Issues of Ensuring the Security of Information Infrastructure of New Generation Enterprises

Alovsat Aliyev
Institute of Information Technology,
Baku, Azerbaijan
alovsat_qaraca@mail.ru
0000-0002-1174-8036

Roza Shahverdiyeva
Institute of Information Technology,
Baku, Azerbaijan
Azerbaijan Technical University
shahverdiyevar@gmail.com
0000-0003-0842-7300

Sunyakhanim Salimkhanova
Azerbaijan University of Architecture and Construction
sunyakhanim.salimkhanova@azmiu.edu.az

***Abstract*—The article is devoted to the study of issues of ensuring the security of the information infrastructure of new generation enterprises. The special relevance of the application of cybersecurity and Artificial Intelligence technologies in the process of Digital Transformation of Enterprises is shown. The directions of improving the security of the information infrastructure of enterprises based on Industry 4.0 and other digital technologies are noted. The main security technologies of the information infrastructure of new generation enterprises are given, its security parameters are studied, and the operating model of the security operations center is developed. An architectural-technological structural model of the security system of the information infrastructure of new generation enterprises is proposed. Relevant recommendations are given on the application and development prospects of the Industry 4.0 platform technologies in the development of a conceptual approach to ensuring the security of the information infrastructure of new generation enterprises.**

Keywords—digital transformation, digital technology, Next-generation enterprise, information infrastructure, cybersecurity technologies

I. INTRODUCTION

At present, the dynamic development of the most diverse areas of society and economy in the technological context has become one of the global trends. The processes of application of digital technologies and transformation in areas such as science, education, industry, etc. are being implemented rapidly. New initiatives are being put forward in the world to expand the application of digitalization and innovations. The development of areas of application of technologies such as artificial intelligence, Internet of Things (IoT), 5G, robotization, supercomputers, etc. necessitates the expansion of the high-tech sector and their complex application.

All this, reflected in international and national legislative documents, requires the improvement of the security of the information infrastructure of new generation enterprises on the basis of Industry 4.0 and other digital technologies, and the resolution of the security issues of its infrastructure. In such a situation, ensuring the security of the information infrastructure of new generation enterprises, the emergence of countless cybersecurity threats in the activities of the enterprise, and their prevention are considered of important issues.

The implementation of technological development, digitalization, cybersecurity, and Artificial Intelligence technologies in all areas of the country, the establishment of a digital ecosystem within the framework of digital development, the formation of successful enterprises and startups in the ICT field, and the support for the creation of innovation centers have been set as a task in the Digital Development Concept of Azerbaijan (https://president.az/az/articles/view/67938).

It is no coincidence that during the period covered by the Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027, in addition to organizing the formation and maintenance of a register of information security and cybersecurity risks, it is also intended to strengthen activities for the development of modern digital technologies, as well as technologies based on artificial intelligence, that can prevent threats related to information aggression and distortion of truth, and violation of national values (https://president.az/az/articles/view/60949). All this has necessitated the study of some of the current problems of ensuring the security of the information infrastructure of new generation enterprises at the national and regional levels. In this regard, ensuring the security of information infrastructure in new generation enterprises is a complex issue that encompasses not only technological approaches but also all aspects related to management and strategic planning. Therefore, developing the right approaches to such issues can increase both the stability of operations in enterprises and increase customer trust.

II. PROBLEM STATEMENT

The new paradigm of the current economy is aimed at taking into account the complexities of the rapidly developing world, where traditional models are no longer sufficient, and at solving a number of key problems. These innovations are reshaping the industry, and business models and leading to the emergence of a new generation technological economy. Ensuring the security of the information infrastructure of new generation enterprises, and increasing its cyber resilience based on digital technologies is a multifaceted problem. Developing a conceptual approach based on artificial intelligence technologies in a comprehensive manner to solve such problems is of great importance. Therefore, it is desirable for scientists and specialists in the relevant field to pay attention to such an urgent problem in their scientific works, and it is a significant contribution to the formation of a new generation economy.

Certain scientific research has been conducted in the relevant field on the issues of ensuring the security of the information infrastructure of new generation enterprises. There are relevant publications in scientific journals indexed in various high scientific databases in this field in different years. The requirements for solving the relevant problems set forth in those [1-7] publications should be taken into account in the complex formation of a new generation of the technological economy and in the analysis of its development problems. Therefore, although the analysis of the above mentioned problems has been studied to some extent in the scientific works of many scientists and specialists, the need for a deeper and more comprehensive study of this process, as

well as the development of various approaches to solving the problems that have arisen, still remains and remains relevant.

III. Security Technologies of the Information Infrastructure of New Generation Enterprises

New generation enterprises are the most modern enterprises that have the technical and technological infrastructure, necessary human and material resources that allow them to operate on the basis of digital transformation, innovative management models, flexibility and sustainable development principles. The main characteristics of such enterprises include: 1)Digital transformation and technological innovations, 2)Artificial intelligence, Big Data, cloud computing, IoT, 5G, etc. 3)Digital platforms and ecosystems, 4)Automated processes, 5)Smart systems, 6) Agile and adaptive management, 7)Investments in human capital and innovation, 8) Digital skills, 9)Data-driven management, 10)Sustainability and green economy principles, 11)New business models and digital revenue streams, 12)Cryptocurrencies and blockchain-based financial systems, etc.

New generation enterprises, unlike traditional enterprises, are enterprises that are formed and developed by prioritizing digitalization, innovation, flexibility and sustainable development. These enterprises have the opportunity to develop faster and adapt to market changes thanks to their business models integrated with modern technologies. Traditional enterprises, on the other hand, react to changes more slowly because they have a fundamental structure based on stability and long-term experience. Along with the development of the modern economy, enterprises are also transformed by adapting to changing market demands. As a result of this transformation, new generation enterprises based on digital technologies, operating with flexible management models and with the wide application of innovations have been formed. Traditional enterprises, on the other hand, have business structures based on stable, bureaucratic and mainly product-oriented approaches that have been applied for many years.

The differences between the new generation and traditional enterprises manifest in various aspects. New generation enterprises establish their activities entirely in a digital environment and provide their services through online platforms. Unlike traditional enterprises, they are not limited to only producing products or services, but also create an open innovation environment. The main differences between New Generation enterprises and traditional enterprises can be presented as in Table 1.

Table 1. Main differences between New generation enterprises and traditional enterprises

Features	New generation enterprises	Traditional enterprises
Application and use of techno-logies	Artificial intelligence, Big Data, blockchain, IoT, and cloud technologies are actively used	Mainly traditional technologies are used, digital transformation is relatively slow
Business model	Digital platforms, cloud-based services (SaaS, PaaS), sharing economy, open innovation	Mainly direct sales of products and services, traditional production and distribution models
Management structure	Agile structure, quickly adaptable decision-making mechanism	Hierarchical, bureaucratic and more static management structure
Work environment and collaboration	Remote and hybrid work models are widespread, open to collaboration and innovation	Primarily office-based work schedule, traditional working hours, and a structured work environment
Customer approach	Data-driven personalized services, real-time response to customer feedback	Mass production, standard products and services, late response
Innovation and market access	Rapid innovation cycle, collaboration with startup ecosystem	Slow innovation, traditional product development strategies
Financing and investment	Collective financing (crowdfunding), risk capital	Mainly bank loans, investors and traditional financing methods
Sustainability and social responsibility	Green technologies, carbon footprint reduction, circular economy principles	The focus is on profits, while sustainability issues may take a back seat

The results of empirical research and international experience should be taken into account in the formation of next-generation enterprises. They are of great importance in realizing the competitive advantages of next-generation enterprises and determining their development strategies.

Table 2 presents information on different approaches to the successful implementation of next-generation enterprises in some different countries.

Table 2. Strategies and results applied to next-generation enterprises in some countries

Countries/Enterprises	Applied strategy	Results achieved
Germany – Industry 4.0	Automated manufacturing and smart factories	25-30% increase in productivity, cost reduction
China – Alibaba	Artificial intelligence-based trading and the use of Big Data	Global leadership in e-commerce, effective logistics systems
USA – Tesla	Autonomous transportation and green energy strategies	Dominance in the electric car market, reducing carbon emissions
Sweden – Spotify	Mobile-based business model and Artificial Intelligence recommendation systems	Revolutionary changes in the music industry, market leadership
Singapore – Digital Government	Blockchain-based government services	80% reduction in paper documents, transparent management

Information security of new generation enterprises protects the information, software, networks, and systems that support the activities of the enterprise. Since the information infrastructure of enterprises provides for the processing and transmission of information on a larger scale using various digital tools, its security is of particular importance.

Ensuring the security of information infrastructure in new generation enterprises ensures the correct and reliable functioning of work environments integrated with modern technologies. The main security technologies applied to ensure the security of information infrastructure in new generation enterprises can be given as in Figure 1.

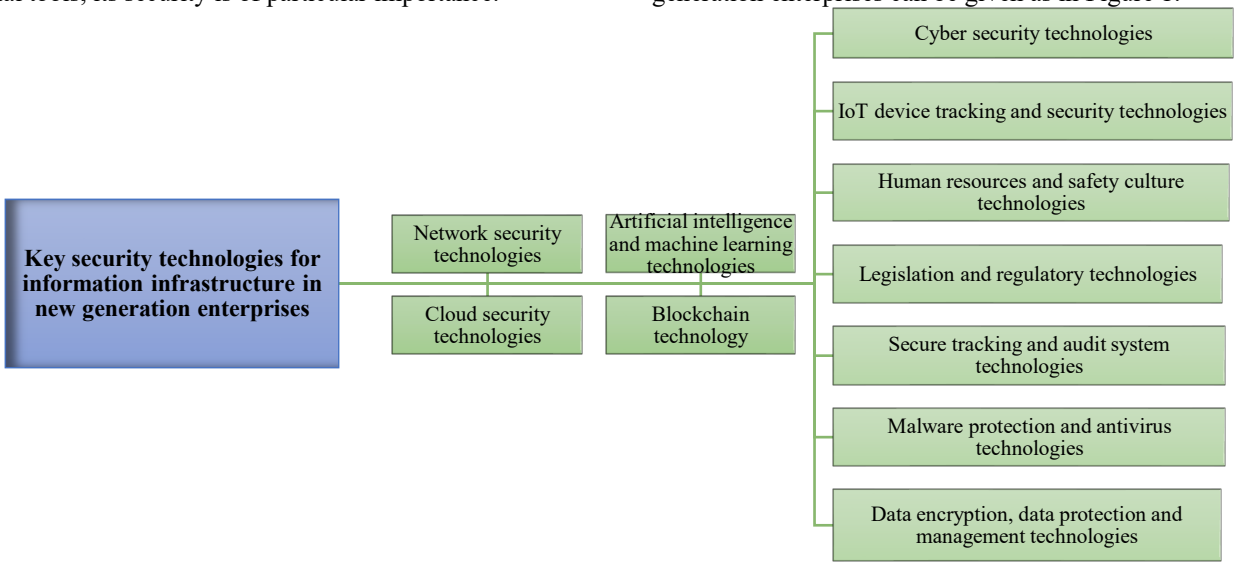

Fig. 1. Key security technologies for information infrastructure in new generation enterprises *(compiled by the authors based on the analysis and systematization of scientific literature)*

Ensuring the security of the information infrastructure of new generation enterprises requires a multidisciplinary and multidirectional approach. This approach includes both technological measures and organizational and legal measures. Ensuring security is possible not only on systems and tools but also by educating staff and complying with relevant legislative requirements. By systematically implementing these measures, organizations protect their data and operate sustainably and reliably. The implementation of security technologies in new generation enterprises helps organizations effectively manage the risks they face when operating in digital environments. These technologies not only ensure data protection but also increase the overall stability of the enterprise and maintain its customer trust. Regular updating and improvement of these measures, both technologically and managerially, is a guarantee of the long-term successful operation of the organization.

IV. Security Operations Center and Information Security Management System in New Generation Enterprises

Information security in enterprises is usually regulated and protected based on either the International Organization for Standardization ISO 27001: Information Security Management System or the NIST Cybersecurity Framework standard. The International Organization for Standardization ISO 27001 operates and implements a control-based approach that is suitable for auditing and accreditation. The NIST Cybersecurity Framework implements the prevention and response to cyberattacks. The NIST framework has a five-stage life cycle. Both approaches involve the integration of security controls and security management processes [8].

Both ISO 27002 and the NIST Cybersecurity Framework indicate which operational security procedures should be implemented. However, neither of them imposes a specific requirement for establishing a security operations center.

The primary purpose of a security operations center is to provide security for technology infrastructure and operations by monitoring and responding to incidents.

Some security operations centers may have broader authority to liaise with development teams to ensure secure service development. This can be highly effective for the business because it allows for faster security implementation.

This latter form of security operations center is sometimes known as an Integral Security Operations Center due to its strong integration [9].

The extent to which security operations center technology is used, the competencies of staff, and the development of processes can be expressed as in Figure 2. An example of a specific graph and its key elements are shown for each dimension [10].

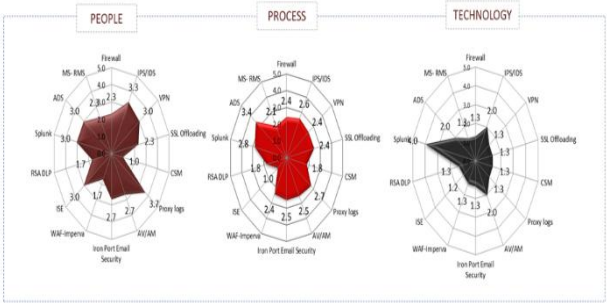

Fig.2. Security example of security operations center *(compiled by the authors based on the analysis and systematization of scientific literature)*

The security operations center team must then detect incoming attacks and respond to the incident as if it were a live attack [11]. The information security management scheme consists of more than 30 activity processes [12]. Such

a complex information security management structure can be expressed as in Figure 3.

Fig. 3. Information security management *(compiled by the authors based on the analysis and systematization of scientific literature)*

Security Operations Center Business Model. A review of the role of the security operations center in nearly 20 operational security processes shows that there is no standard management model for it [13]. However, the work of Steph Shingle and his team reflects the functions of the security operations center such as Intelligence, Basic Security, Monitoring, PenTesting, and Digital Forensics (Figure 4).

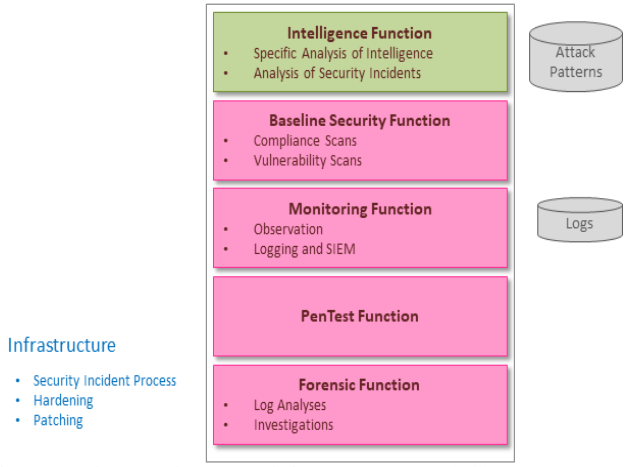

Fig. 4. Security operations center infrastructure *(compiled by the authors based on the analysis and systematization of scientific literature)*

V. Architectural-Technological Model of the Information Infrastructure Security System of New Generation Enterprises

The architectural-technological model of the information infrastructure security system of new generation enterprises is being developed to protect the digital resources of the enterprise and ensure information security and resilience against cyber attacks. The architectural-technological model of enterprises can be proposed as in Figure 5.

Such a model has a multi-level and complex structure and has the property of covering both architectural and technological components. It can be attributed to general methods of information security in new generation enterprises [1, 14]:

1)improvement of legislation regulating relations in the field of information security;

2)determination of responsibility for unauthorized access of users;

3)strengthening the legislative level of the priority of the development of national networks;

4)creation, improvement, and management of an information security assurance system;

5)improvement, use and development of methods of monitoring the effectiveness of information protection tools;

6)training of personnel in the field of information security assurance;

7)formation of a monitoring system for information security indicators;

8) regulation of information security assurance and its financing;

9) economic justification of security systems;

10) assessment of security-related damages, etc.

In the architecture of the information security management model, risk identification and feature discovery are key relationships operating through the data and processing layers [1].

They use data sources such as system logs, network traffic logs, user behavior, and external threat intelligence to support subsequent security management and threat detection through data integration, and smart analysis.

1)System logs use log data generated by operating systems, applications, databases, etc. to monitor and analyze system activities in real-time, identify potential anomalous behaviors, and identify security vulnerabilities. System logs can provide early signs of attack behaviors such as illegal login attempts, unauthorized access, etc.

2)Network traffic logs analyze incoming and outgoing data packets through real-time monitoring of network traffic. Special attention is paid to abnormal traffic and data transfer patterns, identifying potential DDoS attacks, network scanning, and other malicious activities. Traffic logs help detect network-level security threats through feature analysis and behavior recognition.

3)User behavior data such as user login activities, access permission changes, and file operation logs are used to analyze account anomalies. This information helps to determine whether users are abusing permissions, abnormal logins, and other behaviors, and to identify potential internal threats through behavioral analysis models.

4)External threat intelligence information provides information on the latest security vulnerabilities, malicious attack activities, and their patterns, and helps detect cross-domain threats.

The architectural-technological structural model of the security of the information infrastructure of new-generation enterprises can effectively respond to its information security threats as a result of the application of digital technologies, including Artificial Intelligence, Big Data, etc. to increase the efficiency and effectiveness of enterprise information security management.

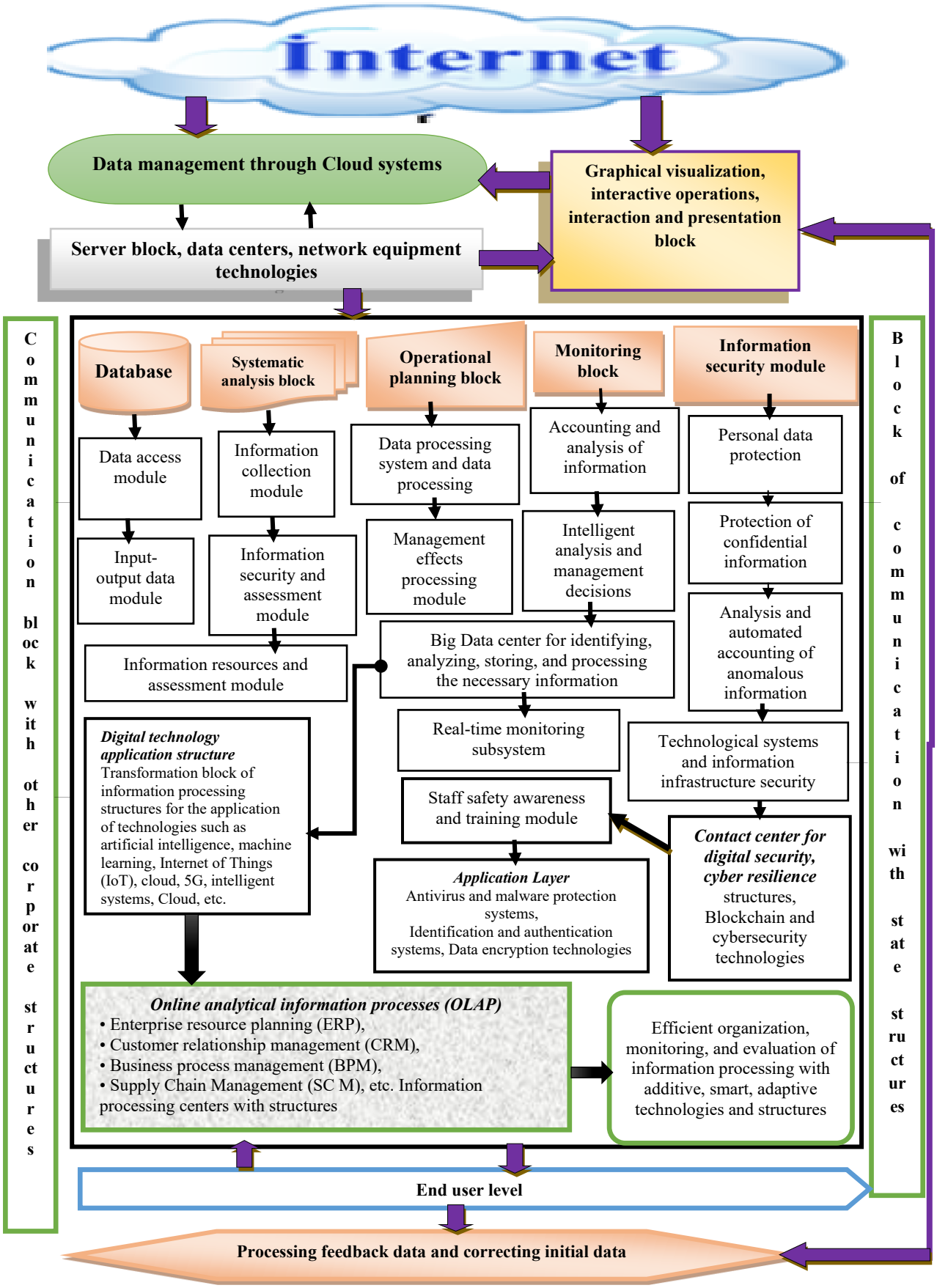

Fig 5. Architectural-technological structural model of the information infrastructure security system of new generation enterprises *(compiled by the authors)*

The interaction of the conceptual coordination blocks of the structural model proposed in the article and taking into account the considered cases can have a positive impact on the effective management of new generation enterprises operating in the conditions of digital network transformations, ensuring the security of their information infrastructure, increasing cyber resilience, and increasing the efficiency of decision-making processes. Since such a model has an open system nature, it reflects the progressive technological changes proposed in state programs, digital development strategies, and perspective concepts, and creates conditions for the inclusion of other structural components in the model.

VI. Conclusion

Ensuring the development of the economy based on digital technologies at the international and national levels, as well as the formation of high-tech sectors, are considered to be the main goals of states. Ensuring the security of the information infrastructure of new generation enterprises requires a comprehensive approach that combines numerous technological and organizational measures. This can be achieved not only by technological measures but also by implementing the human factor, security culture, and regular testing and audits. The correct implementation of these measures will help protect the enterprise's data from security risks.

Although new generation enterprises create more flexible and efficient work environments, they need more complex and comprehensive strategies to combat modern security threats. Ensuring the security of these enterprises, created thanks to technological innovations and digital transformation, can be achieved not only by technical means but also by the culture of the organization, employee education, and compliance with legislative requirements. This is of great importance in terms of protecting the data of both the enterprises themselves and their customers and partners.

New generation enterprises have innovative business models based on digitalization. They produce high-tech products and widely used technologies such as cloud technologies, artificial intelligence, big data (Big Data), and IoT (Internet of Things).

These enterprises require Cloud systems and remote work modes, data management from different locations. The increase in cyber threats, New generation enterprises use digital solutions in supply chain processes, which increases dependence on third parties.

To ensure the security of information infrastructure, technological solutions, Network security, Cloud security, Antivirus for protecting remote devices, and Endpoint Detection and Response solutions should be applied in a comprehensive approach. Management strategies, Risk assessment, and a plan that ensures the continuity of the enterprise in the event of an attack (Disaster Recovery Plan) should be prepared. Employee awareness about cybersecurity should be increased. Legal and regulatory compliance should meet the security requirements set by regulatory bodies.

Digital technologies such as Artificial Intelligence and Automation should be integrated into enterprises, Machine Learning models should identify anomalies and prevent threats at an early stage, and security against data integration and modification should be ensured. Special encryption protocols and certification procedures should be applied for the security of cyber-physical systems and IoT devices.

In the era of increasing cybercrime in the world, the situation of the growth in the field of cyberattacks should be analyzed and appropriate proposals and recommendations should be given to it. Proposals and recommendations should be developed in accordance with the experience of advanced countries in intellectual cybersecurity technologies.

Improving the activities of new generation enterprises, and ensuring the sustainability of their information security with modern technologies will create additional opportunities for increasing the efficiency of its economy and its future development in the conditions of economic management of the country. Fulfilling the issues of ensuring the security of the information infrastructure of new generation enterprises can be characterized as scientific support for management decisions in increasing economic cyber resilience, economic diversification issues, investments in real economic sectors, and ensuring regional technological sovereignty.

References

[1] Ping Li, Limin Zhang. Application of Big Data technology in enterprise information security management. Scientific Reports, 2025, 15:1022. https://doi.org/10.1038/s41598-025-85403-6.

[2] Sunyaev A. et al. The Future of Enterprise Information Systems, Bus. Inf. Syst. Eng., 2023, 65(6), pp.731–751.

[3] Aliyev A.G., Shahverdieva R.O. et al. Issues of development of the information support system of innovative enterprises based on modern digital platforms. Information Technologies, 2023, No.7, vol.29, pp.374-381.

[4] Gebremeskel B.K. et al. Information security challenges during digital transformation. Procedia Comput. Sci. 2023, 219, pp.44–51.

[5] Wu G., Wang J. Enterprise Information Security in the Process of Informatization. In: Huang, C., Chan, YW., Yen, N. (eds) Data Processing Techniques and Applications for Cyber-Physical Systems (DPTA-2019). Advances in Intelligent Systems and Computing, 2020, vol 1088.https://doi.org/10.1007/978-981-15-1468-5_89.

[6] James Pooley. Chapter. Information Security in the Modern Enterprise. Computer and Information Security Handbook (Fourth Edition), 2025, pp.3-11.

[7] Stanchev Plamen, Tomov Yavor et al. Problems and Solution in Ensuring Cybersecurity of IoT Devices for the Needs of Small and Medium Enterprises. 12th International Scientific Conference on Computer Science (COMSCI-2024). DOI 10.1109/COMSCI63166.2024.10778507

[8] Chen H., Liu Y. Evaluating the effectiveness of endpoint security solutions: A comparative study. Journal of Computer Security, 2023, 20(2), pp.145-158.

[9] Crowley Chris. SANS Institute: Common and Best Practices for Security Operations Centers: Results of the2019 SOC Survey, 2019. https://www.sans.org/media/analyst-program/common-practices-security-operations-centers-results-2019-soc-survey-39060.pdf.

[10] McCarthy J., Allan S. Cybersecurity Operations Handbook. Wiley, 2022. https://ifst.onlinelibrary.wiley.com/doi/epdf/10.1002/fsat.3602_11.x,

[11] Jones R., Kim S. Integration of Machine Learning Algorithms in Security Systems: A Review of Recent Advances. IEEE Security & Privacy, 2019, 17(3), pp.29-38.

[12] Bejtlich R. Network Security Monitoring: Detection and Analysis Using Zeek, Wireshark, and More. No Starch Press. 2023.

[13] Chen L., Wang Y. The Role of Security Operations Centers (SOCs) in cyber threat intelligence sharing: A case study of large enterprises. Journal of Information Security, 2022, 11(2), pp.85-97.

[14] Aliyev A.G., Shahverdiyeva R.O. Organizational problems of innovation activities and their solution mechanisms. Monograph, Baku, "Information Technologies", 2023, 532 p.