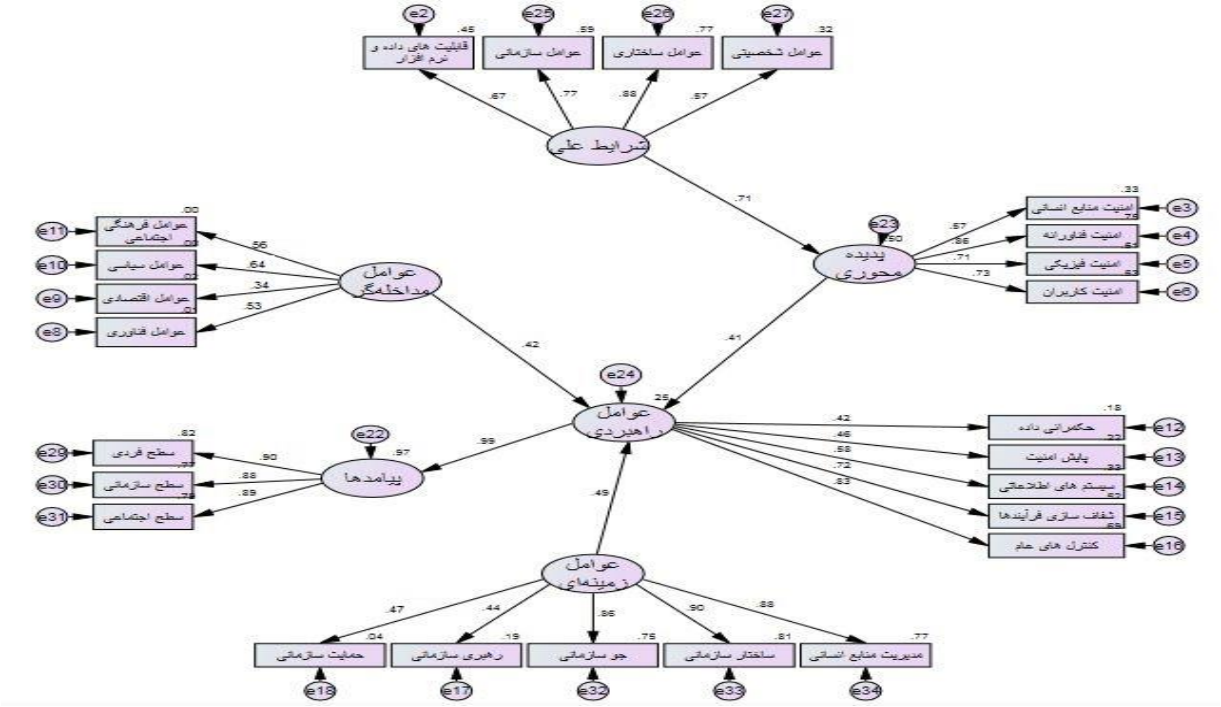
در فرآیند کدگذاری باز، مضمون‌های بسیاری حاصل شد که طی فرآیند رفت و برگشتی تحلیل داده‌ها، مجموعه این داده‌های کیفی اولیه به مقوله‌های کم‌تری تقلیل یافت. مدیریت امنیت اطلاعات به‌عنوان مقولهٔ هسته در این مدل در نظر گرفته شد و مقوله‌های دیگر در پنج طبقه عوامل علی، عوامل زمینه‌ای، عوامل مداخله‌گر، راهبردها و پیامدها قرار گرفتند. در شکل شماره (۱) پارادایم شناسایی شده مدیریت امنیت اطلاعات با رویکرد اسلامی ارائه شده است.



شکل۱. پارادایم مدیریت امنیت

۱۲. Normed fit index
۱۳. Comprative fit index
۱٤. Incremental fit index
۱٥. Tucker-Lewis index
۱٦. Root- mean- square error of approximation

طراحی و تبیین الگوی مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با رویکرد اسلامی، اولین مدل پژوهش ترسیم و روابط بین متغیرهای پنهان در نرم‌افزار AMOS۲۳ مورد بررسی قرار می‌گیرد. در این مورد ابتدا از شاخص‌های برازش اطمینان حاصل کرده و سپس به بررسی روابط مفروض بین متغیرهای پنهان پرداخته شد.



شکل۲. CMIN =۲۹۹,۴۹ ،P = ۰,۰۰۱ ،CMIN/DF = ۱,۶۸ ،RMSEA= ۰,۰۴۲

در شکل فوق روابط متغیرهای پژوهش نشان داده شده است. اعداد ذکر شده بر روی روابط بین متغیرها ضرایب رگرسیونی می‌باشند که بیانگر جهت مثبت رابطه‌ای متغیرهای پیش‌بین بر ملاک می‌باشد. همچنین در ادامه به بررسی شاخص‌های برازش مدل ساختاری پرداخته خواهد شد.

باتوجه‌به نتایج حاصل، در مورد تحلیل برازش مدل باتوجه‌به شاخص‌های برازندگی، می‌توان گفت که مدل تحلیل عاملی جهت طراحی مدل موردنظر دارای برازش مناسبی می‌باشد. به عبارت دیگر، باتوج به مناسب‌بودن شاخص‌های برازندگی می‌توان از این مدل به‌عنوان الگوی مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با تأکید بر تقویت اعتماد سازمانی استفاده کرد.

جدول۳. شاخص‌های نیکویی برازش مدل ساختاری متغیرهای پژوهش

شاخص‌های برازندگی الگو	CMIN	DF	CMIN/DF	NPAR	P	GFI	AGFI	IFI	TLI	CFI	NFI	RMSEA
الگوی برازش شده	۲۹/۴۹۹	۱۷۸	۱/۶۸	۱۴۷	۰/۰۰۱	۰/۹۴	۰/۸۹	۰/۹۸	۰/۹۷	۰/۹۸	۰/۹۶	۰/۰۴۲
مقادیر مطلوب	= df	–	< ۳	–	۰/۰۵ >	۰/۹۰ >	۰/۹۰ >	۰/۹۰ >	۰/۹۰ >	۰/۹۰ >	۰/۹۰ >	<۰/۰۸

نتایج به‌دست‌آمده از آزمون مدل فوق نشان می‌دهد که رابطهٔ مستقیم مؤلفهٔ شرایط علّی بر مؤلفهٔ پدیده محوری (P < ۰/۰۵، t = ۸/۰۵، β = ۰/۷۱) مثبت و معنادار است، همچنین رابطهٔ مستقیم مؤلفهٔ پدیده محوری بر مؤلفهٔ عوامل راهبردی (P < ۰/۰۵، t = ۴/۹۱، β = ۰/۴۱) مثبت و معنادار است. رابطهٔ مستقیم مؤلفهٔ عوامل مداخله‌گر بر مؤلفهٔ عوامل راهبردی (P < ۰/۰۵، t = ۶/۱۸، β = ۰/۴۲) مثبت و معنادار است، همچنین رابطهٔ مستقیم مؤلفهٔ عوامل زمینه‌ای بر مؤلفهٔ عوامل راهبردی (P < ۰/۰۵، t = ۷/۷۹، β = ۰/۴۹) مثبت و معنادار است، رابطهٔ مستقیم مؤلفهٔ عوامل راهبردی بر مؤلفهٔ پیامدها (P < ۰/۰۵، t = ۹/۶۰، β = ۰/۹۹) مثبت و معنادار است.

جدول۴. روابط مستقیم متغیرهای مکنون بر یکدیگر

مسیرها	ضرایب مسیر			سطح معناداری
	پارامتر استاندارد شده	پارامتر استاندارد نشده	مقدار t	
شرایط علّی ← پدیده محوری	۰/۷۱	۰/۶۳	۸/۰۵	۰/۰۰۱
پدیده محوری ← عوامل راهبردی	۰/۴۱	۰/۲۷	۴/۹۱	۰/۰۲۱
عوامل مداخله‌گر ← عوامل راهبردی	۰/۴۲	۰/۳۱	۶/۱۸	۰/۰۰۱
عوامل زمینه‌ای ← عوامل راهبردی	۰/۴۹	۰/۴۳	۷/۷۹	۰/۰۰۱
عوامل راهبردی ← پیامدها	۰/۹۹	۱/۳۲	۹/۶۰	۰/۰۰۱

۵. رویکرد هنری در مدیریت

براساس داده‌های منابع، کاربست عناصر هنری در محیط سازمان، به‌عنوان یک عامل زمینه‌ای با بافتار فرهنگی نقش کلیدی در ترسیم فضایی امن و معنوی دارد. این عناصر را می‌توان در طراحی فضای محیطی، کاربرد انواع آثار هنری مانند فرش، تابلوهای نقاشی یا مینیاتور، نمایش صنایع‌دستی برای تزئین محیط کار اشاره کرد. ترسیم و طراحی محیطی با محوریت فرهنگ اسلامی به فراخور تبلیغ داده‌های اخلاقی محیط امن‌تری را فراهم می‌سازد. نمایش تابلوها خوشنویسی و کتیبه‌ها با مضامین قرآنی و اخلاقی ازجملهٔ این روش‌های راهبردی می‌باشد.

تحقیقات به‌طور مداوم نشان می‌دهد که ترکیب هنر و آثار هنری در محیط‌های اداری می‌تواند تأثیرات مثبت عمیقی بر رفاه، بهره‌وری و رضایت شغلی کلی کارکنان داشته باشد. مطالعات نشان می‌دهد که هنر در محیط کار به کاهش استرس و افزایش سلامت روان کمک می‌کند.

هنر کارکردهای شناختی را تحریک می‌کند و به تفکر خلاق الهام می‌بخشد، که می‌تواند منجر به حل مسئله نوآورانه و ایده‌های تازه شود. این خلاقیت افزایش یافته برای کارکنان یک شرکت است که مستقیماً به موفقیت یک شرکت کمک می‌کند. حضور هنر در محیط‌های کاری به‌طور مثبت بر تعامل کارکنان و فرهنگ شرکت تأثیر می‌گذارد. در ادامه پیشنهادهایی برای استفاده از تابلوها در محیط‌های کاری در مقاله رشد ذهنیت و روحیه کارکنان آورده شده است.

نتیجه‌گیری

وجود استانداردهای گوناگون مدیریت امنیت اطلاعات در جهان و ملزم‌کردن سازمان‌ها و نهادهای داخلی به اجرای آن، هرچند به‌صورت نمادین امکان‌پذیر است لیکن پیاده‌سازی و اجرایی‌کردن دستورالعمل‌های واقعی مندرج در آن، باید در قالب مدل معینی در اختیار سازمان‌ها قرار گیرد. پذیرش مدیریت امنیت اطلاعات مستلزم شناسایی موانع و مشکلات آن و در نهایت شناسایی راهبردهایی برای پذیرش و به‌کارگیری آن است. در راستای نیل به اهداف و نیز پاسخ به پرسش پژوهش، پس از اجرای راهبرد پژوهشی کیفی نظریه‌پردازی داده‌بنیاد، طراحی و تبیین الگوی مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با رویکرد اسلامی با اجزای آن استخراج گردید. در روش نظریه‌پردازی داده‌بنیاد پاسخ به پرسش پژوهش، همان الگوی به‌دست آمده و عناصر آن می‌باشد. در حقیقت، یافته‌های پژوهش؛ مقوله‌ها و مؤلفه‌های آن می‌باشند که در این پژوهش، در قالب الگو بیان شده‌اند (دانایی‌فرد و امامی، ۱۳۸۶). از آنجا که در روش داده‌بنیاد، نظریهٔ جدیدی به‌وجود آمده است لذا همه یافته‌ها قابل مقایسه با ادبیات پیشین نبوده و برای بررسی کامل، بایستی در پژوهش‌های آتی مورد بررسی بیشتر و ارزیابی قرار گیرند. الگوی مدیریت امنیت اطلاعات دارای مزایای مختلفی از قبیل بهبود اعتماد سازمانی، تقویت امنیت ملی، تعالی جامعه، امنیت فیزیکی و تقویت امنیت ملی و ... است. این امر میسر نمی‌شود مگر اینکه قبل از آن مدیریت امنیت اطلاعات مورد پذیرش واقع شود. مهم‌ترین مطلبی که در مورد مدیریت امنیت اطلاعات باید موردتوجه قرار گیرد این است که بُعد

انسانی و رفتار انسانی در این مقوله بسیار مهم و حیاتی می‌باشد، زیرا این انسان‌ها هستند که از سیستم‌ها و اطلاعات استفاده کرده و می‌توانند خواسته یا ناخواسته امنیت اطلاعات را زیر سؤال ببرند. باید توجه داشت که در دنیای امروز چیزی به‌عنوان امنیت مطلق و کامل نمی‌تواند وجود داشته باشد، امروزه چه دنیای واقعی و چه دنیای مجازی مانند زندان شیشه‌ای هستند که همیشه احتمال نشر و گسترش اطلاعات به‌صورت ناخواسته و غیرمجاز در آن وجود خواهد داشت اما می‌توان با رعایت برخی مسائل احتمال وقوع این اتفاقات را به مقدار قابل‌ملاحظه‌ای کاهش داد. همان‌طور که قبلاً بیان شد نظام مدیریت امنیت اطاعات به‌عنوان یک راهکار جامع مدیریتی و فنی برای مقابله با مخاطرات امنیتی پذیرفته شده است. لیکن پیاده‌سازی آن نیازمند وجود یک الگوی جامع است (نقیان فشارکی، ۱۳۹۳).

پیشنهادات کاربردی

- پیشنهاد می‌شود برای استقرار الگوی مدیریت امنیت اطلاعات در یک سازمان، براساس مدل ارائه‌شده اقدام شود و نتیجه آن با وضعیت امنیت اطلاعات سازمان‌های دیگری در همان صنعت که از سایر روش‌ها برای استقرار امنیت اطلاعات استفاده می‌کنند، مقایسه گردد.
- مدیران ارشد سازمان، گروهی را برای طراحی سیاست های امنیت اطلاعات در سازمان خود انتخاب نمایند. سازمان در این خصوص می‌تواند از اعضای هیأت علمی و دانشجویان دانشگاه‌ها که در ارتباط با حوزه IT و امنیت اطلاعات تحقیقاتی دارند دعوت به همکاری نماید.
- دوایر متولی در سازمان‌ها دارایی‌های اطلاعاتی سازمان مطبوع خود را شناسایی نموده و محدودیت‌های دسترسی به آن‌ها مشخص گردد.
- پیشنهاد می‌گردد تمامی مسئولیت‌ها و وظایف امنیتی کارمندان، پیمانکاران و مصرف‌کنندگان باتوجه‌به سیاست امنیتی سازمان به‌طور واضح و آشکاری مستند گردیده و پس از تأیید مدیریت ارشد به ایشان ابلاغ گردد.
- دستورالعملی به‌منظور مدیریت تغییرات کل سازمان در حوزه‌های سخت‌افزار و نرم‌افزار و شبکه و ارتباطات بیرونی دقیق، به‌همراه شناسایی دقیق نقاط پرریسک کسب و کار سازمان، تدوین گردیده و پس از تأیید و تصویب مدیریت ارشد به اجرا درآید.
- استفاده از نظر کارشناسان امنیتی و فرآیندهای شهودی در تعیین معماری مطلوب.
- بالابردن هوش سازمانی و افزایش انعطاف در مدیریت سازمان‌ها با تغییر معماری.
- استخراج قوانین انجمنی که به‌واسطهٔ آن‌ها معماری مطلوب داده‌ها و نیز سیستم اطلاعاتی به معمار و طراحان معماری سازمان پیشنهاد گردد.
- توجه جدی تصمیم‌گیران و سیاستگذاران کشور به حوزه مدیریت امنیت اطلاعات به‌عنوان یکی از راهبردهای مهم اجرایی مدیریت اطلاعات.

- با شناسایی عوامل زمینه‌ای مدیریت امنیت اطلاعات در این پژوهش، مقتضی است خط‌مشی‌گذاران و تصمیم‌گیران و مدیران کشور در راستای اجرایی‌شدن این عوامل برنامه‌ریزی نمایند.
- برنامه‌های حمایتی جهت پذیرش و اجرای داوطلبانه الگوی مدیریت امنیت اطلاعات در سازمان‌های دولتی توسط مراجع متولی تدارک دیده شود.
- با عنایت به اینکه مدیریت امنیت اطلاعات را می‌توان از منظر اسلام و منابع دینی و اندیشهٔ رهبران اسلامی مورد توجه قرار داد، پیشنهاد می‌شود این پدیده طی مطالعاتی جداگانه و در چارچوب روش‌شناسی دینی مورد پژوهش واقع شود.
- ایجاد مجموعه‌ای سازمان یافته و بدون افزونگی از داده‌های مرتبط به هم در محیط سازمان.
- افزایش نفوذ و تأثیر به‌کارگیری پایگاه داده مرکزی در سازمان.
- استفاده از DBMS یکپارچه و نرمال‌شده به‌همراه یک اپراتور امنیتی در کنار آن.
- پیشنهاد می‌شود مدیران قبل از پیاده‌سازی سیستم مدیریت امنیت اطلاعات نسبت به فراهم‌نمودن بسترهای لازم فناوری، درون‌سازمانی و در نهایت برون‌سازمانی اقدام نمایند و با برنامه‌ریزی مناسب و اختصاص بودجه‌های لازم، امر پیاده‌سازی سیستم مدیریت امنیت اطلاعات را تسهیل کند.
- در پژوهش‌های آینده، راهکارهای اجرایی برای رسیدن به وضعیت مطلوب، در حوزه فرض مدیریت امنیت اطلاعات برای مدل حاصل از این پژوهش، تدوین گردد.
- محافظت از داده‌ها در برابر دسترسی غیرمجاز، استفاده، تغییر، افشا و تخریب
- تأمین امنیت داده با راهکارهایی همانند حفاظت توسط رمز عبور یا احراز هویت چند عاملی.
- استفاده از تلفن همراه و رمز یکبار مصرف برای ایجاد یک لایه حفاظتی اضافه علاوه‌بر رمز عبور معمولی.
- اقدامات احتیاطی مانند پشتیبان‌گیری از دستگاه‌های مورد استفاده به‌صورت منظم و ایجاد رمزهای عبور پیچیده و طولانی.

فهرست منابع و مآخذ:

کتاب‌ها

میوالد، اریک. (۱۳۸۵). مبانی امنیت شبکه. ترجمه: گروه پژوهشی فناوری اطلاعات جهاد دانشگاهی صنعتی شریف. تهران: انتشارات انستیتو ایز ایزان.

مقالات

امینی، معصومه؛ وکیلی مفرد، حسین؛ صابری محمدکریم. (۱۳۹۸). «شناسایی عوامل موثر بر مدیریت امنیت اطلاعات کتابخانه‌ها و مراکز اطلاع‌رسانی دانشگاه علوم پزشکی همدان». تحقیقات کتابداری و اطلاع‌رسانی دانشگاهی، ۳، ۵۳.

حدادی هرندی، علی‌اکبر؛ والمحمدی، چنگیز و صالحی صدقیانی، جمشید. (۱۳۹۸). «مدیریت امنیت اطلاعات در کسب و کار هوشمند». علمی پژوهشی مدیریت بحران ۸، (ویژه‌نامه هوشمندسازی)، ۲۵-۳۳.

دانایی‌فرد، حسن؛ ابدالی، رقیه؛ محمودی کوچکسرایی، علی‌اصغر. (۱۳۹۹). «پژوهش‌های فساد و سلامت اداری در ایران: مرور دامنه‌ای (حیطه‌ای)»، دانش حسابرسی،۲۰(۷۹)، ۲۰۱-۲۱۸.

دانایی‌فرد، حسن؛ رجب‌زاده، علی؛ حصیری، اسد. (۱۳۸۸). «ارتقا اعتماد درون سازمانی در بخش دولتی: بررسی نقش شایستگی مدیریتی مدیران». پژوهش‌های مدیریت، شماره چهارم، ۵۹-۹۰.

دهقانی، محمد؛ رحمت‌پسند فتیده، زری؛ آراسته، زهرا؛ شکری‌زاده بزنجانی و کبری، آگاهی. (۱۳۹۸). «نگرش و عملکرد کارکنان بخش مدیریت اطلاعات سلامت بیمارستان‌های ایران نسبت به امنیت اطلاعات سلامت». مجله مدیریت اطلاعات سلامت، شماره اول، ۹-۳.

شمس، شهاب‌الدین؛ اسفندیاری مقدم، امیر. (۱۳۹۴). «ارتباط ابعاد مختلف اعتماد سازمانی با رضایت شغلی کارکنان». مطالعات مدیریت (بهبود و تحول)، شماره ۷۷، ۱۷۱- ۱۸۵.

عاشوری‌زاده، سهیلا. (۱۳۹۱). «رابطه فرهنگ سازمانی با مدیریت امنیت اطلاعات در بانک ملی ایران». پایان‌نامه کارشناسی ارشد. دانشگاه علامه طباطبایی.

محمدی، مهین؛ شیخ ظاهری، عباس؛ کرمانی، فرزانه. (۱۳۹۸). «مقایسه الگوریتم‌های بیمار محور برای امنیت اطلاعات سلامت در شبکه‌های اجتماعی سلامت و محیط ابر». مجله اطلاع‌رسانی پزشکی نوین، دوره پنجم، شماره دوم، ۶۸-۷۹.

پایان‌نامه‌ها

آرام، محمدرضا. (۱۳۸۸). «بررسی و سنجش مؤلفه‌های مؤثر بر مدیریت امنیت اطلاعات شرکت گاز پارس جنوبی». پایان‌نامه کارشناسی ارشد دانشگاه شهید بهشتی.

English sources

Boritz, J. E. (۲۰۰٤). *Managing enterprise information integrity: security, control, and audit issues*. Isaca.

Chang. E. (۲۰۰۷). An Investigation of Organizational Culture on Information Security Management. Academy of Management Journal, ۳۵: ٤۲۱-٤۳۸.

Chathoth, P. K., Mak, B., Sim, J., Jauhari, V., & Manaktola, K. (۲۰۱۱). Assessing dimensions of organizational trust across cultures: A comparative analysis of US and Indian full service hotels. *International Journal of Hospitality Management*, *30* (۲), ۲۳۳-۲٤۲.

Hansche, S. (۲۰۰۱). Designing a security awareness program: Part ۱. *Information systems security*, *9* (٦), ۱-۹.

Heidari, S., & Mohammadi, S. (۲۰۱۲). A New Model for Information Security Management in Service-Oriented Enterprise Architecture. *American Journal of Scientific Research*, (۷٦), ۱۱۴-۱۳۲.

Ho, S. M. (۲۰۰۸). A Framework of Coordinated Defense. In *Proceedings of the Second International Conference on Computational Cultural Dynamics* (pp. ۳۹-٤٤).

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (۲۰۰۳). An integrated system theory of information security management. *Information Management & Computer Security*.

Kadam, A. W. (۲۰۰۷). Information security policy development and implementation. *Information Systems Security*, *16* (٥), ۲٤٦-۲٥٦.

Kambwiri, L. (۲۰۱۲). An Appraisal of Information Security Management at Chancellor College, University of Malawi.

Kauspadiene, L., Cenys, A., Goranin, N., Tjoa, S., & Ramanauskaite, S. (۲۰۱۷). High-level self-sustaining information security management framework. *Baltic Journal of Modern Computing*, *5* (۱), ۱۰۷.

Kline, R. B. (۲۰۱۱). Principles and practice of structural equation modeling: Guilford press.

Kim, S., Kim, S., & Lee, G. (۲۰۰۹). Structure design and test of enterprise security management system with advanced internal security. *Future Generation Computer Systems*, ۲٥(۳), ۳٥۸-۳٦۳.

Mitchell, R. C., Marcella, R., & Baxter, G. (۱۹۹۹). Corporate information security management. *New Library World*.

Park, E. H., Kim, J., & Park, Y. S. (۲۰۱۷). The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security*, *65*, ٦٤-۷٦.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (۲۰۱٤). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, *42*, ۱٦٥-۱۷٦.

Veiga. A. & Martins, N. (۲۰۱۷) "Defining and Identifying Dominant Information Security Cultures and Subcultures." Computers & Security, ۷۰: ۷۲-۹٤.

Vermeulen, C., & Von Solms, R. (۲۰۰۲). The information security management toolbox–taking the pain out of security management. *Information management & computer security*.

Whitener, E. M. (۲۰۰۱). Do "high commitment" human resource practices affect employee commitment? A cross-level analysis using hierarchical linear modeling. *Journal of management*, *27* (٥), ٥۱٥-٥۳٥.

Whitener, E. M., Brodt, S. E., Korsgaard, M. A., & Werner, J. M. (۱۹۹۸). Managers as initiators of trust: An exchange relationship framework for understanding managerial trustworthy behavior. *Academy of management review*, *23* (۳), ٥۱۳-٥۳۰.

Whitley, R. (۱۹۹۹). *Divergent capitalisms: The social structuring and change of business systems*. OUP Oxford.

Whitman, M. E., & Mattord, H. J. (۲۰۱۱). *Principles of information security*. Cengage Learning.