University of Sistan and Baluchestan

Public Management Researches

Print ISSN: 2538 - 3418 Online ISSN: 2676 - 7880

Iranian Academy of Management Sciences

Identifying and Prioritizing the Effective Factors of the Information Networks Security of Sistan and Baluchestan Province Prisons

Hadi Esmaeeli*[1], Shahpour Rahmani[2], Ahmad Kazemi[3]

1. Assistant Professor of Information Technology Engineering Department, Faculty of Electrical and Computer Science, University of Sistan and Baluchestan, Zahedan, Iran.(Corresponding Author) Email: esmaeeli@ece.usb.ac.ir
2. Instructor of Computer Science Department, Faculty of Mathematics, Statistics and Computer Science, University of Sistan and Baluchestan, Zahedan, Iran.
3. Instructor of Computer Science Department, Faculty of Mathematics, Statistics and Computer Science, University of Sistan and Baluchestan, Zahedan, Iran.

Abstract

The existence of information technology (IT) system, nowadays, does not guarantee appropriate outcomes for organizations, unless they ascertained their information security protocols and procedures are well-designed and their IT assets are protected from external and internal threats. The purpose of the present study is to identify and prioritize the factors which are influential in the security of the information networks of prisons of Sistan and Baluchestan (S&B) province. To this end, first a list of important criteria was compiled. Then, the effective factors of the security of electronic information networks of Prison Directorate General of S&B were identified by filling out a questionnaire. The population of the study were experts, specialists and university professors who were fully acquainted with the concept of IT network security. Since the statistical community was limited, there was no need for sampling. The criteria were then weighted and ranked using fuzzy analytical hierarchy process (AHP). The results of the study indicated that the field of infrastructure, content and application are of the highest importance from the perspectives of policy makers and prison governors.

Introduction

Some institutions and organizations have more important information from this regard, information security is more important for them. The General Directorate of Prisons in Sistan and Baluchestan Province has vital information resources, the loss of which and its leakage can cause great harm and violate the privacy and dignity of individuals; For example, CCTV images that may provide valuable information to abusers inside and outside the organization. The organization has an independent workgroup for information technology management, in which the number of experts with related education is more than ten. In this sub office, there are software systems: accounting and finance, warehousing, salaries and property, secretariat, administrative correspondence and archives. The data collected to identify the

current IT situation of the General Directorate of Prisons in the fields of software, hardware, network and human resource, Indicates the lack of software to expedite internal affairs and appropriate security hardware within the organization and appropriate procedures for establishing communication network security.

Case study

This study intends to identify and prioritize the factors affecting the security of information networks in the General Directorate of Prisons of Sistan and Baluchestan Province.

Theoretical framework

Since the phenomenon of information technology in the General Directorate of Prisons of the province and in particular Zahedan Prison is not very old, determining its strategies requires multifaceted information; In this research, a pluralistic approach will be followed in the method and tools of data collection. In other words, this research tries to combine the characteristics of quantitative data (survey) and qualitative data (content analysis and archival studies) with a pluralistic approach and thus add to the richness of the research. The pluralistic approach in collecting information about the security of electronic information networks in the province's prisons and prioritizing them allows qualitative and in-depth analyzes to be combined with statistical analysis, increasing the internal validity of the test and the reliability of the collected information. Also reveal aspects of the research topic that may have been hidden.

In terms of the purpose of this research, it is a descriptive-field research. Most of the analyzes performed in different stages of the research are quantitative and qualitative methods that are performed in the form of document analysis, stakeholder analysis and quantitative data analysis.

Methodology

In this research, a questionnaire was used as one of the research tools and according to the scope of the subject and the multiplicity of indicators, questionnaires consisting of several sections were developed and in order to collect the required data, experts and those involved in ICT development in Some organizations as well as the General Directorate of Prisons were studied as a research community. Through face-to-face interviews and completing a questionnaire, the opinions of experts and managers of the studied organizations on adding, deleting or merging criteria were obtained. According to the results of this questionnaire and interviews, the most important criteria in the four fields of "infrastructure, content and application" and "policies and strategies" and "institutions" and "human resources" and 23 sub-criteria identified in the framework of these four areas was categorized. To obtain the relative weight of the four main fields as well as the identified sub-criteria, questionnaires were designed based on pairwise comparisons and fuzzy Analytical Hierarchy Process (AHP) method. These questionnaires were answered by employees and information technology experts of government organizations. In order to analyze the data with a fuzzy approach, the numbers obtained from the questionnaires should be converted into their equivalent triangular fuzzy numbers.

To analyze these data, fuzzy AHP method and Chang's developmental analysis method were used.

Discussion and Results

The results obtained from the implementation of fuzzy AHP algorithm and Chang developmental analysis method on the research data extracted from the questionnaires show that the infrastructure, content and application context with a relative weight of 0.314 is the most important. After infrastructure, content and application, human resources, policy and strategy and institutions with the weight of 0.272, 0.231 and 0.183 are in the next positions, respectively. The incompatibility rate of comparisons in this section is (CIg = 0.09) and (CIm = 0.09) and since this value is less than zero, the compatibility of the questionnaires is acceptable.

Conclusion

The ranking of quad criteria for improving the security of electronic information networks of prisons in Sistan and Baluchestan province indicates that the field of infrastructure, content and application has the highest importance for the managers and decision-making experts. This implies that the overall managerial attitude of the general administration is only based on the creation of technical-telecommunication platforms. The existence of such an attitude seems to be promising to increase the level of infrastructure and content and human resources. However, the factor of infrastructure, content and application is decisive and can be considered as the first evaluation criterion. In addition to the infrastructure, content and application context, the human resources context is also of great importance. From the point of view of the experts of the society which has been studied, the two contexts of "policies and strategies" and "institutions" are less important than the two contexts of "infrastructure, content and application" and "human resources". This indicates that the factors related to these fields are of lower importance compared to the criteria that are directly related to the context of infrastructure, content and application and human resources.

Keywords: Prison, Electronic Network, Information Security**.**

Article Type: Research Article

Cite this article: Esmaeeli, H., Rahmani, Sh., & Kazemi, .(2022). A Identifying and Prioritizing the Effective Factors of the Information Networks Security of Sistan and Baluchestan Province Prisons, *Public Management Researches*, 15 (55), 305-320. (In Persian)

DOI:10.22111/JMR.2022.34281.5079

Received: 13 May. 2020 **Revised:** 20 Nov. 2021 **Accepted**: 12 Mar. 2022

Publisher: University of Sistan and Baluchestan

پژوهش‌های مدیریت عمومی
شاپا چاپی: ۳۴۱۸-۲۵۳۸ شاپا الکترونیکی: ۷۸۸۰-۲۶۷۶
دانشگاه سیستان و بلوچستان
انجمن علوم مدیریت ایران

عوامل مؤثر بر ایجاد امنیت در شبکه‌های اطلاعاتی اداره کل زندان‌های استان سیستان و بلوچستان و اولویت‌بندی آنها

هادی اسماعیلی درمیان*[۱]– شاهپور رحمانی[۲]– احمد کاظمی[۳]

۱. نویسنده مسئول، استادیار، عضو هیات علمی دانشگاه سیستان و بلوچستان، زاهدان، ایران.
esmaeeli@ece.usb.ac.ir
۲. مربی، عضو هیات علمی دانشگاه سیستان و بلوچستان، زاهدان، ایران.
۳. مربی، عضو هیات علمی دانشگاه سیستان و بلوچستان، زاهدان، ایران

چکیده

امروزه داشتن یک سیستم فناوری اطلاعات به معنای موفقیت یا تضمین نتایج خوب برای سازمان نیست، مگر اینکه سازمانها اطمینان حاصل کنند از اینکه پروتکل‌ها و رویه های امنیت اطلاعاتی آنها به خوبی طراحی شده و دارایی‌های فناوری اطلاعات آنها در برابر تهدیدات خارجی و داخلی محافظت می-شوند. هدف تحقیق حاضر شناسایی عوامل مؤثر بر ایجاد امنیت در شبکه‌های اطلاعاتی اداره کل زندان‌های استان سیستان و بلوچستان و اولویت‌بندی آنها می باشد. برای این منظور ابتدا فهرستی از معیارهای حائز اهمیت تدوین شد و سپس از طریق تکمیل نمودن پرسشنامه، عوامل مؤثر بر ایجاد امنیت شبکه های اطلاعاتی الکترونیکی اداره کل زندان‌ها مشخص گردید. جامعه آماری در این تحقیق شامل کارشناسان و متخصصان خبره و اساتید دانشگاهی می‌شود که آشنایی کامل با کلیات امنیت شبکه را نیز داشته باشند که بدلیل محدودیت جامعه آماری، نمونه‌گیری ضرورتی ندارد. سپس با تجزیه و تحلیل داده‌ها از طریق روش تحلیل سلسله مراتبی فازی معیارها وزن‌دهی و رتبه بندی شدند. نتایج تحقیق حاکی از آن است که حوزه زیرساخت و محتوی و کاربرد از دیدگاه مدیران و خبرگان تصمیم‌گیرنده دارای بالاترین اهمیت است.

واژه‌های کلیدی : زندان، شبکه‌های اطلاعاتی، امنیت اطلاعات

استناد: اسماعیلی درمیان، هادی؛ رحمانی، شاهپور؛ کاظمی، احمد (۱۴۰۱). عوامل موثر بر ایجاد امنیت در شبکه‌های اطلاعاتی اداره کل زندان‌های استان سیستان و بلوچستان و اولویت‌بندی، *پژوهش‌های مدیریت عمومی*. ۱۵(۵۵)، ۳۲۰-۳۰۵ .

تاریخ دریافت: ۱۳۹۹/۰۲/۲۴ **تاریخ ویرایش:** ۱۴۰۰/۰۸/۲۹ **تاریخ پذیرش:** ۱۴۰۰/۱۲/۲۱
نوع مقاله: علمی پژوهشی **DOI:** 10.22111/JMR.2022.34281.5079
ناشر: دانشگاه سیستان و بلوچستان

مقدمه

در عصر حاضر اطلاعات بعنوان یک منبع استراتژیک و یک شایستگی کلیدی برای سازمان‌ها از اهمیت ویژه‌ای برخوردار است. از این رو برای استفاده صحیح از این منبع پرمنفعت، موضوع امنیت اطلاعات در دستور کار سازمان‌های پیشرو قرار گرفته است. در عصر حاضر همچنین پیشرفت‌های شگرفی در زمینه ابزارها و فناوری‌های انتقال این اطلاعات صورت گرفته است و به دلیل گسترش این فناوری‌های اطلاعاتی و الکترونیکی بخش عظیمی از ارائه خدمات و فعالیت‌های دولتی از شیوه سنتی به الکترونیکی تغییر شکل پیدا کرده و دولت الکترونیک را بوجود آورده است. دولت الکترونیک زمانی به حقیقت می‌پیوندد که امنیت آن نیز تامین شده باشد. دولت الکترونیکی از طریق بسترهای اینترنتی و شبکه‌ای که امکان دستیابی به اطلاعات دقیق، سریع و آسان را فراهم می‌کند امکان‌پذیر می‌باشد. ضمن مهم دانستن زیرساخت‌های شبکه‌ای و اینترنتی باید این نکته را در نظر داشت که برای پیاده‌سازی دولت الکترونیک شاید مهم‌ترین عامل تاثیرگذار، فرهنگ‌سازی در زمینه‌ی استفاده از ابزارهای دولت الکترونیک و ایجاد تعهد و اعتماد نسبت به آن در بین مدیران، کارکنان و مشتریان باشد. کنترل دستیابی و نحوه استفاده از اطلاعات به اشتراک گذاشته شده و بطور کلی امنیت اطلاعات در شبکه‌های اطلاعاتی، بعنوان چالشی برای سازمان‌های امروزی مطرح شده است که لزوم به کارگیری پژوهش در این زمینه را دو چندان کرده است. همچنین با پیدایش شیوه‌های نوین مدیریت دولتی، جنبه‌های جدیدی از تهدیدات امنیتی نیز ظهور پیدا کرده است. برای پیاده‌سازی امنیت تنها توجه به مسائل فنی کافی نیست بلکه ایجاد سیاست‌های کنترلی و استانداردکردن آن و همچنین ایجاد روالهای صحیح، درصد امنیت اطلاعات را بالا خواهد برد و همین امر بکارگیری سیستم-های، مدیریت امنیت اطلاعات را الزامی کرده است *(Bohrani & Yazdi, 2019)*.

بعضی از نهادها و سازمان‌ها اطلاعات مهم تری در اختیار دارند و از این حیث امنیت اطلاعات برای آنها اهمیت دو چندانی پیدا می‌نماید. گردش اطلاعات درون سازمان از یک سو، ارتباط با نهادهای دیگر از سویی دیگر به اهمیت امن بودن اطلاعات می‌افزاید؛ اما نکته حایز اهمیت در بسیاری از سازمان‌ها، داشتن اطلاعات حساس از افراد ثالث است که این اطلاعات در صورتی که به بیرون از سازمان درز پیدا کند باعث مشکلاتی جبران ناپذیر

خواهد شد. اطلاعات حساس و محرمانه، در دسترس بودن اطلاعات، مخفی نگاه داشتن اطلاعات از دید افراد فاقد صلاحیت لازم، اهمیت امنیت اطلاعات و شبکه‌های کامپیوتری را نشان می‌دهد *(Ghasemi Shabankareh, Mokhtari & Amini Lari, 2017)*. در سازمان مورد بررسی ما در این پژوهش (سازمان زندان‌ها و اقدامات تامینی و تربیتی) نیز امنیت اطلاعات از جنبه‌های مختلفی قابل بررسی است. اطلاعات حساس که از دست دادن آن‌ها و درز آن‌ها به بیرون باعث صدمات بسیار و نقض حریم خصوصی و حیثیت افراد می‌شود؛ به عنوان مثال تصاویر دوربین‌های مداربسته که اطلاعات بسیار ارزشمندی را ممکن است به سوء استفاده‌گران در داخل یا بیرون سازمان بدهد.

اداره کل زندان‌های استان سیستان و بلوچستان واحد سازمانی مستقلی برای مدیریت فناوری اطلاعات دارد که تعداد کارشناسان دارای تحصیلات مرتبط در این واحد بیش از ده نفر می‌باشند. در این سازمان سیستم‌های نرم‌افزاری: حسابداری و مالی، انبارداری، حقوق و دستمزد و اموال، دبیرخانه، مکاتبات اداری و بایگانی وجود دارند. داده‌هایی که جهت شناخت وضعیت موجود انفورماتیکی اداره کل زندان‌های استان در حوزه‌های نرم‌افزار، سخت‌افزار، شبکه و نیروی انسانی جمع‌آوری گردید، بیانگر فقدان نرم‌افزارها جهت تسریع امور داخلی و سخت‌افزارهای امنیتی مناسب درون سازمان و روال‌های مناسب برای برقراری امنیت شبکه‌های ارتباطی می‌باشد.

از اینرو این پژوهش درنظر دارد با شناسایی عوامل مؤثر بر ایجاد امنیت در شبکه‌های اطلاعاتی اداره کل زندان‌های استان سیستان و بلوچستان و اولویت‌بندی آن‌ها، بتواند گامی در جهت برقراری بیشتر امنیت در شبکه‌های ارتباطی این سازمان بردارد.

پیشینه پژوهش

سیستم و شبکه‌های اطلاعاتی غالباً در معرض انواع مختلف تهدیدات هستند که می‌توانند خسارت‌هایی ایجاد کنند که منجر به خسارات مالی قابل توجهی شود. خسارات امنیتی اطلاعات می‌تواند از ضررهای ناچیز تا تخریب کل سیستم اطلاعات باشد. تأثیرات تهدیدات مختلف بسیار متفاوت است: برخی بر محرمانه بودن یا یکپارچگی داده‌ها تأثیر می‌گذارند، در حالی‌که برخی دیگر در دسترس‌پذیری یک سیستم تأثیر می‌گذارند. در حال حاضر، سازمان‌ها در تلاشند تا بفهمند تهدیدهای موجود در مورد دارایی‌های اطلاعاتی آنها

چه هستند و چگونه به وسایل لازم برای مبارزه با آنها که همچنان یک چالش است، دست یابند *(Jouinia, Ben, Ben Arfa Rabai & Ben Aissa, 2014)*.

در سازمان‌های امروز که اغلب دارای ابعاد و ساختارهای پیچیده و از نظر فیزیکی توزیع شده هستند، تنها ذکر این که چه کارهایی باید توسط چه کسانی (شرح وظایف) انجام شود، کافی نیست. بلکه فرآیندها، داده‌ها، نقش افراد، سیستم‌ها و فنّاوری‌های مورد استفاده، باید با اهداف و راهبردهای سازمان همخوانی داشته باشند. چنین امری مستلزم آن است که سازمان دارای یک نقشه از تمام ابعاد خود باشد تا بتواند با استفاده از این نقشه، روابط بین اجزاء سازمان را درک نموده و در صورت نیاز با تغییرات هماهنگ نماید. این نقشه بایستی حاوی اطلاعات افراد، فرآیندها، مکان‌ها، سیستم‌ها و دیگر ابعاد و خصوصیات سازمان باشد. امنیت اطلاعات عبارت است از حفاظت زیرساخت‌های فناوری اطلاعات و تضمین دردسترس‌بودن آن. چانگ و هو (۲۰۱۶)، به عوامل سازمانی موثر در پیاده‌سازی مدیریت امنیت اطلاعات پرداختند. این پژوهشگران ضمن تاکید بر نیاز سازمان‌ها به ساختارهای مدیریتی برای حفظ دارائی‌های اطلاعاتی، این گونه ساختارهای امنیتی را سلاحی موثر برای بقاء در عرصه رقابت عنوان می‌کنند. هر سازمان باید ارزش اطلاعات خود را ارزیابی کند و سپس یک خط مشی امنیتی برای مواردی که باید مورد محافظت قرار گیرد مشخص نماید *(Hariri & Nazari, 2012)*.

در شبکه‌های اطلاعاتی، اطلاعات نقش بسیار حیاتی برای سازمان‌ها ایفا می‌نماید و به علت وجود هکرها و شکل‌گیری انواع جرایم اینترنتی، امروزه اهمیت حفظ و نگهداری اطلاعات بویژه اطلاعات محرمانه بیش از پیش احساس می‌شود بنابراین مهمترین وظیفه سازمان‌ها، اجرا و پیاده‌سازی یکی از استانداردهای مدیریت امنیت اطلاعات می‌باشد. سیستم مدیریت امنیت اطلاعات می‌تواند بعنوان ابزاری در جهت طراحی، پیاده‌سازی و کنترل امنیت نرم‌افزار و سخت فزار یک سیستم اطلاعاتی به سازمان‌ها در جهت استقرار یک فضای تبادل اطلاعاتی ایمن کمک کند *(Khaleghi , 2015)*.

هر چه نقش یک سازمان در نظم بخشیدن به جامعه حساس‌تر باشد، لزوم بکارگیری روش‌های جدید و مطابق با آخرین تحولات و دستاوردهای فناوری اطلاعات بیشتر می‌گردد. این امر سازمان را مجبور می‌کند تا درب های خود را به سوی دنیای مجازی و الکترونیکی

این فناوری بگشایند. دنیایی که در آن فعالیت‌ها بسیار سریع‌تر و مطمئن‌تر انجام می‌گیرد و نیازی به تراکم جمعیت در دنیای فیزیکی نخواهد بود. این چنین راهبردی می‌تواند از هزینه‌های بالای انجام کار، برخوردها و ناراحتی‌های روانی، فساد اداری و ده‌ها مشکل دیگری که همه روزه در ادارات و سازمان‌های بزرگ وجود دارد، بکاهد.

هر روز خبرهای زیادی در مورد تهدیدات و مشکلات بوجود آمده برای سیستم‌های اطلاعاتی بسیاری از سازمان‌ها، بانک‌ها و حتی سازمان‌هایی که ظاهراً اقدامات امنیتی نیز انجام داده‌اند می‌شنویم و از طرفی بسیاری از کاربران این سیستم‌ها حتی کسانی‌که سالهاست با کامپیوتر در ارتباط هستند، درک کافی درباره واقعیت این تهدیدات و راهکارهای مقابله با آن ندارند.

هدف از امنیت اطلاعات در یک سازمان، حفظ سرمایه‌های آن (نرم‌افزاری، سخت افزاری، اطلاعاتی و ارتباطی، و نیروی انسانی) در مقابل هرگونه تهدید (اعم از دسترسی غیرمجاز به اطلاعات، خطرات ناشی از محیط و سیستم، و خطرات ایجاد شده از سوی کاربران) است و برای رسیدن به این هدف، نیاز به یک برنامه منسجم است. فرایند امنیت اطلاعات را نمی‌توان یک باره در یک نظام مدیریتی پیاده کرد بلکه نیازمند یک فرایند مداوم، شامل این مراحل است:

۱. برنامه ریزی- برپایی شرایط اولیه سیستم
۲. اجرا- پیاده سازی و اجرای سیستم
۳. ارزیابی و کنترل- فعالیت‌های نظارتی و بررسی فعالیت‌های انجام شده
۴. بهبود و اصلاح- فعالیت‌های نگهداری و بهبود مستمر *(Broderick, 2006)*.

امنیت اطلاعات یکسری اقداماتی است که برای حفاظت از اطلاعات و سیستم‌های اطلاعاتی طراحی می‌شوند. بنابراین امنیت اطلاعات تنها خود اطلاعات را پوشش نمی‌دهد بلکه تمامی زیرساختی که استفاده از آنرا فراهم می‌کند را نیز شامل می‌شود. آن شامل سخت افزار، نرم افزار، تهدیدات، امنیت فیزیکی عامل‌های انسانی نیز می‌شود که هرکدام از این اجزاء مشخصه‌های خود را دارند و باید شناسایی و پایش شوند. بنابراین در عصر امروزی که اینترنت در تمام جاها نفوذ کرده است، امنیت اطلاعات یک نقش کلیدی را دارد. امروزه شاهد آن هستیم که اطلاعات زیادی از سازمان‌های مختلف به سرقت می‌روند و همچنین

هر روزه با سهولت بیشتری اطلاعات، فناوری‌ها و ابزارهای نفوذ گسترده‌ای در اختیار همگان قرار می‌گیرد بنابراین لازم است که اقدامات امنیتی بسیار مناسبی برای سازمان‌ها مخصوصا سازمان‌های امنیتی انجام داد.

در این بین از نقش بسیار پررنگ افراد شاغل در سازمان‌ها در از بین بردن امنیت اطلاعات نباید غافل شد به حدی که انسان را در لایه‌های امنیت، در با اهمیت‌ترین لایه قرار می‌دهند، یک انسان می‌تواند به راحتی کاری انجام دهد که هزینه‌های فیزیکی بسیاری بر روی امنیت اطلاعات را بی اثر جلوه دهد، ناگفته نماند که انسان ضعیف‌ترین عنصر زنجیره امنیت است. در تحقیق دیگری نشان داده شد که پیشرفت‌های بی‌شمار فنی در فناوری اطلاعات همیشه محیط‌های ایمن‌تری ایجاد نمی‌کند. و امنیت اطلاعات فقط به عنوان یک مشکل فنی توصیف نمی‌شود. رایانه‌ها توسط مردم اداره می‌شوند و این بدان معنی است که عامل انسانی یک مولفه مهم در امنیت اطلاعات است. بنابراین، پیشنهاد می‌شود، برای جلوگیری از نقض اطلاعات و داده‌ها، سازمان‌ها باید یک چارچوب امنیتی جامع را با استفاده از عامل انسانی اتخاذ کنند*(Safianu &, Twum, 2016)*.

امروزه اکثر کارهای سازمان‌ها از طریق سیستم‌های اطلاعاتی انجام می‌شود و حجم زیادی از اطلاعات حیاتی آن‌ها در این سیستم‌ها ذخیره می‌شوند. این امر یکسری سوالات مهم را به همراه دارد.

سوالات تحقیق

با توجه به موضوع عوامل مؤثر بر ایجاد امنیت در شبکه‌های اطلاعاتی اداره کل زندان-های استان سیستان و بلوچستان و اولویت‌بندی آنها، سوالات تحقیق عبارتند از:

۱. عوامل مؤثر بر ایجاد امنیت در شبکه‌های اطلاعاتی اداره کل زندان‌های استان سیستان و بلوچستان کدامند؟

۲. اولویت‌بندی عوامل مؤثر بر ایجاد امنیت در شبکه‌های اطلاعاتی اداره کل زندان-های استان سیستان و بلوچستان به چه صورت می‌باشد؟

روش‌شناسی تحقیق

الگوی تدوین عوامل مؤثر بر ایجاد امنیت در شبکه‌های اطلاعاتی اداره کل زندان‌های استان سیستان و بلوچستان و اولویت‌بندی آنها، روش‌شناسی خاص خود را می‌طلبد. از آن

جایی که پدیده فناوری اطلاعات در اداره کل زندان‌های استان و بطور خاص زندان زاهدان از قدمت چندانی برخوردار نیست، تعیین راهبردهای آن به اطلاعات چندجانبه نیاز دارد؛ در این پژوهش رویکرد کثرتگرایانه در روش و ابزار گردآوری اطلاعات دنبال خواهد شد. به عبارتی دیگر، این پژوهش درصدد است با رویکردی کثرتگرایانه خصوصیات داده های کمی (پیمایش) و داده‌های کیفی (تحلیل محتوا و مطالعات آرشیوی) را با یکدیگر تلفیق نموده و از این طریق بر غنای تحقیق بیفزاید. رویکرد کثرت‌گرایی در جمع‌آوری اطلاعات مربوط به امنیت شبکه‌های اطلاعاتی الکترونیکی زندان‌های استان و اولویت بندی آنها این امکان را فراهم می‌کند تا تحلیل‌های کیفی و عمیق با کند و کاوهای آماری تلفیق شوند، اعتبار درونی آزمون و پایایی اطلاعات گردآوری شده افزایش یابد و همچنین جنبه‌هایی از موضوع پژوهش که احتمال پنهان ماندن آنها بوده است آشکار شود (*Faghihi & Bamdadsofi, 1999*).

از نظر هدف این تحقیق، پژوهشی، توصیفی- میدانی به شمار می‌رود. عموم تحلیل‌های صورت گرفته در مراحل مختلف پژوهش، به روشهای کمی وکیفی بوده که در قالب شیوه-های تحلیل اسناد، تحلیل ذینفع و تحلیل دادهای کمی صورت می‌پذیرد.

در این تحقیق از ابزار پرسشنامه به عنوان یکی از ابزارهای تحقیق استفاده شد و با توجه به گستردگی موضوع و کثرت شاخص‌ها پرسشنامه‌های متشکل از چند بخش تدوین گردید و به منظور گردآوری داده‌های موردنیاز، صاحب نظران و دست اندرکاران توسعه فناوری اطلاعات وارتباطات در برخی سازمان‌ها و نیز اداره کل زندان‌ها به عنوان جامعه تحقیق مورد مطالعه قرار گرفت.

جهت شناسایی عوامل موثر بر امنیت شبکه های اطلاعاتی الکترونیکی زندان های استان سیستان و بلوچستان و اولویت‌بندی آنها، پس از بررسی پیشینه و مطالعه تحقیقات انجام شده در حوزه سیستم مدیریت امنیت اطلاعات، فهرستی از بسترهای موثر که بیشترین تکرار را در تحقیقات انجام شده داشتند، شناسایی شد و بر اساس شاخص‌های اهداف تحقیق در وضعیت مطلوب و در قالب چهار حوزه کلی دسته‌بندی گردید. فهرست بدست آمده در اختیار خبرگان و کارشناسان حوزه مورد مطالعه قرار گرفت. از طریق انجام مصاحبه حضوری و تکمیل نمودن پرسشنامه، نظر کارشناسان و مدیران سازمانهای مورد مطالعه راجع به افزودن، حذف و یا ادغام معیارها اخذ شد. با توجه به نتایج بدست آمده از این

پرسشنامه و مصاحبه‌های صورت گرفته، مهم‌ترین معیارها در چهار حوزه زیرساخت و محتوی و کاربرد، سیاست‌ها و راهبردها، نهادها و منابع انسانی با استفاده از مدل UNDP (*Ronaghan, 2017*) و ۲۳ زیرمعیار شناسایی شده در چهارچوب این چهار حوزه دسته-بندی شدند.

جدول شماره ۱: معیارهای اصلی امنیت شبکه‌های اطلاعاتی الکترونیکی زندان های استان بر اساس مدل UNDP[1]

معیارهای اصلی	زیر معیارها
سیاست ها و راهبردها	۱.تهیه و تدوین قوانین و آیین‌نامه‌های اجرایی مدیریت امنیت اطلاعات در اداره کل زندان‌های استان ۲.تعیین و بازنگری میزان حق دسترسی کارکنان و کاربران اداره کل زندان‌های استان به اطلاعات ۳.برنامه‌ریزی مبتنی بر راهبردها و اهداف بلندمدت در اداره کل زندان‌های استان ۴.شناسایی اولویت‌های امنیت اطلاعات و شبکه ارتباطی اداره کل زندان‌های استان ۵.جهت‌گیری و سیاست‌گذاری مشخص در حوزه امنیت فناوری اطلاعات و ارتباطات ۶.توجه ویژه به امنیت فناوری اطلاعات و ارتباطات در اسناد بالادستی
منابع انسانی	۱.مدیریت و طبقه‌بندی مناسب نیروی انسانی اداره کل زندان‌های استان ۲.فرهنگ پذیرش و باور کارکنان اداره کل زندان‌های استان از حوزه فناوری اطلاعات و ارتباطات ۳.توسعه فرهنگ به کارگیری امکانات رایانه‌ای در بین پرسنل اداره کل زندان‌های استان ۴.استفاده از نیروهای متخصص فناوری اطلاعات و ارتباطات ۵.تعهد مدیریت نسبت به پیاده سازی امنیت اطلاعات و تعیین مسئولیت و وظایف کارکنان ۶.آشنایی مدیران و کارکنان با دستاوردها و کاربردهای فناوری اطلاعات ۷.برگزاری دوره‌های تحصیلی، آموزشی و آگاه‌سازی مدیران و کارکنان
زیرساخت و محتوی و کاربرد	۱.تامین امنیت شبکه ارتباطی و اطلاعاتی اداره کل زندان‌های استان ۲.بهره‌گیری از استانداردهای سخت افزاری و نرم افزاری ۳.به روزرسانی مرتب تجهیزات، نرم‌افزارها، وب سایت و سامانه‌های اداره کل زندان‌های استان ۴.آموزش الکترونیک، کاربردها، محتوی دیجیتال ۵.سامانه گزارش‌گیری و گزارش رخدادها ۶.بهینه‌سازی و بهبود زیرساخت مخابراتی و شبکه ارتباطی اداره کل زندان‌های استان

[1] United Nations Development Programme

نهادها	۱.استفاده از بخش خصوصی فعال در حوزه فناوری اطلاعات و ارتباطات در اداره کل زندان‌های استان ۲.هماهنگی مناسب میان دستگاه‌های مختلف دولتی مرتبط با اداره کل زندان‌های استان در بهره-گیری از فناوری اطلاعات و ارتباطات ۳.به کارگیری از استانداردهای مطرح در حوزه فناوری اطلاعات و ارتباطات در شرکت‌های خصوصی جهت ارزیابی راحت‌تر آنها و برون سپاری مطمئن‌تر پروژه‌ها به آنها ۴.دسترسی اداره کل زندان‌های استان به شبکه دولت

برای بدست آوردن وزن نسبی چهار بستر اصلی و نیز زیرمعیارهای شناسایی شده، پرسشنامه‌هایی بر اساس مقایسه‌های زوجی و روش AHP[1] فازی طراحی شد. این پرسشنامه‌ها میان کارکنان و کارشناسان فناوری اطلاعات سازمانهای دولتی توزیع گردید. جهت انجام تجزیه و تحلیل داده‌ها با رویکرد فازی بایستی اعداد بدست آمده از پرسشنامه‌ها به اعداد فازی مثلثی معادل خود تبدیل شوند. برای تجزیه و تحلیل این داده‌ها از روش AHP فازی و تکنیک تحلیل توسعه‌ای چانگ استفاده گردید.

جدول شماره ۲: نتایج بدست آمده از پیاده‌سازی الگوریتم AHP فازی

ردیف	معیارهای اصلی	وزن نسبی در حالت فازی
۱	زیرساخت و محتوی و کاربرد	0.314
۲	منابع انسانی	0.272
۳	سیاست ها و راهبردها	0.231
۴	نهادها	0.183

همان‌طور که در این جدول مشاهده می‌شود بستر زیرساخت و محتوی و کاربرد با وزن نسبی ۴ ۰,۳۱ بیشترین اهمیت را دارد. پس از بستر زیرساخت و محتوی و کاربرد، بسترهای منابع انسانی، سیاست و راهبرد و نهادها به ترتیب با وزن ۰,۲۷۲، ۰,۲۳۱ و ۰,۱۸۳در جایگاه‌های بعدی قرار دارند. نرخ ناسازگاری مقایسات در این بخش (Clg=0.09) و (Clm=0.09) می‌باشد و از آنجا که این مقدار کمتر از صفر است، سازگاری پرسشنامه‌ها در حد قابل قبولی قرار دارد.

[1] Analytic Hierarchy Process

شش زیرمعیار حوزه سیاست‌ها و راهبردها نسبت به هم مورد مقایسه دو به دو قرار گرفته‌اند تا وزن نسبی هر یک از آنها محاسبه گردد، زیرمعیار قوانین و آیین‌نامه‌های اجرایی با وزن نسبی ۰,۲۶ بیشترین وزن را به خود اختصاص داده است. معیارهای میزان حق دسترسی، برنامه‌ریزی مبتنی بر راهبردها و اهداف بلندمدت، شناسایی اولویت‌های توسعه فناوری اطلاعات، جهت‌گیری و سیاست‌گذاری مشخص در توزیع اعتبارات سازمانی، توجه ویژه به فناوری اطلاعات و ارتباطات در اسناد بالادستی توجه به موضوع امنیت و تهیه و تدوین قوانین در جایگاه‌های بعدی قرار دارند.

در حوزه منابع انسانی زیرمعیارهای تعهد مدیریت نسبت به پیاده‌سازی امنیت، برگزاری دوره‌های تحصیلی-آموزشی با وزن نسبی ۰,۱۷ بیشترین وزن را به خود اختصاص داده‌اند. معیارهای استفاده از نیروهای متخصص فناوری و فرهنگ پذیرش و باور حوزه فناوری اطلاعات و ارتباطات و آشنایی با دستاوردها و کاربردهای فناوری و مدیریت و طبقه‌بندی مناسب نیروی انسانی سازمان و توسعه فرهنگ به کارگیری امکانات رایانه‌ای در جایگاه‌های بعدی قرار دارند.

در حوزه زیرساخت، محتوی و کاربرد، زیرمعیار نظارت بر نرم‌افزارهای برون‌سپاری شده با وزن نسبی ۰,۲۴ بیشترین وزن را به خود اختصاص داده است. معیارهای جداسازی سیستم‌های حساس، به روز رسانی مرتب تجهیزات، نرم افزارها، وب سایت و سامانه‌ها، کنترل آسیب‌پذیری‌های فنی و تست نفوذ، تامین و تعمیر و نگهداری از سخت افزارها و تجهیزات کارا و مناسب و تامین امنیت شبکه در جایگاه‌های بعدی قرار دارند.

در حوزه نهادها، زیرمعیار استفاده از بخش خصوصی فعال بومی با وزن نسبی ۰,۳۵ بیشترین وزن را به خود اختصاص داده است. معیارهای هماهنگی مناسب میان دستگاه‌های مختلف دولتی مرتبط، دسترسی سازمان به شبکه دولت، به‌کارگیری از استانداردهای مطرح در حوزه فناوری اطلاعات و ارتباطات در جایگاه‌های بعدی قرار دارند.

نتیجه گیری

رتبه‌بندی معیارهای چهارگانه جهت ارتقا امنیت شبکه‌های اطلاعاتی الکترونیکی زندان-های استان سیستان و بلوچستان، حاکی از آن است که حوزه زیرساخت و محتوی و کاربرد از دیدگاه مدیران و خبرگان تصمیم‌گیرنده دارای بالاترین اهمیت است. این امر نشان می-

دهد، نگرش کلی مدیریتی حاکم بر این اداره کل تنها مبتنی بر ایجاد بسترهای فنی-مخابراتی است. به نظر می‌رسد وجود چنین نگرشی نویدبخش افزایش سطح بسترهای زیرساخت و محتوی و منابع انسانی باشد. با این وجود عامل زیرساخت و محتوی و کاربرد، تعیین‌کننده بوده و اولین معیار ارزیابی به شمار می‌رود. علاوه بر بستر زیرساخت و محتوی و کاربرد، بستر منابع انسانی نیز اهمیت بالایی دارد.

از دیدگاه خبرگان جامعه مورد مطالعه، دو بستر "سیاست‌ها و راهبردها" و "نهادها" نسبت به دو بستر "زیرساخت و محتوی و کاربرد" و "منابع انسانی" از اهمیت کمتری برخوردارند. این امر حاکی از آن است که عوامل مربوط به این حوزه‌ها اهمیت پایین‌تری در مقایسه با معیارهایی دارند که به طور مستقیم با بستر زیرساخت، محتوی و کاربرد و منابع انسانی در ارتباط هستند.

منابع فارسی

بحرانی، پیام و یزدی، مهران (۱۳۸۸). اهمیت و لزوم سیستم مدیریت امنیت اطلاعات در دولت الکترونیک. *دومین کنفرانس بین المللی نظام اداری الکترونیکی*، مرکز همایش های علمی طاپکو، تهران

حریری، نجلا و نظری، زهرا (۱۳۹۱). امنیت اطلاعات در کتابخانه‌های دیجیتالی ایران. *فصلنامه علمی-پژوهشی کتابداری و اطلاع رسانی*، شماره دوم، جلد ۱۵

حقیقی، محمد و سیحون، علیرضا (۱۳۸۸). ارائه مدل بلوغ الکترونیکی برای فرآیندهای ارائه خدمات در صنعت بیمه کشور وآزمون آن در شرکت بیمه پارسیان. *فصلنامه صنعت بیمه*، سال بیست وسوم، شماره ۳ و ۴، پاییز و زمستان ۱۳۸۸، صص ۱۱۱-۷۷

خالقی، محمود. راهنمای پیاده‌سازی سیستم مدیریت امنیت اطلاعات. تهران: دبیرخانه شورای عالی امنیت فضای تبادل اطلاعات کشور،۱۳۸۳

فقیهی, ابوالحسن, بامدادصوفی, جهانیار. (۱۳۷۵). کثرت گرایی روش تحقیق در پژوهش های سازمانی. *مطالعات مدیریت (بهبود و تحول)*، ۶(۲۱,۲۲)، ۵۴-۷۱.

قاسمی شبانکاره، کبرا; مختاری، وحید و امینی لاری، منصور (۱۳۸۶). امنیت و تجارت الکترونیکی. *چهارمین همایش ملی تجارت الکترونیک*. تهران.

کاشفی، امید و زمانی‌فر، آزاده(۱۳۹۱). *بلوغ دولت الکترونیک*. تهران: دبیرخانه شورای عالی اطلاع رسانی

References

Bohrani, P. and Yazdi, M. (2019). The Importance and Necessity of Information Security Management System in E-Government. *2nd International Conference on Electronic Administration System*, TAPCO Scientific Conference Center, Tehran. (In Persian)

Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report*. 11(1), pp. 26–31.

Faghihi, A., Bamdadsofi, J. (1999). " Triangulation in organizationl studies ". *Management Studies in Development and Evolution*, 6(21.22), 54-71. (In Persian)

Ghasemi Shabankareh, C.; Mokhtari, V. and Amini Lari, M. (2017). Security and E-Commerce. *4th National Conference on E-Commerce*. Tehran. (In Persian)

Haghighi, M. and Seyhoun, A. (2019). Presenting an Electronic Maturity Model for the Processes of Providing Services in the Iranian Insurance Industry and its Testing in Parsian Insurance Company. *Insurance Industry Quarterly*, 26(2 and 3), pp. 77- 111. (In Persian)

Hariri, N. and Nazari, Z. (2012). Information Security in Iranian Digital Libraries. *Journal of Library and Information Science*, 16(2), pp. 61-90. (In Persian)

HO, A, T. (2002). "Reinventing Local Governments and the Egovernment Initiative". Public Administration Review, *International Journal of Information Management*, 62(4), pp. 434-444.

Jouinia, M.; Ben, L.; Ben Arfa Rabai L. and Ben Aissa, A. (2014). " Classification of security threats in information systems". *Procedia Computer Science*, 32, pp. 489 – 496.

Kashefi, O. and Zamani Far, A. (2012). E-Government Maturity. Tehran: *Secretariat of the Supreme Information Council*. (In Persian)

Khaleghi, M. (2015). Implementation Guide for Information Security Management System. Tehran: *Secretariat of the Supreme Council of the Security of the Information Exchange Space of the State*. (In Persian)

Kritzinger E. and Smith E. (2008), " Information security management: An information security retrieval and awareness model for industry", *Computers & Security*, 27(5-6), pp. 224-231.

Mir, M.; Ghasemi M. and Dehghani M. (2019), Evaluation of Entrepreneurship Attitudes among Prisoners of Zahedan Central Prison, *National Conference on Economics, Development Management and Entrepreneurship with the Approach of Supporting Iranian Goods*, Zahedan. (In Persian)

Ronaghan, S. A. (2017). “Benchmarking E-government: A Global Perspective. Assessing the Progress of The UN Member States”. *United Nations Division for Public Economics and Public Administration*, New York.

Safianu, O. and Twum, F. (2016). "Information System Security Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection". *International Journal of Computer Applications*. 143(5), pp. 8-14.

Susanto, H., Almunawar, M.N., & Tuan, Y.C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences IJECS-IJENS.* 11(5).