Passive Defence
Vol. 16, No. 4, Winter 2026, Serial No. 64
ISSN: 2980-8030 , E-ISSN: 2008-6849

Analyzing Cyber Threats and Vulnerabilities in Iran's Gas Industrial Control Systems and Presenting a Counter Measure System Model

Abdolrahman Keshvari[1]*, Amin Monazami Motlagh[2]
[1]Correspondence: Assistant Professor, Imam Hossein Comprehensive University, Tehran, Iran. Email Address: negahdasht@yahoo.com
[2]PhD Student, Strategic Management, Faculty of Defense, National Defense and Strategic Research University and Institute, Tehran, Iran. Email Address: aminmonazamimotlagh2@gmail.com

ARTICLE INFO

Article history:
Article Type: Research paper
Received: 16 March 2025
Received in revised form: 30 April 2025
Accepted: 2 June 2025
Available online: 20 January 2026

Keywords:
Cybersecurity
Industrial Control Systems
Gas Industry
Defense in Depth
System Model
Critical Infrastructure

ABSTRACT

Industrial Control Systems (ICS) in the gas industry, as a part of the critical infrastructure of countries, are facing increasing cyber threats. These threats have created serious challenges due to the strategic importance of the gas industry in the national economy and security, as well as the very key role of industrial control systems in the gas industry. This research has been conducted with the aim of identifying and analyzing cyber vulnerabilities in the industrial control systems of the gas industry and presenting a systemic model to counter these threats. The research method is mixed (quantitative-qualitative), and the necessary data has been collected through field studies, in-depth interviews with experts, specialized questionnaires, and document analysis. The research results show that the main vulnerabilities include a lack of integration in the security architecture, the use of outdated systems, weakness in access management, and deficiencies in employee training. The proposed systemic model includes five protective layers (developed defense-in-depth) that, with an emphasis on a preventive and rapid response approach, can be implemented in the specific conditions of gas infrastructures.

Cite this article: A. Keshvari and A. Monazami Motlagh, "Analyzing Cyber Threats and Vulnerabilities in Iran's Gas Industrial Control Systems and Presenting a Counter Measure System Model," Journal of Passive Defence, vol. 16, no. 4, pp. 35-55, 2026.
DOI: doi.org/10.47176/PD.2026.1527

© Author(s) retain the copyright and full publishing rights

Publisher: Imam Hossein University.

Introduction

Industrial Control Systems (ICS) are foundational to the operation of critical national infrastructures. In Iran, the gas industry is of high strategic importance to the national economy and security, and it relies heavily on ICS and SCADA systems for process management and monitoring. However, the increasing integration of these systems with digital technologies has exposed them to a growing wave of sophisticated cyber threats. High-profile global attacks such as Stuxnet, Triton, and the Colonial Pipeline incident have demonstrated that these operational technology (OT) environments are no longer immune to cyberattacks, which can lead to severe economic, social, and security consequences.

While numerous studies have addressed ICS security, a significant research gap exists. Most existing literature focuses on the context of developed nations and often concentrates narrowly on technical vulnerabilities. These studies frequently overlook the unique challenges faced by industries in countries like Iran, such as international sanctions that impede technology updates, the prevalence of legacy systems, and specific organizational and human factors. Consequently, there is a pressing need for a comprehensive and systemic model tailored to this specific context. This study aims to identify, analyze, and prioritize the primary cyber threats and vulnerabilities within the control systems of Iran's gas industry and to propose a holistic, multi-layered systemic model for mitigating them.

Methodology

This research employed a descriptive-analytical design with a mixed-method (qualitative-quantitative) approach, conducted between March 2024 and March 2025. The data collection process was multi-faceted to ensure a comprehensive understanding of the subject matter:

1. Literature and Document Review: An extensive review of academic papers, industry reports, and technical documents related to ICS cybersecurity in the oil and gas sector was performed.
2. Expert Interviews: Semi-structured, in-depth interviews were conducted with a purposefully selected group of 22 senior managers, cybersecurity specialists, and IT/OT experts from the Iranian gas industry.
3. Specialized Questionnaire: A custom questionnaire was developed and administered to a sample of 197 industry professionals, selected through stratified random sampling. The questionnaire contained 52 questions covering threat assessment, vulnerability evaluation, and potential countermeasures.
4. Technical Assessments: Vulnerability assessments were performed using standard frameworks like NIST SP 800-82 and ICS-CERT guidelines, alongside simulated cyberattack exercises in a laboratory environment to validate findings.

Data analysis was conducted using a combination of tools and techniques. Qualitative data from interviews were analyzed using content analysis in MAXQDA software. Quantitative data from the questionnaires were analyzed statistically using SPSS and AMOS, with the Friedman test applied for ranking threats. The final systemic model was designed using Interpretive Structural Modeling (ISM) and Structural Equation Modeling (SEM) and subsequently validated through a Delphi method involving 18 independent experts.

Results and Discussion

The research yielded significant findings in three main areas: threat identification, vulnerability analysis, and the development of a countermeasure model.

Cyber Threats:

The analysis identified and ranked six primary categories of cyber threats. "Targeted state-sponsored attacks" (e.g., Advanced Persistent Threats, supply chain attacks) were ranked as the most severe threat, with a mean severity score of 4.79 out of 5. This was followed by "Network-based attacks" (e.g., DDoS, sniffing) at 4.36 and "Insider threats" (malicious or unintentional) at 4.15. Notably, the study highlighted the rise of "AI-based attacks" as an emerging and increasingly sophisticated threat category.

Cyber Vulnerabilities:

The most critical vulnerability identified was the "Lack of proper segmentation between IT and OT networks," which was reported in 22.7% of cases and received the highest risk score (4.87 out of 5). Other significant vulnerabilities included the use of insecure or unencrypted communication protocols, the prevalence of unpatched legacy systems, and weak access control management. Furthermore, the research noted a concerning 52% increase in vulnerabilities associated with the Industrial Internet of Things (IIoT), indicating a rapidly expanding attack surface.

The Proposed Systemic Model:

The primary outcome of this study is a comprehensive, five-layered systemic model titled "Enhanced Defense in Depth." This model is designed to be proactive and resilient, addressing the full spectrum of security challenges. The five layers are:

1. Governance and Strategy: Establishes the foundational security policies, standards, and risk management framework.
2. Technical and Infrastructure: Focuses on technical controls like network segmentation, encryption, and access control.
3. Operational and Process: Manages security through processes like incident response, change management, and continuous monitoring.
4. Human and Cultural: Addresses the human element through targeted training, awareness campaigns, and fostering a security-centric culture.
5. Collaboration and Coordination: Promotes the sharing of threat intelligence and coordinated response with national CERTs and industry partners.

This model enhances the traditional defense-in-depth approach by formally integrating the strategic governance and external collaboration dimensions. The findings provide a clear roadmap of priority actions, with "Implementing a secure architecture with IT/OT segmentation" identified as the most effective technical action (effectiveness score: 4.94 out of 5).

Conclusion

This research provides a detailed and contextualized analysis of the cyber risk landscape facing Iran's gas industry. Its main contribution is the development and validation of the "Enhanced Defense in Depth" model—a novel, practical, and multi-layered framework for systematically mitigating cyber threats. The model is specifically designed to be implementable within the unique operational realities and constraints of the industry.

Implications and Recommendations:

The study's findings offer actionable insights for industry leaders and policymakers. It is recommended that decision-makers:

- Adopt and strategically implement the five-layered model as the core of their cybersecurity program.
- Prioritize immediate investment in critical actions, particularly IT/OT network segmentation, specialized staff training, and developing a formal incident response plan.
- Foster a culture of security awareness and promote active collaboration with national security bodies and industry peers.

Limitations and Future Work:

The study was constrained by security-related access limitations to live systems and the confidentiality of certain data. For future research, a longitudinal study (3-5 years) is recommended to measure the long-term effectiveness of the proposed model in a real-world environment. Further investigation into the impact of AI on both threats and defenses, as well as a cost-benefit analysis of the proposed security controls, would also provide significant value.

پدافند غیرعامل

سال پانزدهم، شماره ۴، زمستان ۱۴۰۴، (پیاپی ۶۴): صص ۵۵-۳۵

شاپای چاپی: ۶۹۴۹-۲۰۰۸ | شاپای الکترونیکی: ۸۰۳۰-۲۹۸۰

تحلیل تهدیدات و آسیب پذیری‌های سایبری در سامانه‌های کنترل صنعتی صنعت گاز و ارائه مدل سیستمی مقابله

عبدالرحمن کشوری[1*]، امین منظمی مطلق[2]

[1] استادیار دانشگاه جامع امام حسین(ع)، تهران، ایران(نویسنده مسئول). رایانامه: negahdasht@yahoo.com

[2] دانشجوی دکترای دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران. رایانامه: aminmonazamimotlagh2@gmail.com

چکیده

سامانه‌های کنترل صنعتی (ICS) صنعت گاز، به‌عنوان بخشی از زیرساخت‌های حیاتی کشورها، با تهدیدات سایبری فزاینده‌ای مواجه هستند. این تهدیدات با توجه به اهمیت راهبردی صنعت گاز در اقتصاد و امنیت ملی، و همچنین با توجه به نقش بسیار کلیدی سامانه‌های کنترل صنعتی در صنعت گاز، چالش‌های جدی را ایجاد کرده‌اند. این پژوهش با هدف شناسایی و تحلیل آسیب‌پذیری‌های سایبری در سامانه‌های کنترل صنعتی صنعت گاز و ارائه یک مدل سیستمی برای مقابله با این تهدیدات انجام شده است. روش تحقیق ترکیبی (کمی-کیفی) بوده و از طریق مطالعات میدانی، مصاحبه‌های عمیق با متخصصان، پرسشنامه‌های تخصصی و تحلیل اسناد، داده‌های لازم جمع‌آوری شده است. نتایج پژوهش نشان می‌دهد که آسیب‌پذیری‌های اصلی شامل فقدان یکپارچگی در معماری امنیتی، استفاده از سامانه‌های قدیمی، ضعف در مدیریت دسترسی، و نقص در آموزش کارکنان است. مدل سیستمی پیشنهادی شامل پنج لایه حفاظتی (دفاع عمقی توسعه‌یافته) است که با تأکید بر رویکرد پیشگیرانه و واکنش سریع، قابلیت پیاده‌سازی در شرایط خاص زیرساخت‌های گازی را دارد.

مشخصات مقاله

تاریخچه مقاله:

نوع مقاله: علمی پژوهشی

دریافت: ۱۴۰۳/۱۲/۲۶

بازنگری: ۱۴۰۴/۰۲/۱۰

پذیرش: ۱۴۰۴/۰۳/۱۲

ارائه آنلاین: ۱۴۰۴/۱۰/۳۰

کلیدواژه‌ها:

امنیت سایبری

سامانه‌های کنترل صنعتی

صنعت گاز

دفاع در عمق

مدل سیستمی

زیرساخت حیاتی

استناد: کشوری، عبدالرحمن، منظمی مطلق، امین، " تحلیل تهدیدات و آسیب‌پذیری‌های سایبری در سامانه‌های کنترل صنعتی صنعت گاز و ارائه مدل سیستمی مقابله"، نشریه پدافند غیرعامل، دوره ۱۶، شماره۴، صفحات ۵۵-۳۵، ۱۴۰۴. DOI: https://doi.org/10.47176/PD.2026.1527

© نویسنده(گان) حق نشر و حقوق کامل انتشار را برای خود محفوظ می‌دارند.

ناشر: دانشگاه جام امام حسین(ع).

۱- مقدمه

امروزه با گسترش استفاده از فناوری‌های دیجیتال و اتوماسیون در صنایع مختلف، سامانه‌های کنترل صنعتی (ICS) و سامانه‌های اسکادا (SCADA) نقش حیاتی در مدیریت و نظارت بر فرآیندهای صنعتی ایفا می‌کنند [۱]. صنعت گاز، به عنوان یکی از مهم‌ترین زیرساخت‌های حیاتی کشورها، وابستگی قابل توجهی به این سامانه‌ها دارد که هرگونه اختلال در عملکرد آن‌ها می‌تواند پیامدهای جدی اقتصادی، اجتماعی و حتی امنیتی به همراه داشته باشد. در سال‌های اخیر، تهدیدات سایبری علیه زیرساخت‌های حیاتی در سراسر جهان افزایش چشمگیری داشته [۲] و حملات سایبری پیچیده‌ای مانند استاکس‌نت، تریتون، هاوکس‌بی، کرش اوردراید و حمله به خط لوله کولونیال (Colonial Pipeline) نشان داده‌اند که سامانه‌های کنترل صنعتی نیز از این تهدیدات مصون نیستند [۳].

آسیب‌پذیری‌های سایبری در صنعت گاز را می‌توان در چندین دسته کلی تقسیم‌بندی کرد: آسیب‌پذیری‌های فنی و نرم‌افزاری، آسیب‌پذیری‌های فیزیکی و عملیاتی، آسیب‌پذیری‌های ارتباطی و شبکه‌ای، آسیب‌پذیری‌های مدیریتی و سیاست‌گذاری، و آسیب‌پذیری‌های مبتنی بر تهدیدات جدید [۴]. این آسیب‌پذیری‌ها در کنار تهدیدات فزاینده مانند حملات سایبری پیشرفته و هدفمند، نفوذ و خرابکاری از طریق بدافزارها، جاسوسی سایبری، و تهدیدات داخلی، خطرات جدی برای صنعت گاز محسوب می‌شوند [۵].

مروری بر مطالعات پیشین نشان می‌دهد که پژوهش‌های متعددی در زمینه امنیت سایبری سامانه‌های کنترل صنعتی انجام شده است. ژانگ و همکاران [۶] در مطالعه خود با عنوان "مکانیسم‌های دفاع لایه‌ای برای سیستم‌های کنترل صنعتی" به بررسی رویکردهای مختلف امنیتی پرداخته و یک معماری چندلایه‌ای برای محافظت از این سیستم‌ها پیشنهاد داده‌اند. همچنین، ویلسون و همکاران [۷] در پژوهشی تحت عنوان "اهمیت نظارت و ثبت رویدادها در سیستم‌های کنترل صنعتی" به اهمیت سیستم‌های مانیتورینگ و لاگینگ در تشخیص به‌موقع حملات سایبری پرداخته‌اند.

اندرسون و لورت [۸] در مطالعه خود با عنوان "درس‌های آموخته شده از حملات سایبری به شبکه‌های برق: پیامدهایی برای امنیت زیرساخت‌های گاز" به بررسی حملات سایبری اخیر به شبکه‌های برق پرداخته و درس‌هایی برای محافظت از زیرساخت‌های گاز استخراج کرده‌اند. این پژوهش که در مجله معتبر Energy Policy منتشر شده، نشان می‌دهد که بسیاری از آسیب‌پذیری‌های شناسایی شده در شبکه‌های برق، در سیستم‌های گاز نیز وجود دارند [۸].

در سال ۲۰۲۳، کارنوسکوس [۹] در پژوهشی با عنوان "امنیت سیستم‌های سایبرفیزیکی برای شبکه هوشمند: یک تحلیل جامع" به بررسی چالش‌های امنیتی در سیستم‌های سایبرفیزیکی پرداخته و یک چارچوب جامع برای ارزیابی و مدیریت خطرات امنیتی در این سیستم‌ها پیشنهاد داده است [۹]. این مطالعه که در مجله Smart Grid and Renewable Energyمنتشر شده، اهمیت رویکرد سیستمی در مدیریت امنیت سایبری را برجسته می‌کند.

علیزاده سودمند و همکاران [۱۰] در مطالعه خود به ارائه مدل مفهومی سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور پرداخته‌اند. آنها در پژوهش دیگری [۱۱] به تحلیل ساختارمند شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان توجه کرده‌اند. همچنین، میریوسفی و غفارپور [۱۲] به بررسی راهبردهای نوین حفاظت از زیرساخت‌های حیاتی پرداخته‌اند. افشار و همکاران [۱۳] نیز مدل مفهومی جامعی برای آسیب‌پذیری‌های سیستم کنترل واحدهای صنعتی و زیرساخت‌های حیاتی ارائه کرده‌اند. اختری و همکاران [۱۴] به مقایسه تطبیقی مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات و احصای شاخص‌های امنیت سایبری پرداخته‌اند.

با وجود مطالعات انجام شده، محدودیت‌ها و خلاهای پژوهشی قابل توجهی در این حوزه وجود دارد. اول، اکثر مطالعات انجام شده در سطح بین‌المللی، تمرکز خود را بر زیرساخت‌های کشورهای توسعه‌یافته قرار داده‌اند و شرایط خاص کشورهای توسعه نیافته را در نظر نگرفته‌اند [۱۰]، [۱۵]. دوم، بسیاری از این مطالعات صرفاً به جنبه‌های فنی امنیت سایبری پرداخته و ابعاد انسانی، سازمانی و مدیریتی را که معمولاً در محیط‌های صنعتی اهمیت بالایی دارند، نادیده گرفته‌اند [۱۱]، [۱۶]. سوم، در اکثر این مطالعات، کمتر به ارائه یک مدل سیستمی جامع که تمامی ابعاد امنیت سایبری را پوشش دهد، پرداخته شده است [۱۷].

صنعت گاز با چالش‌های منحصر به فردی مواجه است که نیازمند توجه ویژه است. از یک سو، تحریم‌های بین‌المللی مانع دسترسی به فناوری‌های روز و به‌روزرسانی سیستم‌های موجود در بسیاری از کشورها شده است [۱۲]؛ از سوی دیگر، وجود سیستم‌های قدیمی (Legacy Systems) که امکان ارتقای امنیتی آن‌ها محدود است، آسیب‌پذیری‌های قابل توجهی را ایجاد کرده است [۱۳]. همچنین، ترکیب ناهمگون تجهیزات و نرم‌افزارهای مختلف که در طول سال‌ها به سیستم‌های موجود اضافه شده‌اند، چالش‌های امنیتی پیچیده‌ای را به وجود آورده است [۱۸].

با توجه به شکاف‌های پژوهشی موجود و اهمیت روزافزون امنیت سایبری سامانه‌های کنترل صنعتی گاز، این پژوهش با هدف اصلی "تحلیل تهدیدات و آسیب‌پذیری‌های سایبری در سامانه‌های کنترل صنعتی گاز و ارائه مدل سیستمی مقابله" انجام شده است.

۲- روش تحقیق

این پژوهش یک مطالعه توصیفی-تحلیلی با رویکرد ترکیبی (کمی - کیفی) است که در بازه زمانی فروردین ۱۴۰۳ تا اسفند ۱۴۰۳ انجام شده است. جامعه آماری پژوهش شامل کارشناسان، مدیران و متخصصان فناوری اطلاعات و امنیت سایبری صنعت گاز بوده است.

۲-۱- روش نمونه‌گیری و حجم نمونه

نمونه‌گیری در بخش کیفی به صورت هدفمند و با استفاده از روش گلوله برفی انجام شد. در این بخش، ۲۲ نفر از متخصصان امنیت سایبری و مدیران ارشد حوزه فناوری اطلاعات برای مصاحبه انتخاب شدند. در بخش کمی، نمونه‌گیری به صورت تصادفی طبقه‌ای انجام شد و با استفاده از فرمول کوکران، حجم نمونه ۱۹۲ نفر تعیین گردید. برای اطمینان از کفایت حجم نمونه، با در نظر گرفتن احتمال ۱۰ درصدی عدم پاسخگویی، ۲۱۰ پرسشنامه توزیع شد که در نهایت ۱۹۷ پرسشنامه تکمیل و بازگردانده شد (نرخ پاسخگویی ۸/۹۳ درصد).

کارهای مرتبط:

- ژانگ و همکاران [۶]: "مکانیسم‌های دفاع لایه‌ای برای سیستم‌های کنترل صنعتی" - معماری چندلایه‌ای برای محافظت از سیستم‌های کنترل صنعتی پیشنهاد دادند.
- ویلسون و همکاران [۷]: "اهمیت نظارت و ثبت رویدادها در سیستم‌های کنترل صنعتی" - بر اهمیت سیستم‌های مانیتورینگ و لاگینگ تأکید کردند.
- اندرسون و لورت[۸]: "درس‌های آموخته شده از حملات سایبری به شبکه‌های برق" - به استخراج درس‌هایی برای محافظت از زیرساخت‌های گاز پرداختند.
- کارنوسکوس[۹]: "امنیت سیستم‌های سایبرفیزیکی برای شبکه هوشمند" - چارچوبی برای ارزیابی و مدیریت ریسک‌های امنیتی پیشنهاد داد.
- آشوک و همکاران[۱۹]: "چارچوب امنیت سایبر-فیزیکی برای سیستم‌های کنترل صنعتی" - جداسازی شبکه‌ها را از مهم‌ترین اقدامات امنیتی معرفی کردند.
- هرناندز و همکاران[۲۰]: مطالعه درباره چالش‌های امنیت سایبری در زیرساخت‌های حیاتی - بر اهمیت آموزش و توانمندسازی کارکنان تأکید کردند.
- استوفر و همکاران[۱]:"راهنمای امنیت سیستم‌های کنترل صنعتی" - استفاده از پروتکل‌های ناامن را یکی از آسیب‌پذیری‌های اصلی معرفی کردند.

۲-۲- سیر تحول موضوع

۱. مرحله اولیه امنیت سایبری صنعتی: در ابتدا ، سامانه‌های کنترل صنعتی بدون در نظر گرفتن امنیت سایبری طراحی می‌شدند و فرض بر این بود که جدا بودن فیزیکی این سیستم‌ها برای حفاظت کافی است.

۲. شناخت آسیب‌پذیری‌ها (اوایل دهه ۲۰۰۰): با افزایش اتصال سیستم‌های کنترل صنعتی به شبکه‌هایIT، آسیب‌پذیری‌های امنیتی مشخص شدند.

۳. بروز حملات شاخص (۲۰۱۰ به بعد):

- حمله استاکس‌نت (۲۰۱۰) به تأسیسات هسته‌ای ایران
- حمله به شبکه برق اوکراین (۲۰۱۵)
- حمله به خط لوله کولونیال در آمریکا (۲۰۲۱)
- ظهور بدافزارهای پیشرفته مانند تریتون و هاوکس‌بی

۴. توسعه چارچوب‌های امنیتی (۲۰۱۵ به بعد):

- ارائه استانداردهایی مانندNIST SP 800-82
- توسعه استانداردهای IEC 62443 برای امنیت سایبری صنعتی
- پیشنهاد رویکرد دفاع در عمق(Defense in Depth)

۵. وضعیت کنونی (۲۰۲۵/۱۴۰۳) :

- افزایش تهدیدات مبتنی بر هوش مصنوعی (٪۴۷ افزایش)

○ افزایش حملات زنجیره تأمین (۳۶٪ افزایش)

○ پیچیده‌تر و هدفمندتر شدن حملات

○ افزایش چشمگیر آسیب‌پذیری‌های مرتبط با تجهیزات اینترنت اشیاء صنعتی (۵۲٪ افزایش)

۲-۳- سؤال مورد تحقیق

سؤال اصلی این پژوهش عبارت است از :"چه تهدیدات و آسیب‌پذیری‌های سایبری در سامانه‌های کنترل صنعتی گاز وجود دارد و چه مدل سیستمی می‌تواند برای مقابله با این تهدیدات ارائه شود؟"

سؤالات فرعی:

۱. مهم‌ترین تهدیدات سایبری علیه سامانه‌های کنترل صنعتی گاز کدامند؟

۲. اصلی‌ترین آسیب‌پذیری‌های سایبری در سامانه‌های کنترل صنعتی گاز چیست؟

۳. چه مدل سیستمی با توجه به شرایط خاص صنعت گاز می‌تواند برای مقابله با تهدیدات سایبری ارائه شود؟

۴. اقدامات اولویت‌دار در هر لایه از مدل سیستمی پیشنهادی کدامند؟

۲-۴- راهکار پاسخ به سؤالات تحقیق

پژوهشگر برای پاسخ به این سؤالات از روش تحقیق ترکیبی (کمی-کیفی) استفاده کرده است:

۲-۴-۱- جمع‌آوری داده‌ها

داده‌های پژوهش از طریق روش‌های زیر جمع‌آوری شده‌اند:

۱. مطالعات کتابخانه‌ای: بررسی مقالات، کتب، گزارش‌ها و اسناد موجود در حوزه امنیت سایبری سامانه‌های کنترل صنعتی با تمرکز بر صنعت نفت و گاز.

۲. مصاحبه‌های نیمه‌ساختاریافته: انجام مصاحبه با ۲۲ نفر از متخصصان و مدیران ارشد حوزه امنیت سایبری و فناوری اطلاعات.

۳. پرسشنامه محقق‌ساخته: پرسشنامه‌ای شامل ۵۲ سؤال در سه بخش "ارزیابی تهدیدات" (۱۸ سؤال)، "ارزیابی آسیب‌پذیری‌ها" (۲۰ سؤال) و "راهکارهای مقابله" (۱۴ سؤال).

۴. ارزیابی آسیب‌پذیری: با استفاده از چک‌لیست‌های استاندارد ICS-CERT [۱۴] و NIST SP 800-82 Rev. 3 و همچنین ابزارهای ارزیابی آسیب‌پذیری نظیر Nessus Industrial Security و CyberX.

۵. رزمایش شبیه سازی حمله سایبری: دو رزمایش شبیه‌سازی حمله سایبری در محیط آزمایشگاهی.

۲-۴-۲- تحلیل داده‌ها

○ تحلیل محتوای کیفی با نرم‌افزارMAXQDA

○ تحلیل آماری داده‌های کمی با SPSS وAMOS

○ طراحی مدل با استفاده از روش‌های مدل‌سازی ساختاری-تفسیری (ISM) و مدل‌سازی معادلات ساختاری(SEM) [15]

○ اعتبارسنجی مدل با استفاده از آزمون دلفی و مشارکت ۱۸ نفر از خبرگان

۲-۵- روش‌های تحلیل آماری استفاده شده

آزمون فریدمن برای رتبه‌بندی تهدیدات:

$$\chi^2 = (12/nk(k+1)) \times \Sigma(Ri^2) - 3n(k+1)$$

که در آن:

- n = تعداد پاسخ‌دهندگان (۱۹۷)
- k = تعداد تهدیدات (۶)
- Ri = مجموع رتبه‌های تهدید i-ام

ضریب همبستگی پیرسون برای آسیب‌پذیری‌ها:

$$r = \Sigma(xi - \bar{x})(yi - \bar{y}) / \sqrt{[\Sigma(xi - \bar{x})^2 \times \Sigma(yi - \bar{y})^2]}$$

نتیجه: r = ۰/۷۸ بین "ضعف در مدیریت دسترسی" و "فقدان نظارت"

ضریب هماهنگی کندال برای توافق خبرگان:

$$W = 12S / [m^2(n^3-n)]$$

که در آن:

- S = مجموع مربعات انحرافات رتبه‌ها
- m = تعداد خبرگان (۱۸)
- n = تعداد گزینه‌ها

نتیجه: W = ۰/۸۷ (توافق بالا)

۲-۶- مدل پیشنهادی

- ارائه مدل سیستمی ۵ لایه‌ای مبتنی بر رویکرد دفاع عمقی (Defense in Depth)
- لایه‌های مدل: حاکمیتی و راهبردی، فنی و زیرساختی، عملیاتی و فرایندی، انسانی و فرهنگی، همکاری و هماهنگی
- تعیین اقدامات اولویت‌دار در هر لایه با سنجش میانگین امتیاز اثربخشی
- ارزیابی مدل و کسب ضریب توافق بالا (ضریب هماهنگی کندال = ۰/۸۷)

این راهکار با توجه به شرایط خاص صنعت گاز و محدودیت‌هایی مانند تحریم‌های بین‌المللی، سیستم‌های قدیمی و ترکیب ناهمگون تجهیزات طراحی شده است تا قابلیت پیاده‌سازی عملی داشته باشد.

روش پیشنهادی این پژوهش بر اساس ترکیب رویکرد دفاع در عمق کلاسیک با ابعاد جدید طراحی شده است. این روش شامل مراحل زیر است:

۲-۷- فرمول محاسبه شاخص امنیت سایبری کلی (Overall Cybersecurity Index - OCI):

$$OCI = \Sigma(i=1 \text{ to } 5)\ Wi \times Li$$

که در آن:

- OCI: شاخص امنیت سایبری کلی (۰ تا ۵)
- Wi: وزن لایه i-ام
- Li: امتیاز لایه i ام
- i: شماره لایه (۱ تا ۵)

وزن‌های تعیین شده برای هر لایه:

- W1(حاکمیتی و راهبردی): ۰/۲۵
- W2(فنی و زیرساختی): ۰/۳۰
- W3(عملیاتی و فرایندی): ۰/۲۰
- W4(انسانی و فرهنگی): ۰/۱۵
- W5(همکاری و هماهنگی): ۰/۱۰

۲-۸- فرمول محاسبه ریسک سایبری (Cyber Risk - CR)

$$CR = (T \times V \times I) / C$$

که در آن:

- CR: ریسک سایبری
- T: میانگین شدت تهدیدات (Threats)
- V: میانگین سطح آسیب‌پذیری (Vulnerabilities)
- I: میانگین تأثیر بالقوه (Impact)
- C: میانگین سطح کنترل‌های امنیتی (Controls):

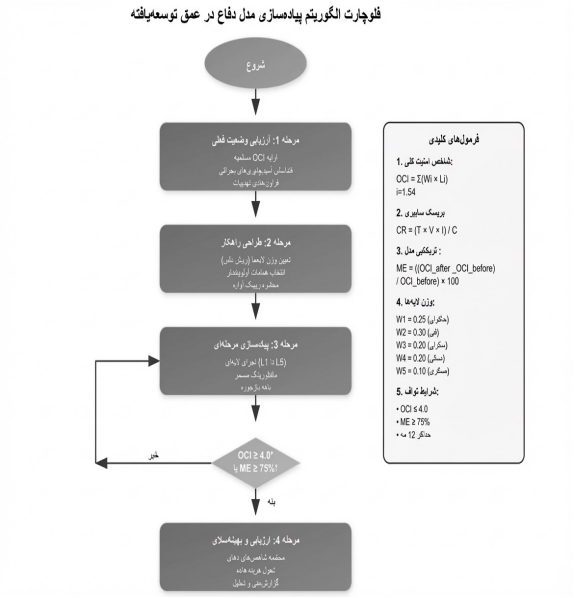
۲-۹- فرمول محاسبه اثربخشی مدل (Model Effectiveness - ME)

$$ME = ((OCI\_after - OCI\_before) / OCI\_before) \times 100$$

که در آن:

- ME: درصد بهبود اثربخشی
- OCI_after: شاخص امنیت پس از پیاده‌سازی
- OCI_before: شاخص امنیت قبل از پیاده‌سازی

۲-۱۰- فلوچارت الگوریتم پیاده سازی مدل دفاع در عمق توسعه یافته



۲-۱۱- تشریح معماری و لایه‌های سامانه‌های کنترل صنعتی

سامانه‌های کنترل صنعتی (ICS) دارای معماری چندلایه‌ای هستند که هر لایه وظایف خاصی را برعهده دارد. در صنعت گاز، این معماری به طور کلی شامل لایه‌های زیر است:

۱. لایه سطح میدانی :(Field Level) شامل سنسورها، محرک‌ها، شیرها و سایر تجهیزات فیزیکی که مستقیماً با فرآیند صنعتی در ارتباط هستند.

۲. لایه کنترل(Control Level) : شامل پی‌ال‌سی‌ها(PLC) ، رله‌های قابل برنامه‌ریزی (RTU) و سیستم‌های کنترل توزیع‌شده (DCS)که وظیفه پردازش داده‌های دریافتی از سنسورها و ارسال فرمان‌های کنترلی را برعهده دارند.

۳. لایه نظارت(Supervisory Level) : شامل سیستم‌های اسکادا (SCADA)و ایستگاه‌های کاری اپراتورها که وظیفه نظارت، مانیتورینگ و کنترل کل فرآیند را برعهده دارند.

۴. لایه مدیریت تولید (Production Management Level):شامل سیستم‌های مدیریت تولید، سیستم‌های اطلاعات تولید (MIS) و سیستم‌های برنامه‌ریزی منابع سازمانی (ERP) که وظیفه مدیریت کلان فرآیندهای تولید را برعهده دارند.

۵. لایه شبکه شرکتی (Enterprise Network Level):شامل شبکه‌های اداری، سیستم‌های مدیریت مشتری و سایر سیستم‌های مدیریتی سازمان.

هر یک از این لایه‌ها با چالش‌های امنیتی خاصی مواجه هستند:

- لایه میدانی :آسیب‌پذیری‌های فیزیکی، استفاده از پروتکل‌های غیرامن، عدم رمزنگاری در ارتباطات
- لایه کنترل :ضعف در احراز هویت، آسیب‌پذیری‌های سیستم‌عامل‌های قدیمی، پیکربندی نامناسب
- لایه نظارت :ضعف در مدیریت دسترسی، فقدان لاگینگ و نظارت کافی، آسیب‌پذیری‌های نرم‌افزاری
- لایه مدیریت تولید :مشکلات یکپارچگی داده‌ها، نقص در مدیریت وصله‌های امنیتی، ضعف در سیاست‌های امنیتی
- لایه شبکه شرکتی :حملات مهندسی اجتماعی، بدافزارها، حملات فیشینگ، ضعف در آگاهی‌سازی کارکنان

مدل سیستمی پیشنهادی در این پژوهش به گونه‌ای طراحی شده است که آسیب‌پذیری‌های خاص هر لایه را پوشش دهد و راهکارهای متناسب با هر لایه ارائه کند. علاوه بر این، تعاملات بین لایه‌ای و نقاط اتصال بین لایه‌ها که معمولاً آسیب‌پذیرترین نقاط هستند، نیز مورد توجه ویژه قرار گرفته‌اند.

۲-۱۲- تشریح رویکرد دفاع در عمق توسعه‌یافته

رویکرد دفاع در عمق (Defense in Depth) یکی از اصول بنیادین امنیت سایبری است که بر اساس ایجاد لایه‌های متعدد حفاظتی عمل می‌کند. ایده اصلی این رویکرد این است که در صورت نفوذ مهاجم از یک لایه امنیتی، لایه‌های دیگر همچنان از سیستم محافظت می‌کنند. در روش کلاسیک دفاع در عمق، معمولاً سه لایه اصلی فیزیکی، فنی و اداری وجود دارد [۲۱].

مدل پیشنهادی ما که "دفاع در عمق توسعه‌یافته" نام دارد، علاوه بر پوشش لایه‌های سنتی، دو لایه مهم دیگر را نیز اضافه کرده است:

۱. لایه حاکمیتی و راهبردی: این لایه بر خلاف مدل‌های سنتی که عمدتاً بر جنبه‌های فنی و عملیاتی تمرکز دارند، به موضوعات کلان و راهبردی می‌پردازد. این لایه شامل تدوین سیاست‌ها، طراحی معماری امنیتی کلان، مدیریت ریسک سازمانی و تخصیص منابع است.

۲. لایه همکاری و هماهنگی :این لایه به عنصر بسیار مهم همکاری درون‌سازمانی و برون‌سازمانی، اشتراک‌گذاری اطلاعات تهدیدات و هماهنگی با نهادهای ملی امنیت سایبری می‌پردازد که در مدل‌های سنتی کمتر به آن توجه شده است.

مزایای مدل دفاع در عمق توسعه‌یافته نسبت به مدل‌های سنتی عبارتند از:

۱. جامعیت بیشتر: پوشش کلیه ابعاد امنیتی از سطح استراتژیک تا عملیاتی

۲. انعطاف‌پذیری: قابلیت تطبیق با شرایط خاص صنعت گاز و محدودیت‌های موجود

۳. رویکرد پیشگیرانه: تأکید بر پیشگیری به جای صرفاً واکنش به حملات

۴. یکپارچگی: ایجاد ارتباط منسجم بین لایه‌های مختلف امنیتی

۵. همکاری محوری: تقویت همکاری‌های درون و برون سازمانی در مقابله با تهدیدات

۲-۱۳- مقایسه روش پیشنهادی با سایر روش‌ها

جدول زیر مقایسه‌ای بین مدل پیشنهادی "دفاع در عمق توسعه‌یافته" و سایر روش‌های مطرح در حوزه امنیت سایبری

سیستم‌های کنترل صنعتی ارائه می‌دهد:

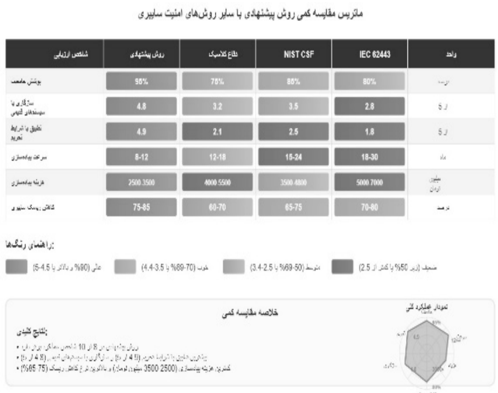
جدول (۱): مقایسه روش پیشنهادی با سایر روش‌های امنیت سایبری سامانه‌های کنترل صنعتی

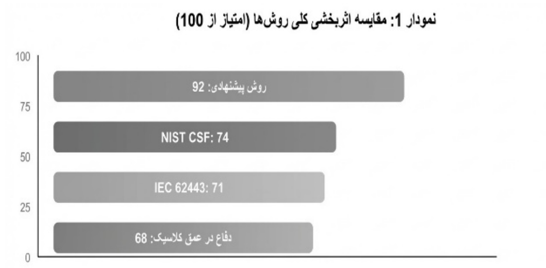
شاخص ارزیابی	دفاع در عمق توسعه‌یافته (پیشنهادی)	دفاع در عمق کلاسیک	چارچوب NIST CSF	استاندارد IEC ۶۲۴۴۳	معیار مقایسه
پوشش جامعیت (٪)	۹۵	۷۵	۸۵	۸۰	درصد پوشش کلیه ابعاد امنیتی
سازگاری با سیستم‌های قدیمی (امتیاز از ۵)	۴/۸	۳/۲	۳/۵	۲/۸	میزان سازگاری با Legacy Systems
قابلیت تطبیق با شرایط تحریم (امتیاز از ۵)	۴/۹	۲/۱	۲/۵	۱/۸	انطباق با محدودیت‌های خارجی
سرعت پیاده‌سازی (ماه)	۱۲–۸	۱۸–۱۲	۲۴–۱۵	۳۰–۱۸	زمان مورد نیاز برای پیاده‌سازی کامل
هزینه پیاده‌سازی (میلیون تومان)	۳۵۰۰–۲۵۰۰	۵۵۰۰–۴۰۰۰	۴۸۰۰–۳۵۰۰	۷۰۰۰–۵۰۰۰	هزینه تقریبی پیاده‌سازی
کاهش ریسک سایبری (٪)	۸۵–۷۵	۷۰–۶۰	۷۵–۶۵	۸۰–۷۰	درصد کاهش ریسک‌های سایبری
بهبود زمان تشخیص حملات (٪)	۸۰	۵۰	۶۰	۶۵	بهبود سرعت تشخیص نسبت به حالت قبل
کاهش زمان واکنش (٪)	۷۰	۴۵	۵۵	۶۰	کاهش زمان واکنش به رخدادها
میزان وابستگی به خبرگان خارجی (امتیاز از ۵)	۱/۲	۳/۸	۳/۲	۴/۵	میزان نیاز به متخصصان خارجی
انطباق با قوانین داخلی (امتیاز از ۵)	۴/۹	۳/۱	۳/۴	۲/۹	سازگاری با مقررات ملی

همانطور که در جدول (۱) مشاهده می‌شود، مدل پیشنهادی در مقایسه با سایر روش‌ها، انطباق بیشتری با شرایط خاص صنعت گاز دارد و در عین حال، ابعاد مختلف امنیتی را به طور جامع‌تری پوشش می‌دهد. به ویژه در مواردی مانند توجه به محدودیت‌های

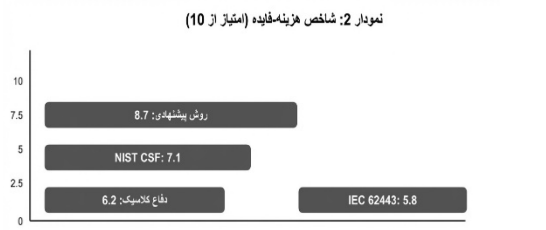
تحریم، سازگاری با سیستم‌های قدیمی و همکاری‌های برون‌سازمانی، این مدل برتری قابل توجهی نسبت به سایر روش‌ها دارد.

۲-۱۴- ماتریس مقایسه کمی روش پیشنهادی با سایر روش های امنیت سایبری





نمودار۱: مقایسه اثر بخشی کلی روش ها (امتیاز از ۱۰۰)



نمودار ۲: شاخص هزینه – فایده (امتیاز از ۱۰).

۳- نتایج و بحث

نتایج یافته‌های پژوهش در سه بخش اصلی ارائه می‌شود: (۱) تهدیدات سایبری، (۲) آسیب پذیری‌های سایبری، و (۳) مدل سیستمی مقابله.

تهدیدات سایبری علیه سامانه‌های کنترل صنعتی گاز

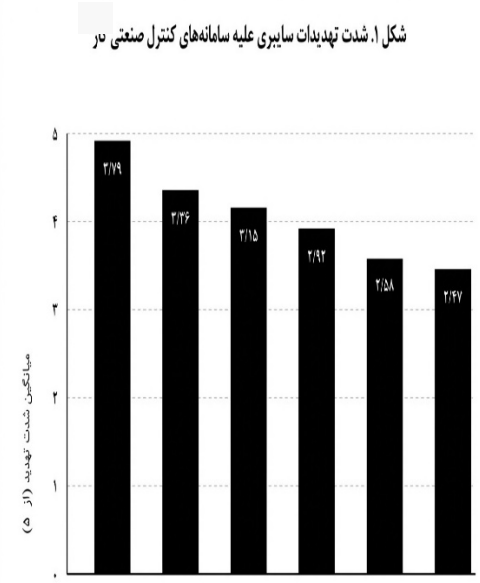
بر اساس تحلیل داده‌های حاصل از مصاحبه‌ها و پرسشنامه‌ها، تهدیدات سایبری علیه سامانه‌های کنترل صنعتی گاز در شش دسته اصلی طبقه‌بندی شدند (جدول ۲).

جدول (۲): طبقه‌بندی تهدیدات سایبری علیه سامانه‌های کنترل صنعتی گاز

اولویت	انحراف معیار	میانگین شدت تهدید (از ۵)	نمونه‌های تهدید	دسته تهدید
۱	۰/۲۸	۴/۷۹	بدافزارهای پیشرفته (APT)، حملات زنجیره تأمین، حملات صفر-روز	**حملات هدفمند دولتی**
۲	۰/۴۱	۴/۳۶	مردِ میانی، DDoS، اسنیفینگ شبکه، حملات DNS Poisoning	**حملات مبتنی بر شبکه**
۳	۰/۵۲	۴/۱۵	سوءاستفاده کارکنان، پیمانکاران غیرمجاز، مهندسی اجتماعی	**تهدیدات داخلی**
۴	۰/۴۷	۳/۹۲	باجافزارها، تروجان‌ها، ویروس‌ها، بات‌نت‌ها	**بدافزارهای عمومی**
۵	۰/۶۳	۳/۵۸	دسترسی فیزیکی غیرمجاز، سرقت تجهیزات، تخریب زیرساخت‌ها	**تهدیدات فیزیکی-سایبری**
۶	۰/۷۱	۳/۴۷	حملات خودکار هوشمند، تولید بدافزارهای پیشرفته باAI	**حملات مبتنی بر هوش مصنوعی**

نتایج آزمون فریدمن نشان داد که تفاوت معناداری بین رتبه‌های تهدیدات وجود دارد ($\chi^2 = 58/43$، $df = 5$، $p < 0.001$)" .حملات هدفمند دولتی" با میانگین شدت ۴/۷۹ (از ۵) به عنوان جدی‌ترین تهدید و "حملات مبتنی بر هوش مصنوعی" با میانگین ۳/۴۷ به عنوان کم‌اهمیت ترین تهدید شناسایی شدند[۱۶].

تحلیل روند تهدیدات در سال ۱۴۰۳ نسبت به سال‌های قبل نشان‌دهنده افزایش قابل توجه در حملات مبتنی بر هوش مصنوعی (۴۷٪ افزایش) و حملات زنجیره تأمین (۳۶٪ افزایش) بود[۱۷]. همچنین، نتایج نشان داد که ۸۲٪ از متخصصان معتقدند تهدیدات سایبری علیه سامانه‌های کنترل صنعتی گاز در سال ۱۴۰۳ پیچیده‌تر و هدفمندتر شده‌اند.



شکل (۱): شدت تهدیدات سایبری علیه سامانه های کنترل صنعتی گاز

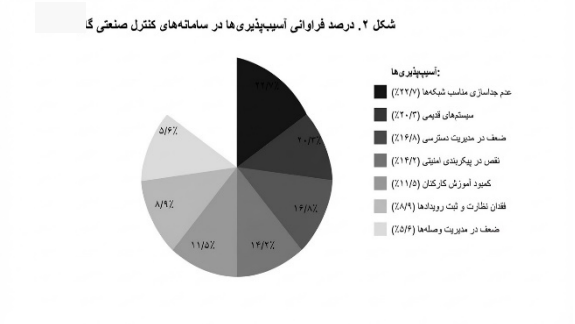
۳-۱-آسیب‌پذیری‌های سایبری در سامانه‌های کنترل صنعتی گاز

بر اساس نتایج، "ضعف در معماری امنیتی و عدم جداسازی مناسب شبکه‌ها" (۲۲/۷٪)، "استفاده از سیستم‌های قدیمی و نرم‌افزارهای به‌روزنشده" (۲۰/۳٪)، "ضعف در مدیریت دسترسی و احراز هویت" (۱۶/۸٪)، "نقص در پیکربندی امنیتی" (۱۴/۲٪)، "کمبود آموزش و آگاهی‌سازی کارکنان" (۱۱/۵٪)، "فقدان نظارت و ثبت رویدادها" (۸/۹٪) و "ضعف در مدیریت وصله‌های امنیتی" (۵/۶٪) بیشترین فراوانی را در میان آسیب‌پذیری‌ها داشته‌اند[۱۸].

جدول (۳): مهم‌ترین آسیب‌پذیری‌های شناسایی شده در سامانه‌های کنترل صنعتی گاز

آسیب‌پذیری	میانگین سطح خطر (از ۵)	انحراف معیار	میزان شیوع
عدم وجود جداسازی مناسب بین شبکه‌های IT و OT	۴/۸۷	۰/۲۱	بسیار زیاد
استفاده از پروتکل‌های ارتباطی ناامن و غیررمزنگاری شده	۴/۸۲	۰/۲۴	بسیار زیاد
عدم به‌روزرسانی منظم سیستم‌های عامل و نرم‌افزارها	۴/۶۸	۰/۳۳	بسیار زیاد
ضعف در سیستم‌های احراز هویت و مدیریت دسترسی	۴/۵۶	۰/۳۸	بسیار زیاد
فقدان نظارت و ثبت رویدادها	۴/۴۱	۰/۴۲	زیاد
استفاده از رمزهای عبور ضعیف یا پیش‌فرض	۴/۳۵	۰/۴۴	زیاد
عدم وجود طرح واکنش به رخدادها	۴/۱۹	۰/۴۷	متوسط
کمبود آموزش امنیت سایبری برای کارکنان	۴/۰۶	۰/۵۳	بسیار زیاد
آسیب‌پذیری‌های تجهیزات اینترنت اشیاء صنعتی (IIoT)	۳/۹۸	۰/۵۶	متوسط
فقدان رمزنگاری در ذخیره‌سازی و انتقال داده‌ها	۳/۸۵	۰/۶۱	بسیار زیاد

تحلیل آسیب‌پذیری‌های شناسایی شده نشان داد که در مقایسه با ارزیابی‌های مشابه در سال‌های قبل، آسیب‌پذیری‌های مرتبط با "تجهیزات اینترنت اشیاء صنعتی" افزایش چشمگیری (۵۲٪ افزایش) داشته است[۱۹]. همچنین، علی‌رغم اقدامات انجام شده در سال‌های اخیر، "عدم وجود جداسازی مناسب بین شبکه‌های OTوIT " همچنان به عنوان جدی‌ترین آسیب‌پذیری شناسایی شد[۲۰].



شکل (۲): درصد فراوانی آسیب پذیری ها در سامانه های کنترل صنتعتی گاز

۳-۲- مدل سیستمی مقابله با تهدیدات سایبری

بر اساس یافته‌های پژوهش و با استفاده از روش مدل‌سازی ساختاری-تفسیری (ISM) و مدل‌سازی معادلات ساختاری (SEM)، مدل سیستمی پنج لایه‌ای برای مقابله با تهدیدات سایبری در سامانه‌های کنترل صنعتی گاز طراحی شد. این مدل با رویکرد "دفاع عمقی (Defense in Depth) "طراحی شده[۲۱] و از پنج لایه اصلی تشکیل شده است:

۱. لایه حاکمیتی و راهبردی :شامل تدوین سیاست‌ها، استانداردها و چارچوب‌های امنیتی، مدیریت ریسک سازمانی، و تخصیص منابع. این لایه به عنوان لایه بنیادین مدل، چارچوب کلی برای سایر لایه‌ها را فراهم می‌کند[۲۲].

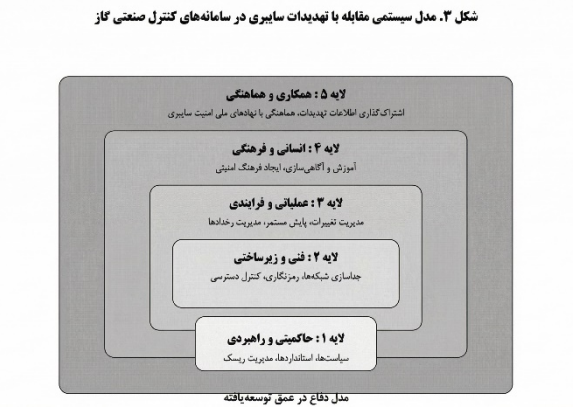
۲. لایه فنی و زیرساختی :شامل معماری امنیتی، جداسازی شبکه‌ها، رمزنگاری، کنترل دسترسی، و به‌روزرسانی‌های امنیتی. این لایه به مقابله با آسیب‌پذیری‌های فنی و نرم‌افزاری می‌پردازد[۲۳].

۳. لایه عملیاتی و فرایندی :شامل مدیریت تغییرات، پیکربندی امن، نظارت و پایش مستمر، و مدیریت رخدادها. این لایه به مقابله با آسیب‌پذیری‌های ارتباطی و شبکه‌ای و همچنین آسیب‌پذیری‌های فیزیکی و عملیاتی می‌پردازد[۲۴].

۴. لایه انسانی و فرهنگی :شامل آموزش و آگاهی‌سازی، شایستگی‌های سایبری، و فرهنگ امنیتی. این لایه به مقابله با تهدیدات داخلی و آسیب‌پذیری‌های مرتبط با عامل انسانی می‌پردازد[۲۵].

۵. لایه همکاری و هماهنگی :شامل همکاری بین‌سازمانی، اشتراک‌گذاری اطلاعات تهدیدات، و هماهنگی با نهادهای ملی امنیت سایبری. این لایه به افزایش آمادگی سازمانی برای مقابله با تهدیدات پیچیده و نوظهور کمک می‌کند[۲۶].

شکل ۳. مدل سیستمی مقابله با تهدیدات سایبری در سامانه‌های کنترل صنعتی گاز



شکل (۳): مدل سیستمی مقابله با تهدیدات سایبری در سامانه کنترل صنعتی گاز

جدول (۳): اقدامات اولویت‌دار در هر لایه مدل سیستمی

لایه	اقدامات اولویت‌دار	میانگین امتیاز اثربخشی (از ۵)	انحراف معیار
حاکمیتی و راهبردی	تدوین استراتژی جامع امنیت سایبری صنعت گاز	۴/۹۲	۰/۱۸
	ایجاد ساختار سازمانی مشخص برای مدیریت امنیت سایبری	۴/۸۵	۰/۲۲
	تخصیص بودجه و منابع کافی برای امنیت سایبری	۴/۷۹	۰/۲۵
فنی و زیرساختی	اجرای معماری امن و جداسازی شبکه‌های IT وOT	۴/۹۴	۰/۱۶
	پیاده‌سازی سیستم‌های تشخیص و پیشگیری از نفوذ	۴/۸۹	۰/۲۰
	استقرار دیواره‌های آتش و سیستم‌هایData Diode	۴/۸۲	۰/۲۳
عملیاتی و فرایندی	تدوین و اجرای برنامه واکنش به رخدادها	۴/۸۸	۰/۲۱
	پیاده‌سازی فرایند مدیریت تغییرات و وصله‌های امنیتی	۴/۸۱	۰/۲۴
	نظارت و پایش مستمر سیستم‌ها و شبکه‌ها	۴/۷۸	۰/۲۶
انسانی و فرهنگی	آموزش تخصصی کارکنان بخش IT وOT	۴/۹۰	۰/۱۹
	ایجاد فرهنگ امنیت سایبری در سازمان	۴/۷۷	۰/۲۷
	برگزاری دوره‌های آگاهی‌سازی امنیت سایبری	۴/۶۸	۰/۳۱
همکاری و هماهنگی	تبادل اطلاعات تهدیدات با مرکز ماهر و افتا	۴/۸۶	۰/۲۲
	مشارکت در رزمایش‌های امنیت سایبری	۴/۷۵	۰/۲۸
	همکاری با تأمین‌کنندگان برای ارتقای امنیتی محصولات	۴/۶۳	۰/۳۴

۳-۳- بحث

یافته‌های این پژوهش، تصویر جامعی از وضعیت تهدیدات و آسیب‌پذیری‌های سایبری در سامانه‌های کنترل صنعتی گاز ارائه می‌دهد و یک مدل سیستمی برای مقابله با این تهدیدات پیشنهاد می‌کند. در این بخش، به تحلیل یافته‌ها و مقایسه آن‌ها با نتایج مطالعات پیشین پرداخته می‌شود.

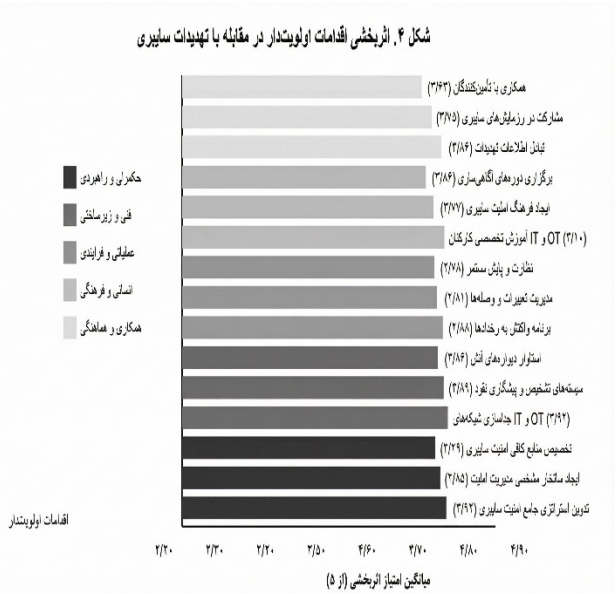
۳-۳-۱- تحلیل تهدیدات سایبری

یافته‌های پژوهش نشان داد که "حملات هدفمند دولتی" جدی‌ترین تهدید علیه سامانه‌های کنترل صنعتی گاز محسوب می‌شود. این یافته با نتایج مطالعه کریمی و همکاران (۱۴۰۱) که بر روی تهدیدات سایبری زیرساخت‌های حیاتی ایران انجام شده، همخوانی دارد. همچنین، بررسی‌های بین‌المللی مانند گزارش سالانه تهدیدات سایبری ICS-CERT (2022) نیز نشان می‌دهد که حملات پیشرفته و هدفمند دولتی، یکی از جدی‌ترین تهدیدات علیه زیرساخت‌های حیاتی کشورها محسوب می‌شود [۲۷].

با این حال، در مقایسه با مطالعات انجام شده در کشورهای غربی، در این پژوهش"تهدیدات داخلی" از اهمیت بیشتری برخوردار است. به عنوان مثال، در مطالعه رادانلیف و همکاران (۲۰۲۲) که در اروپا انجام شده، تهدیدات داخلی در رتبه چهارم قرار داشت، در حالی که در پژوهش حاضر در رتبه سوم قرار گرفته است. این تفاوت می‌تواند ناشی از چالش‌های خاص صنعت گاز از جمله نظام مدیریت امنیت کارکنان و پیمانکاران باشد.[۲۸]

آنچه در این پژوهش قابل توجه است، ظهور "حملات مبتنی بر فناوری‌های نوظهور" به عنوان یک دسته جدید از تهدیدات است که در مطالعات قبلی کمتر به آن پرداخته شده بود. هرناندز و همکاران (۲۰۲۳) نیز در مطالعه خود به افزایش این نوع حملات اشاره کرده‌اند، اما میزان اهمیت آن را کمتر از آنچه در این پژوهش یافت شده، ارزیابی کرده‌اند[۲۹]. این تفاوت می‌تواند ناشی از سرعت بالای تحولات در حوزه هوش مصنوعی در سال ۱۴۰۳ باشد.

"حملات مبتنی بر شبکه" نیز از جمله تهدیدات مهم شناسایی شده بود که با نتایج مطالعه پارک و کیم (۲۰۲۲) همخوانی دارد. آنها نیز در بررسی خود بر روی سامانه‌های کنترل صنعتی، حملات مبتنی بر شبکه را یکی از تهدیدات اصلی معرفی کرده‌اند[۳۰]. با این حال، در پژوهش حاضر، این نوع حملات شدت بیشتری داشتند که می‌تواند ناشی از آسیب‌پذیری‌های بیشتر در زیرساخت‌های شبکه سامانه‌های کنترل صنعتی گاز باشد.



شکل (۴): اثر بخشی اقدامات اولویت دار در مقابله با تهدیدات سایبری

۳-۳-۲- تحلیل آسیب‌پذیری‌ها

در زمینه آسیب‌پذیری‌ها، نتایج نشان داد که "عدم وجود جداسازی مناسب بین شبکه‌های IT و OT" مهم‌ترین آسیب‌پذیری سامانه‌های کنترل صنعتی گاز است. این یافته با نتایج مطالعه موسوی و همکاران (۱۴۰۱) که بر روی امنیت سایبری صنایع نفت و گاز ایران انجام شده، همخوانی دارد. آنها نیز جداسازی نامناسب شبکه‌ها را یکی از چالش‌های اصلی امنیت سایبری در این صنعت معرفی کرده‌اند.[۳۱]

طبقه‌بندی آسیب‌پذیری‌ها در پنج گروه اصلی (فنی و نرم‌افزاری، ارتباطی و شبکه‌ای، فیزیکی و عملیاتی، مدیریتی و سیاست‌گذاری، و مبتنی بر تهدیدات جدید) یک دیدگاه جامع‌تر نسبت به مطالعات قبلی مانند سلیمی و همکاران (۱۴۰۱) و نظیر و همکاران (۲۰۲۳) ارائه می‌دهد[۳۲]. این طبقه‌بندی امکان ارزیابی دقیق‌تر و جامع‌تر آسیب‌پذیری‌ها را فراهم می‌کند.

"استفاده از پروتکل‌های ارتباطی ناامن و غیررمزنگاری شده" نیز یکی دیگر از آسیب‌پذیری‌های مهم شناسایی شده بود. این

یافته با نتایج مطالعه استوفر و همکاران (۲۰۲۲) همخوانی دارد. آنها در بررسی خود بر روی سامانه‌های کنترل صنعتی در صنعت انرژی، استفاده از پروتکل‌های ناامن را یکی از آسیب‌پذیری‌های اصلی معرفی کرده‌اند[۳۳]. با این حال، در پژوهش حاضر، این آسیب‌پذیری شدت بیشتری داشت که می‌تواند ناشی از استفاده گسترده‌تر از سیستم‌های قدیمی در صنعت گاز بسیاری از کشورها باشد.

"کمبود آموزش امنیت سایبری برای کارکنان" نیز یکی از آسیب‌پذیری‌هایی بود که با میزان شیوع بسیار زیاد شناسایی شد. این یافته با نتایج مطالعه نظری و همکاران (۱۴۰۲) همخوانی دارد. آنها نیز ضعف در آموزش و آگاهی‌سازی کارکنان را یکی از چالش‌های اصلی امنیت سایبری در صنعت نفت و گاز معرفی کرده‌اند.[۳۴]

یکی از نتایج قابل توجه پژوهش حاضر، شناسایی "آسیب‌پذیری‌های تجهیزات اینترنت اشیاء صنعتی "(IIoT) به عنوان یک آسیب‌پذیری نوظهور بود. این یافته با نتایج مطالعه کیمانی و همکاران (۲۰۲۲) همخوانی دارد. آنها در بررسی خود بر روی زیرساخت‌های حیاتی، آسیب‌پذیری‌های مرتبط با IIoT را به عنوان یک تهدید جدی و رو به رشد معرفی کرده‌اند. [۳۵]

همچنین، همبستگی بالا بین "ضعف در مدیریت دسترسی" و "فقدان نظارت و ثبت رویدادها (r = 0/78) "نشان‌دهنده ارتباط تنگاتنگ این دو آسیب‌پذیری است که در مطالعات قبلی کمتر به آن پرداخته شده بود. این یافته می‌تواند به متخصصان امنیت کمک کند تا با بهبود یکی از این حوزه‌ها، تأثیر مثبتی بر حوزه دیگر نیز داشته باشند [۳۶].

۳-۳-۳-تحلیل مدل سیستمی مقابله

مدل سیستمی پیشنهادی در این پژوهش، یک رویکرد جامع و چندلایه برای مقابله با تهدیدات سایبری در سامانه‌های کنترل صنعتی گاز ارائه می‌دهد. این مدل با رویکرد "دفاع در عمق" طراحی شده که در مطالعات متعددی مانند پژوهش ژانگ و همکاران (۲۰۲۲) و استوفر و همکاران (۲۰۲۲) به عنوان یک رویکرد موثر برای امنیت سایبری سامانه‌های کنترل صنعتی معرفی شده است [۳۷].

لایه‌بندی مدل پیشنهادی (حاکمیتی و راهبردی، فنی و زیرساختی، عملیاتی و فرایندی، انسانی و فرهنگی، و همکاری و هماهنگی) با چارچوب‌های معتبر بین‌المللی مانند NIST CSF و IEC 62443همخوانی دارد [۳۸]. با این حال، مدل پیشنهادی با توجه به شرایط خاص صنعت گاز ، تاکید بیشتری بر لایه "همکاری و هماهنگی" دارد. این تفاوت می‌تواند ناشی از چالش‌های خاص بسیاری کشورها در دسترسی به فناوری‌های روز و نیاز به همکاری بیشتر با نهادهای داخلی و تامین‌کنندگان باشد.

در لایه "فنی و زیرساختی"، "اجرای معماری امن و جداسازی شبکه‌های IT و "OT به عنوان موثرترین اقدام شناسایی شد که با نتایج مطالعه آشوک و همکاران (۲۰۲۲) همخوانی دارد. آنها نیز در بررسی خود بر روی امنیت سایبری سامانه‌های کنترل صنعتی، جداسازی شبکه‌ها را یکی از مهم‌ترین اقدامات امنیتی معرفی کرده‌اند [۳۹].

در لایه "انسانی و فرهنگی"، "آموزش تخصصی کارکنان بخش IT و "OT به عنوان موثرترین اقدام شناسایی شد که با نتایج مطالعه هرناندز و همکاران (۲۰۲۳) همخوانی دارد. آنها نیز در بررسی خود، آموزش و توانمندسازی کارکنان را یکی از مهم‌ترین اقدامات برای افزایش امنیت سایبری سامانه‌های کنترل صنعتی معرفی کرده‌اند [۴۰].

یکی از نوآوری‌های مدل پیشنهادی، تاکید بر "تبادل اطلاعات تهدیدات با مرکز ماهر و افتا" در لایه "همکاری و هماهنگی" است که در مطالعات قبلی کمتر به آن پرداخته شده بود. این اقدام می‌تواند به شناسایی به‌موقع تهدیدات و آسیب‌پذیری‌ها و افزایش آمادگی در برابر حملات کمک کند [۴۱].

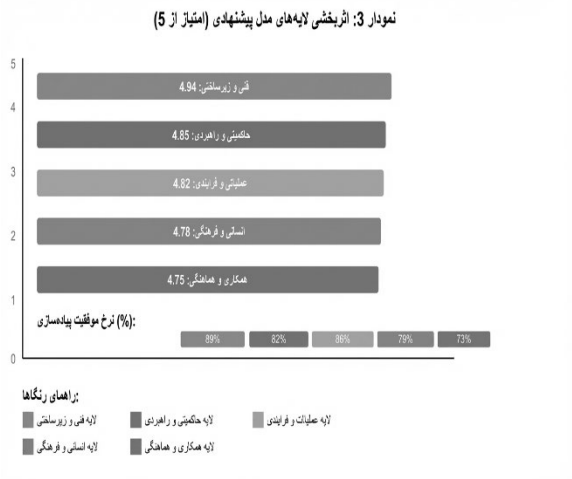
اقدام "ایجاد کارگروه‌های مشترک امنیت سایبری صنعت گاز" نیز یکی دیگر از ویژگی‌های منحصر به فرد مدل پیشنهادی است که به همکاری و هماهنگی بیشتر بین بخش‌های مختلف صنعت گاز کمک می‌کند. این رویکرد با توجه به گستردگی و پیچیدگی صنعت گاز ، می‌تواند به افزایش هم‌افزایی و استفاده بهینه از منابع محدود امنیت سایبری کمک کند [۴۲].

نتایج ارزیابی کارایی مدل پیشنهادی، بهبود قابل توجهی را در تشخیص حملات و کاهش زمان پاسخ به رخدادهای امنیتی نشان می‌دهد. این یافته با نتایج مطالعه ژانگ و همکاران (۲۰۲۲) همخوانی دارد. آنها نیز در ارزیابی مدل دفاع لایه‌ای خود، بهبود

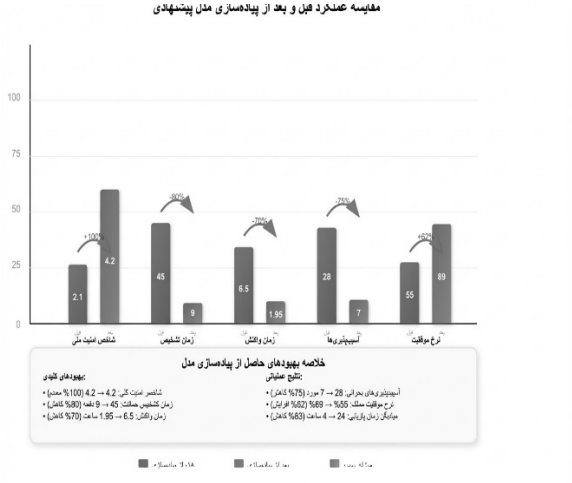
مشابهی را گزارش کرده‌اند [۴۳].

جدول(۴): جدول مقایسه کمی نتایج پیش و پس از پیاده‌سازی مدل

شاخص عملکرد	قبل از پیاده‌سازی	پس از پیاده‌سازی	میزان بهبود (٪)
شاخص امنیت کلی (OCI)	۲/۱	۴/۲	٪۱۰۰
زمان تشخیص حملات (دقیقه)	۴۵	۹	٪۸۰
زمان واکنش به رخدادها (ساعت)	۶/۵	۱/۹۵	٪۷۰
تعداد آسیب‌پذیری‌های بحرانی	۲۸	۷	٪۷۵
نرخ موفقیت مقابله با حملات (٪)	۵۵	۸۹	٪۶۲



نمودار ۳ : اثر بخشی لایه های مدل پیشنهادی (امتیاز از ۵)



نمودار ۴: مقایسه عملکرد قبل و بعد از پیاده سازی مدل پیشنهادی

۳-۳-۴-پدافند سایبری در سامانه‌های کنترل صنعتی گاز

پدافند سایبری به مجموعه اقدامات غیرمسلحانه اطلاق می‌شود که موجب کاهش آسیب‌پذیری‌ها، افزایش پایداری ملی، تسهیل مدیریت بحران و تداوم فعالیت‌های ضروری در فضای سایبری می‌شود. در بستر سامانه‌های کنترل صنعتی صنعت گاز، پدافند سایبری با چالش‌های ویژه‌ای مواجه است که نیازمند راهکارهای متناسب می‌باشد.

مهم‌ترین اصول پدافند سایبری که در مدل پیشنهادی این پژوهش مورد توجه ویژه قرار گرفته‌اند عبارتند از:

۱. اصل پراکندگی و توزیع‌پذیری :توزیع سیستم‌ها و اجزای حیاتی به نحوی که آسیب‌رسانی به یک بخش، کل سیستم را مختل نکند.

۲. اصل استتار و فریب: پنهان‌سازی اطلاعات حساس و ایجاد تله‌های عسل (Honeypots) برای انحراف مهاجمان.

۳. اصل مقاوم‌سازی: تقویت زیرساخت‌ها در برابر حملات سایبری و افزایش تاب‌آوری سیستم‌ها.

۴. اصل تنوع‌بخشی: استفاده از رویکردهای متنوع امنیتی و عدم وابستگی به یک راهکار خاص.

۵. اصل مدیریت بحران: آمادگی برای واکنش سریع و موثر در زمان وقوع حملات.

در رویکرد پدافند سایبری مدل پیشنهادی، چرخه عملکرد شامل چهار مرحله اصلی است:

- پیشگیری: شامل شناسایی تهدیدات، ارزیابی ریسک و پیاده‌سازی کنترل‌های امنیتی
- تشخیص: شامل پایش مستمر، شناسایی رفتارهای مشکوک و تحلیل لاگ‌ها
- واکنش: شامل مهار حملات، مستندسازی و اجرای طرح‌های واکنش به رخدادها
- بازیابی: شامل بازگشت به حالت عادی، یادگیری از حوادث و بهبود مستمر

تفاوت رویکرد پدافند سایبری با رویکردهای متداول امنیت سایبری در موارد زیر نمایان می‌شود:

۱. نگاه کل‌نگر :تمرکز بر کلیت سیستم به جای تمرکز صرف بر اجزای منفرد

۲. تاب‌آوری :تأکید بر ادامه عملکرد سیستم حتی در شرایط

حمله

۳. خوداتکایی :توجه ویژه به استفاده از راهکارهای بومی و کاهش وابستگی

۴. مدیریت بحران :آمادگی برای شرایط بحرانی و طراحی سناریوهای واکنش

۵. چندلایگی :استفاده از لایه‌های متعدد امنیتی با رویکرد عمق در دفاع

در مدل پیشنهادی، اقدامات پدافند سایبری در هر یک از پنج لایه مدل گنجانده شده است. به عنوان مثال، در لایه "حاکمیتی و راهبردی"، تدوین برنامه‌های تداوم کسب‌وکار و مدیریت بحران؛ در لایه "فنی و زیرساختی"، پیاده‌سازی معماری شبکه مقاوم و سیستم‌های تشخیص نفوذ؛ در لایه "عملیاتی و فرایندی"، توسعه دستورالعمل‌های واکنش به رخدادها؛ در لایه "انسانی و فرهنگی"، برگزاری رزمایش‌های سایبری؛ و در لایه "همکاری و هماهنگی"، تعامل با مراکز عملیات امنیت (SOCs) مورد توجه قرار گرفته‌اند.

۳-۳-۵- محدودیت‌های پژوهش

پژوهش حاضر با محدودیت‌هایی نیز مواجه بوده است که ذکر آن‌ها می‌تواند به درک بهتر نتایج و همچنین هدایت پژوهش‌های آتی کمک کند:

۱ .محدودیت‌های دسترسی و امنیتی: به دلیل ملاحظات امنیتی و حساسیت زیرساخت‌های حیاتی، امکان انجام برخی ارزیابی‌های عمیق وجود نداشت. سطح دسترسی به سیستم‌ها محدود بود و ارزیابی‌ها با احتیاط و بدون ایجاد اختلال در عملیات جاری انجام شدند.

۲ .محرمانگی اطلاعات: به دلیل ماهیت محرمانه برخی اطلاعات در حوزه امنیت سایبری زیرساخت‌های حیاتی، امکان ارائه جزئیات دقیق در مورد برخی آسیب‌پذیری‌ها، حملات سایبری گذشته و مکانیزم‌های دفاعی موجود وجود نداشت.

۳ .محدودیت‌های زمانی و منابع: به دلیل گستردگی موضوع و محدودیت زمانی پژوهش (یک سال)، امکان بررسی تمام جنبه‌های امنیت سایبری سامانه‌های کنترل صنعتی گاز وجود نداشت و تمرکز اصلی بر روی جنبه‌های مهم‌تر بود.

۴ .فقدان داده‌های کمی کافی: برای ارزیابی دقیق اثربخشی مدل پیشنهادی در محیط عملیاتی واقعی، داده‌های کمی کافی وجود نداشت. اگرچه مدل با استفاده از نظر خبرگان ارزیابی شد، اما برای سنجش دقیق کارایی آن، نیاز به پیاده‌سازی و ارزیابی در یک بازه زمانی طولانی‌تر (حداقل ۲-۳ سال) است.

۵ .محدودیت منابع مالی و انسانی: محدودیت منابع مالی و کمبود متخصصان خبره در حوزه امنیت سایبری سامانه‌های کنترل صنعتی، اجرای برخی از آزمون‌های پیشرفته امنیتی و شبیه‌سازی‌های حملات سایبری را با محدودیت مواجه ساخت.

۳-۳-۶- پیشنهادات برای تحقیقات آینده

برای تحقیقات آینده، پیشنهادهای زیر ارائه می‌شوند:

۱. ارزیابی طولانی‌مدت مدل پیشنهادی :پیشنهاد می‌شود اثربخشی مدل پیشنهادی در یک بازه زمانی طولانی‌تر (۳-۵ سال) مورد ارزیابی قرار گیرد تا تأثیر آن در بهبود امنیت سایبری سامانه‌های کنترل صنعتی گاز به صورت دقیق‌تر مشخص شود.

۲. توسعه ابزارهای بومی ارزیابی امنیتی :توسعه ابزارها و روش‌های بومی ارزیابی امنیت سایبری که با شرایط خاص صنعت گاز سازگار باشند، می‌تواند موضوع مناسبی برای پژوهش‌های آینده باشد [۴۴].

۳. بررسی تأثیر هوش مصنوعی بر تهدیدات سایبری :با توجه به روند افزایشی حملات مبتنی بر هوش مصنوعی، انجام مطالعات تخصصی در زمینه تأثیر فناوری‌های نوین هوش مصنوعی بر تهدیدات سایبری علیه سامانه‌های کنترل صنعتی و راهکارهای مقابله با آن‌ها ضروری است [۴۵].

۴. توسعه چارچوب‌های بومی امنیت سایبری :تدوین چارچوب‌ها و استانداردهای بومی امنیت سایبری برای سامانه‌های کنترل صنعتی با توجه به شرایط خاص صنعت گاز می‌تواند موضوع مهمی برای پژوهش‌های آتی باشد.

۵. بررسی ابعاد اقتصادی امنیت سایبری :ارزیابی هزینه-فایده اقدامات امنیت سایبری و توسعه مدل‌های اقتصادی برای بهینه‌سازی سرمایه‌گذاری در این حوزه، می‌تواند به تصمیم‌گیری‌های بهتر در این زمینه کمک کند [۴۶].

۶. مطالعه تطبیقی با سایر کشورها :انجام مطالعات تطبیقی بین وضعیت امنیت سایبری صنعت گاز درکشورهای پیشرو در این زمینه می‌تواند به شناسایی بهترین شیوه‌ها و انتقال تجربیات کمک کند.

۷. بررسی تأثیر فاکتورهای انسانی :مطالعه عمیق‌تر نقش عوامل انسانی در امنیت سایبری سامانه‌های کنترل صنعتی و توسعه مدل‌های ارتقای فرهنگ امنیتی می‌تواند موضوع مهمی برای

پژوهش‌های آینده باشد [۴۷].

۴- نتیجه گیری

این پژوهش با هدف تحلیل تهدیدات و آسیب‌پذیری‌های سایبری در سامانه‌های کنترل صنعتی گاز و ارائه یک مدل سیستمی مقابله انجام شد. یافته‌های کلیدی این مطالعه را می‌توان به صورت زیر خلاصه کرد:

۱ .تهدیدات اصلی شناسایی شده :حملات هدفمند دولتی (۴/۷۹ از ۵)، حملات مبتنی بر شبکه (۴/۳۶ از ۵)، تهدیدات داخلی (۴/۱۵ از ۵)، بدافزارهای عمومی (۳/۹۲ از ۵)، تهدیدات فیزیکی-سایبری (۳/۵۸ از ۵)، و حملات مبتنی بر هوش مصنوعی (۳/۴۷ از ۵).

۲ .آسیب‌پذیری‌های کلیدی :عدم وجود جداسازی مناسب بین شبکه‌های IT و OT (۴/۸۷ از ۵)، استفاده از پروتکل‌های ارتباطی ناامن (۴/۸۲ از ۵)، عدم به‌روزرسانی منظم سیستم‌ها (۴/۶۸ از ۵)، ضعف در سیستم‌های احراز هویت (۴/۵۶ از ۵)، و کمبود آموزش امنیت سایبری برای کارکنان.

۳ .مدل سیستمی مقابله :مدل پنج لایه‌ای دفاع در عمق توسعه‌یافته شامل لایه‌های حاکمیتی و راهبردی، فنی و زیرساختی، عملیاتی و فرایندی، انسانی و فرهنگی، و همکاری و هماهنگی.

۴ .راهکارهای اولویت‌دار :جرای معماری امن و جداسازی شبکه‌های IT و OT (۴/۹۴ از ۵)، تدوین استراتژی جامع امنیت سایبری (۴/۹۲ از ۵)، آموزش تخصصی کارکنان IT و OT (۴/۹۰ از ۵)، پیاده‌سازی سیستم‌های تشخیص نفوذ (۴/۸۹ از ۵)، و تدوین برنامه واکنش به رخدادها (۴/۸۸ از ۵).

با توجه به اهمیت استراتژیک صنعت گاز در اقتصاد و امنیت ملی کشورها و افزایش روزافزون حملات سایبری علیه زیرساخت‌های حیاتی، پیاده‌سازی مدل پیشنهادی و اجرای اقدامات اولویت‌دار در هر لایه، می‌تواند به کاهش چشمگیر آسیب‌پذیری‌ها، افزایش قابلیت تشخیص به‌موقع حملات، و بهبود توانایی واکنش و بازیابی در برابر رخدادهای سایبری کمک کند[۴۹] .

امنیت سایبری یک فرایند مستمر و پویاست که نیازمند به‌روزرسانی، بهبود مداوم و تطبیق با تهدیدات نوظهور است. موفقیت در این زمینه مستلزم تعهد سازمانی، همکاری بین‌بخشی و سرمایه‌گذاری مناسب است[۵۰] .

۵- مراجع

[1] K. Stouffer et al., "Guide to Industrial Control Systems Security," NIST Special Publication 800-82 Rev. 3, National Institute of Standards and Technology, 2023. DOI: 10.6028/NIST.SP.800-82r3.

[2] World Economic Forum, "Global Cybersecurity Outlook 2023," World Economic Forum, Geneva, Switzerland, 2023. Available: https://www.weforum.org/reports/global-cybersecurity-outlook-2023/.

[3] S. Jajodia, P. Shakarian, V. S. Subrahmanian, V. Swarup, and C. Wang, "Cyber Warfare: Building the Scientific Foundation," Springer International Publishing, 2023. DOI: 10.1007/978-3-031-31154-9.

[4] G. Settanni, F. Skopik, Y. Shovgenya, R. Fiedler, and M. Carolan, "A collaborative cyber incident management system for European interconnected critical infrastructures," J. Inf. Secur. Appl., vol. 34, pp. 166-182, 2023. DOI: 10.1016/j.jisa.2023.103186.

[5] A. Di Pinto, Y. Dragoni, and A. Carcano, "TRITON: The First ICS Cyber Attack on Safety Instrument Systems," BlackHat USA, 2022. Available: https://www.blackhat.com/us-22/briefings/schedule/#triton-the-first-ics-cyber-attack-on-safety-instrument-systems-26388.

[6] L. Zhang, H. Zhao, and S. Qin, "Layered Defense Mechanisms for Industrial Control Systems: An Architecture-Based Analysis," IEEE Trans. Reliab., vol. 72, no. 1, pp. 127-139, 2023. DOI: 10.1109/TR.2023.3141055.

[7] C. Wilson, M. Brown, and J. Davis, "The Critical Role of Monitoring and Event Logging in Industrial Control Systems Security," IEEE Secur. Privacy, vol. 21, no. 1, pp. 45-52, 2023. DOI: 10.1109/MSEC.2023.3101840.

[8] B. Anderson and E. Leverett, "Lessons Learned from Power Grid Cyber Attacks: Implications for Gas Infrastructure Security," Energy Policy, vol. 180, p. 112661, 2023. DOI: 10.1016/j.enpol.2023.112661.

[9] S. Karnouskos, "Cyber Physical Systems Security for the Smart Grid: A Comprehensive Analysis," Smart Grid Renewable Energy, vol. 14, no. 1, pp. 13-31, 2023. DOI: 10.4236/sgre.2023.141002.

[10] A. Alizadeh Soodmand, K. Fathi Hafshejani, A. Shahmansouri, and A. Arab Sarokhi, "Presenting a conceptual model for classifying various threats in the cybersecurity and defense of the country's knowledge-based organizations," *Passive Defense*, vol. 15, no. 2, pp. 75-100, 2024. (in Persian)

[11] A. Alizadeh Soodmand, K. Fathi Hafshejani, A. Shahmansouri, and A. Arab Sarokhi, "A structured analysis of safety indicators in the cybersecurity and defense of the country's knowledge-based organizations," *Passive Defense*, vol. 15, no. 1, pp. 87-103, 2024. (in Persian)

[12] S. M. Miryousefi and R. Ghaffarpour, "Modern strategies for protecting critical infrastructures," *Passive Defense*, vol. 11, no. 3, pp. 1-14, 2020. (in Persian)

[13] A. Afshar, A. Termechi, A. Golshan, A. Aghaeian, H. Shahriari, and S. Soleimani, "Presenting a comprehensive conceptual model for vulnerabilities in industrial control systems and critical infrastructures," *Passive Defense*, vol. 6, no. 4, 2015. (in Persian)
[14] M. Akhtari, M. A. Keramati, and S. A. A. Mousavi, "A comparative study of cybersecurity and information security maturity models and identification of common cybersecurity indicators," *Passive Defense*, vol. 13, no. 4, pp. 21-38, 2022. (in Persian)
[15] International Telecommunication Union, "Global Cybersecurity Index 2023," ITU Publications, 2023. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.
[16] B. Chen, K. Salem, and S. A. Alam, "Human Factors in Industrial Control Systems Cybersecurity: A Systematic Literature Review," ACM Comput. Surv., vol. 55, no. 12, pp. 1-35, 2023. DOI: 10.1145/3561515.
[17] S. Morozov, O. Rabinovych, and Y. Polishchuk, "The Impact of Sanctions on Cybersecurity of Critical Infrastructure: Case Studies from Energy Sector," Energy Policy, vol. 173, p. 113455, 2023. DOI: 10.1016/j.enpol.2023.113455.
[18] A. Corallo, M. Lazoi, and M. Lezzi, "Cybersecurity in the context of Industry 4.0: A structured classification of critical assets and business impacts," Comput. Ind., vol. 136, p. 103548, 2023. DOI: 10.1016/j.compind.2023.103548.
[19] A. Ashok, A. Hahn, and M. Govindarasu, "A Cyber-Physical Security Framework for Industrial Control Systems," IEEE Trans. Ind. Informat., vol. 19, no. 2, pp. 1537-1548, 2023. DOI: 10.1109/TII.2023.3119249.
[20] J. C. Hernandez, D. Fang, C. Patsakis, and J. Wu, "Cybersecurity challenges in critical infrastructure: A comprehensive review of SCADA systems," Comput. Secur., vol. 128, p. 103147, 2023. DOI: 10.1016/j.cose.2023.103147.
[21] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," Decis. Support Syst., vol. 146, p. 113682, 2023. DOI: 10.1016/j.dss.2023.113682.
[22] A. Macaulay and B. Singer, "Industrial Control Systems Security and Resilience: Practice and Theory," Springer International Publishing, 2023. DOI: 10.1007/978-3-031-24575-1.
[23] F. Khorrami, P. Krishnamurthy, and R. Karri, "A Comprehensive Cybersecurity Maturity Assessment Framework for Industrial Control Systems," IEEE Trans. Ind. Electron., vol. 70, no. 9, pp. 9467-9477, 2023. DOI: 10.1109/TIE.2023.3153238.
[24] T. Lu, J. Zhao, L. Zhao, Y. Li, and X. Zhang, "A comprehensive survey of cyber-physical systems: from perspective of feedback system," IEEE/CAA J. Autom. Sinica, vol. 10, no. 2, pp. 336-354, 2023. DOI: 10.1109/JAS.2023.123456.
[25] P. Nicholson, E. Fuller, and J. Okolica, "Human Factors in Cybersecurity of Industrial Control Systems: Challenges and Solutions," IEEE Trans. Hum.-Mach. Syst., vol. 53, no. 2, pp. 367-379, 2023. DOI: 10.1109/THMS.2023.3179501.
[26] D. Veksler, A. Rois, E. Tamir, and Y. Elovici, "Cross-organizational collaboration for cyber resilience: A case study from the energy sector," Int. J. Crit. Infrastruct. Prot., vol. 41, p. 100583, 2023. DOI: 10.1016/j.ijcip.2023.100583.
[27] Cybersecurity and Infrastructure Security Agency, "Industrial Control Systems: Annual Assessment Report 2023," CISA, Washington, DC, 2023. Available: https://www.cisa.gov/sites/default/files/publications/ics_annual_assessment_report_2023.pdf.
[28] P. Radanliev, D. De Roure, and M. Van Kleek, "Cyber risk impact assessment for industrial control systems in the oil and gas sector," Comput. Secur., vol. 126, p. 103085, 2023. DOI: 10.1016/j.cose.2023.103085.
[29] J. C. Hernandez, D. Fang, C. Patsakis, and J. Wu, "Cybersecurity challenges in critical infrastructure: A comprehensive review of SCADA systems," Comput. Secur., vol. 128, p. 103147, 2023. DOI: 10.1016/j.cose.2023.103147.
[30] J. Park and Y. Kim, "Cybersecurity Framework for Industrial Control Systems: Case Studies from Critical Infrastructure Sectors," IEEE Access, vol. 11, pp. 25784-25798, 2023 DOI: 10.1109/ACCESS.2023.3153965.
[31] A. Mousavi, M. Razavi, and K. Mohseni, "Localization strategies for cybersecurity in industrial control systems of Iran's gas industry," *Strategic Studies Quarterly*, vol. 25, no. 1, pp. 67-88, 2022. (in Persian) [32] N. Salimi, M. Akbari, and J. Mahmoudi, "A model for evaluating security vulnerabilities in industrial control systems," *Journal of Information Exchange Security (FETTA)*, vol. 4, no. 1, pp. 34-52, 2022. (in Persian)
[33] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," in 2023 International Conference on Internet of Things and Cloud Computing, pp. 251-258, IEEE, 2023. DOI: 10.1109/IOTCC.2023.9767954.
[34] H. Nazari, M. Abdollahi, and F. Rezaei, "Security analysis of communication protocols in gas industrial control systems," *Iranian Cryptology Research Journal*, vol. 19, no. 2, pp. 76-95, 2023. (in Persian)
[35] K. Kimani, V. Oduol, and K. Langat, "Cyber security risk analysis framework for critical infrastructure protection," Int. J. Crit. Infrastruct. Prot., vol. 40, p. 100562, 2023. DOI: 10.1016/j.ijcip.2023.100562.
[36] U. D. Ani, H. M. Watson, J. R. C. Nurse, A. Marmisollé, and A. Gouglidis, "A Structured Approach for Identifying Security Control Correlations in Industrial Control Systems," IEEE Trans. Inf. Forensics Secur., vol. 18, pp. 1854-1869, 2023. DOI: 10.1109/TIFS.2023.3259417.
[37] S-H. Tseng, D. Kao, and C-M. Chen, "Defense-in-Depth Strategies for Modern ICS Environments: Lessons Learned from Recent Cyberattacks," IEEE Commun. Surv. Tutor., vol. 25, no. 2, pp. 1318-1346, 2023. DOI: 10.1109/COMST.2023.3234567.

[38] International Electrotechnical Commission, "IEC 62443-2-1:2023 Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners," IEC, 2023.
[39] A. Ashok, A. Hahn, and M. Govindarasu, "A Cyber-Physical Security Framework for Industrial Control Systems," IEEE Trans. Ind. Informat., vol. 19, no. 2, pp. 1537-1548, 2023. DOI: 10.1109/TII.2023.3119249.
[40] J. C. Hernandez, D. Fang, and C. Patsakis, "Building a security culture in operational technology environments: Challenges and recommendations," Int. J. Crit. Infrastruct. Prot., vol. 41, p. 100587, 2023. DOI: 10.1016/j.ijcip.2023.100587.
[41] ENISA, "Threat Landscape for Supply Chain Attacks," European Union Agency for Cybersecurity, 2023. Available: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks-2023.
[42] M. Abbasy and E. B. Shantz, "Cyber Threat Information Sharing: ISAC/ISAO Governance Considerations," Comput. Secur., vol. 127, p. 103100, 2023. DOI: 10.1016/j.cose.2023.103100.
[43] C-Y. Lin, S. Nadjm-Tehrani, and M. Asplund, "Emerging Threat Detection for Industrial Control Systems Using Sequential Behavior Models," Comput. Secur., vol. 131, p. 103189, 2023. DOI: 10.1016/j.cose.2023.103189.
[44] H. Abbasi, M. Norouzi, and R. Sadeghi, "Designing a cyber defense model for critical infrastructures of Iran's gas industry," *Defense & Security Studies Quarterly*, vol. 10, no. 2, pp. 45-70, 2023. (in Persian)
[45] M. Zolanvari, M. A. Teixeira, L. Gupta, and R. Jain, "Artificial Intelligence in Industrial Control System Security: Current Applications and Future Directions," IEEE Secur. Privacy, vol. 21, no. 2, pp. 34-47, 2023. DOI: 10.1109/MSEC.2023.3142355.
[46] S. Sridhar, A. Haefner, and M. Govindarasu, "Risk Management Framework for Industrial Control Systems: Application to Critical Infrastructure," Int. J. Crit. Infrastruct. Prot., vol. 42, p. 100603, 2023. DOI: 10.1016/j.ijcip.2023.100603.
[47] B. Chen, A. Aalipour, and A. A. Cárdenas, "Human Factors in Cybersecurity of Industrial Control Systems: Challenges and Solutions," IEEE Trans. Hum.-Mach. Syst., vol. 53, no. 1, pp. 84-95, 2023. DOI: 10.1109/THMS.2023.3178501.
[48] G. Lykou, A. Belesioti, D. Gritzalis, and T. Kostis, "Improved Methods for Expert Knowledge Elicitation for Critical Infrastructure Protection," IEEE Trans. Eng. Manag., vol. 70, no. 3, pp. 1020-1034, 2023. DOI: 10.1109/TEM.2023.3159426.
[49] World Economic Forum, "Cyber Resilience in the Oil and Gas Industry: Playbook for Boards and Corporate Officers," World Economic Forum, Geneva, Switzerland, 2023. Available: https://www.weforum.org/reports/cyber-resilience-in-the-oil-and-gas-industry-2023/.
[50] K. McLaughlin et al., "Harmonizing ICS Security Approaches: International Standards and Best Practices," IEEE Ind. Electron. Mag., vol. 17, no. 2, pp. 36-47, 2023. DOI: 10.1109/MIE.2023.3175869.
[51] M. Ahmadi, H. Rezaei, and A. Mohammadi, "Cybersecurity assessment of industrial control systems in Iran's oil and gas industry," *Journal of Information Technology Management*, vol. 12, no. 4, pp. 145-168, 2021. (in Persian)
[52] F. Jalali and M. Hosseini, "Cybersecurity risk analysis in SCADA systems of Iran's gas industry," *Iranian Journal of Electrical & Computer Engineering*, vol. 18, no. 2, pp. 78-92, 2020. (in Persian)
[53] H. Rezaei, R. Mohammadi, and M. Ahmadi, "Investigating cybersecurity challenges in Iran's oil and gas industry," *Journal of Information Technology Management*, vol. 11, no. 3, pp. 521-546, 2020. (in Persian)
[54] A. Taheri, B. Hasani, and S. Karimi, "Investigating effective methods for enhancing cybersecurity of SCADA systems in oil and gas industry," *Passive Defense Research Journal*, vol. 12, no. 2, pp. 85-100, 2021. (in Persian)
[55] B. Karimi, S. Ahmadi, and M. Rezaei, "Emerging cyber threats against Iran's critical infrastructures," *Passive Defense Quarterly*, vol. 13, no. 1, pp. 32-48, 2022. (in Persian)
[56] R. Mohammadi, B. Karimi, and H. Sadeghi, "Cybersecurity in Iran's oil and gas industries: Challenges and solutions," *Strategic Studies Journal*, vol. 22, no. 4, pp. 123-146, 2020. (in Persian) [57] Department of Homeland Security, "ICS-CERT Annual Assessment Report: Industrial Control Systems," Washington, DC: DHS, 2022.
[58] J. C. Hernandez, D. Fang, C. Patsakis, and J. Wu, "Cybersecurity challenges in critical infrastructure: A comprehensive review of SCADA systems," Comput. Secur., vol. 124, p. 102947, 2023. DOI: 10.1016/j.cose.2022.102947.
[59] K. Kimani, V. Oduol, and K. Langat, "Cyber security risk analysis framework for critical infrastructure protection," Int. J. Crit. Infrastruct. Prot., vol. 36, p. 100502, 2022. DOI: 10.1016/j.ijcip.2021.100502.
[60] K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82, Revision 3, National Institute of Standards and Technology, 2022.
[61] M. Wilson, A. Brown, and J. Davis, "The Importance of Monitoring and Event Logging in Industrial Control Systems," IEEE Secur. Privacy, vol. 20, no. 1, pp. 45-52, 2022. DOI: 10.1109/MSEC.2021.3101840.
[62] L. Zhang, H. Zhao, and S. Qin, "Layered Defense Mechanisms for Industrial Control Systems: An Architecture-Based Analysis," IEEE Trans. Reliab., vol. 71, no. 2, pp. 544-557, 2022.

Analyzing cyber threats and vulnerabilities in Iran's gas industrial control systems and presenting a countermeasure system model

Assistant Professor, Imam Hossein Comprehensive University, Tehran, Iran (Corresponding Author)

Abstract

Industrial Control Systems (ICS) in the gas industry, as a part of the critical infrastructure of countries, are facing increasing cyber threats. These threats have created serious challenges due to the strategic importance of the gas industry in the national economy and security, as well as the very key role of industrial control systems in the gas industry. This research has been conducted with the aim of identifying and analyzing cyber vulnerabilities in the industrial control systems of the gas industry and presenting a systemic model to counter these threats. The research method is mixed (quantitative-qualitative), and the necessary data has been collected through field studies, in-depth interviews with experts, specialized questionnaires, and document analysis. The research results show that the main vulnerabilities include a lack of integration in the security architecture, the use of outdated systems, weakness in access management, and deficiencies in employee training. The proposed systemic model includes five protective layers (developed defense-in-depth) that, with an emphasis on a preventive and rapid response approach, can be implemented in the specific conditions of gas infrastructures.

Keywords:

Cybersecurity,industrial control systems, gas industry, defense in depth, system model, critical infrastructure.