software patching and multi-level authentication should, hence, be embraced to reduce attacks. AI techniques can also be utilized in identifying IoT network irregularity.

- The role of standards and regulation

The lack of unified security standards for IoT devices remains a key issue. For example, some producers overlook data encryption procedures during transmission, thus leading to massive data leaks. Global standardization, like ISO/IEC 30141, aims at bringing together security requirements; however, the implementation of the standards requires a lot of time and investment. [6]

These factors highlight the need for a comprehensive approach to cybersecurity in the Internet of Things that addresses both technical and organizational aspects.

Conclusions

Cybersecurity of IoT systems requires a synthesis of theoretical solutions (e.g., quantum cryptography) and practical technologies (hardware protection, optical networks). Further research should focus on adapting these methods to resource-limited devices and developing unified security standards. Only a comprehensive approach will ensure reliable data protection in distributed IoT networks.

References

6. A. Slonopas, "IoT Cybersecurity: Strengthening Defenses against Threats," *American Public University*, May 03, 2024. https://www.apu.apus.edu/area-of-study/information-technology/resources/iot-cybersecurity-strengthening-defenses-against-threats/

7. Forescout Technologies, Inc., "What are the riskiest connected devices right now?," *Forescout*, Jun. 27, 2024. https://www.forescout.com/blog/what-are-the-riskiest-connected-devices-right-now/?utm_source=Securitylabru

8. R. A. Chou and J. Kliewer, "Secure distributed Storage: Rate-Privacy Trade-Off and XOR-Based coding scheme," *arXiv.org*, Jan. 13, 2020. https://arxiv.org/abs/2001.04241

9. D. Chai *et al.*, "Practical Lossless Federated Singular Vector Decomposition over Billion-Scale Data," *arXiv.org*, May 19, 2021. https://arxiv.org/abs/2105.08925

10. D. Dimitrov I., M. Balunović, N. Konstantinov, and M. Vechev, "Data leakage in federated averaging," *arXiv.org*, Jun. 24, 2022. https://arxiv.org/abs/2206.12395

11. "ISO/IEC 30141:2024," *ISO*. https://www.iso.org/standard/88800.html

UDK: 331.108.2:004.7:331.101.3

Student Yevhen Biezhyn
Vasyl' Stus Donetsk National University, Ukraine

DIVERSIFICATION OF THE WORK ENVIRONMENT: THE IMPACT OF ICT ON EMPLOYEE EFFICIENCY AND SATISFACTION

In the contemporary business landscape, certain digital technologies, including collaboration tools and analytical software, are transforming diversity management in organizations. This study explores the influence of these information and communication technologies (ICT) on two aspects: communication effectiveness in diverse teams and business process effectiveness of multicultural business processes. Here, it is relevant to consider how ICT facilitates diverse team integration and enhances their productivity overall.

Diversity problems and the role of digital technologies

Research has demonstrated that diversity in the workplace, though advantageous in general, can present challenges like communication gaps, disagreements, and unequal work burden. [1]

Adoption of technology to break communication barriers is necessary. For instance, sites that incorporate translation facilities, like Microsoft Teams and Zoom, allow for automatic language exchanges, significantly enhancing mutual understanding among employees from different cultural

and linguistic backgrounds. Also, business social networking sites, like Yammer, allow for trust establishment and enhance the degree of interaction between team members.

Research shows that ICT solutions can effectively address these issues using different mechanisms. [2]

Data analysis serves an important role in discrimination prevention. Tableau and Power BI, which are analytical systems, enable staff members to monitor employees' satisfaction, ascertain disparities in workload allocation, and recognize gaps in career development. With such capabilities, managers are able to prevent discrimination risks and ensure equal allocation of tasks.

Beneficial impact of ICT on productivity

Cloud-based applications like Google Workspace and Microsoft 365 enable teams with various skill sets to work on projects simultaneously. Collaboration software encourages the coming together of various ideas into solutions. Studies show that firms that have used collaboration technology have reduced time to complete work tasks by 25% and increased cross-functional collaboration in heterogeneous teams by 20%, especially in scenarios involving cross-cultural projects. [3]

Big data workflow analysis helps to identify individual employee behaviour patterns. Machine learning algorithms can predict the best team for specific tasks according to skills diversity. This creates more efficient task execution.

Management automation is also a significant factor. AI assistants like HR chatbots minimize subjectivity in hiring or assessing employees. This helps in the development of an inclusive culture where skills, rather than stereotypes, are assessed. [4]

Employee satisfaction and IT tools

Work personalization is an important part of employee happiness. Feedback apps on mobile, such as ‘Officevibe’, allow employees to conveniently flag a requirement or discomfort. CRM software interpreting such data allows personalization of the workplace to suit each individual employee.

Flexibility through the use of cloud technologies is also important. Cloud environments provide access to work materials anywhere, which is especially important for people with disabilities or those who simply want to work from home. As “Inclusionhub” notes, this approach improves satisfaction. [5]

The function of information systems in facilitating a heterogeneous environment

Information systems are an integral component of organizational process management, particularly when it comes to diversification operations. They facilitate searching, collecting, storing, transmitting, and processing information that pertains to business processes. To be more precise, the use of enterprise resource planning (ERP) systems allows organizations to have one information environment in which all team members can obtain critical information. This helps improve transparency and employees' trust and reduce the possibility of mistakes occurring due to misinformation.

Conclusions

The integration of information and communication technologies (ICT) in a multicultural workplace is an essential move towards improving the productivity and contentment of workers since it helps bridge the gap in communications, ensure equal access to information, and foster an inclusive culture. [6] The use of digital technologies, such as data analytics, cloud-based systems, and automated processes, not only helps reduce discrimination, but also makes diversity a competitive advantage for organizations. Thus, information technologies are increasingly being viewed as one of the main drivers of success for contemporary businesses that take into consideration the peculiarities of business processes and the interests of their workers.

List of references

1. C. Reinisch and N. Karimi, “Implicit communication challenges in culturally diverse workplaces,” 2020. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1435886/FULLTEXT01.pdf

2. M. A. Fazeli, H. Moghaddasi, A. Hosseini, F. Asadi, and H. Haghighi, "Application of ICT in effective crisis management: A systematic review," *Journal of Emergency Management*, vol. 19, no. 6, pp. 591–606, Nov. 2021, doi: 10.5055/jem.0612.
3. vorecol.com, "How can remote employee integration software address the challenges of crosscultural team dynamics?" https://vorecol.com/blogs/blog-how-can-remote-employee-integration-software-address-the-challenges-of-crosscultural-team-dynamics-151464
4. "AI for reducing bias in HR," Apr. 18, 2025. https://www.akoolblog.com/knowledge-base-article/ai-for-reducing-bias-in-hr
5. J. Howard, "The benefits of remote work for people with disabilities." https://www.inclusionhub.com/articles/benefits-of-remote-work
6. A. Sud, "How technology can help foster inclusivity and productivity at work," *TIME*, Aug. 12, 2021. [Online]. Available: https://time.com/6084759/technology-inclusive-productive-work/

UDK: 004.42:004.056:004.056.5
Student Yevhen Biezhyn
Vasyl' Stus Donetsk National University, Ukraine

APPLICATION OF PARALLEL COMPUTING IN CYBERSECURITY: VULNERABILITY ANALYSIS AND DATA PROTECTION

Modern information systems face a growing number of cyber threats, which requires the development of effective protection methods. Parallel computing is a technology that allows you to simultaneously perform several data processing operations, which significantly speed up the process of analysing vulnerabilities and ensure reliable information protection. The paper discusses the theoretical ramifications of applying these technologies to cybersecurity. [1]

Theoretical foundations of vulnerability analysis based on parallel computing

Vulnerability analysis is a methodical process that aims to identify information system weaknesses that are capable of being exploited for unauthorized access. Concurrent computing is a useful tool for streamlining this process since it enables concurrent processing of huge volumes of data.

Dynamic analysis, which is one of the techniques employed in security audits, [1] consists of executing code and observing its behaviour to determine possible security vulnerabilities. Parallel data processing allows for such analysis at the level of the entire system, quickly detecting anomalies in real time.

In addition, parallel computing is effectively used to test systems for penetration. For example, when scanning a network, several segments can be checked simultaneously, which significantly speeds up the process of identifying weaknesses. This is especially important for large organizations where the number of network access points can be measured in thousands.

Protecting data with parallel computing

Parallel computing also plays an important role in direct data protection. One of the key areas is real-time encryption. Encryption is a process that requires significant computing resources, especially when it comes to large amounts of data. Parallel algorithms allow you to distribute the load among several processors, which speed up key generation and processing of encrypted data.

Another important aspect is distributed security systems. [2] Clusters or massively parallel systems (MPP) provide high availability and resistance to DDoS attacks through load distribution across a number of nodes. Such systems automatically adapt to the situation, thereby proving to be efficient in fending off various kinds of cyberattacks.

Advantages and limitations of parallel computing in cybersecurity

Parallel computing has several benefits that make it vital in the cybersecurity sector. To begin with, it can efficiently enhance the rate of data processing, which is central to the analysis of vast