INFORMATION SECURITY MANAGEMENT IN DIGITAL BUSINESS ENVIRONMENTS

Rasulov Sherzod Sharof ugli
Lecturer, Jizzakh Polytechnic Institute
Toxirov Shoxrux Odiljon ugli
Student, Jizzakh Polytechnic Institute
https://doi.org/10.5281/zenodo.16891981

Abstract: This article explores the principles and practices of managing information security in digital business environments. As companies increasingly rely on digital platforms for operations, communications, and transactions, the risks associated with cyber threats, data breaches, and unauthorized access have significantly grown. The study examines strategic approaches to information security management, including risk assessment, policy development, incident response, and the integration of advanced technologies. It also highlights the importance of compliance with international standards and legal requirements to ensure data confidentiality, integrity, and availability in digital business operations.

Keywords: information security, digital business, cybersecurity, risk management, data protection, incident response, international standards, compliance.

Аннотация: В данной статье рассматриваются принципы и практические аспекты управления информационной безопасностью в условиях цифровой бизнес-среды. По мере того как компании всё больше полагаются на цифровые платформы для ведения операций, коммуникаций и проведения транзакций, значительно возрастают риски, связанные с киберугрозами, утечками данных и несанкционированным доступом. В исследовании анализируются стратегические подходы к управлению информационной безопасностью, включая оценку рисков, разработку политик, реагирование на инциденты и интеграцию передовых технологий. Также подчеркивается важность соблюдения международных стандартов и законодательных требований для обеспечения конфиденциальности, целостности и доступности данных в цифровой бизнес-деятельности.

Ключевые слова: информационная безопасность, цифровой бизнес, кибербезопасность, управление рисками, защита данных, реагирование на инциденты, международные стандарты, соблюдение требований.

Currently, a digital economy is being formed, based on the development and implementation of modern digital technologies in the activities of the population

and organizations. The improvement of big data analysis, the widespread use of mobile devices, and the development of the Internet are undoubtedly innovative elements designed to solve socio-economic problems, both at the level of individual regions and countries, and at the global level. The acceleration and complication of the processes taking place in the modern conditions of the development of digital technologies makes economic entities think about information security. Theft of personal data of citizens and organizations leads not only to material damage, but also manifests itself in damage to reputation.

Loss of trust is an extremely undesirable result of activity, therefore, information security issues require solutions both at the state level and at the level of individual organizations. Cyber-attacks can be global: in May 2017, computers in more than 150 countries were infected with the WannaCry virus, disrupting the activities of the UK National Health Service (NHS), the Spanish telecommunications company Telefónica, the American logistics company FedEx, Germany's largest rail operator Deutsche Bahn and many other organizations around the world; car concerns Nissan Motor and Renault have temporarily suspended production at several production sites[1].

Concerns about the consequences of losing personal information are related to the existence of data theft cases, directly or indirectly related to digital technologies. A significant part of the incidents is related to the violation of the privacy policy, integrity and availability of information that underlies socio-economic activity in the digital environment. Over time, these violations become more widespread, frequent and complex in terms of eliminating their consequences. Information security breaches also occur due to fraudulent activities of organizations to which users have provided personal information.

The growth in the number of information security violations in the context of the digitalization of the economy is associated with the constant complication and growth of the use of digital technologies. In recent years, both large and small organizations have faced more frequent and more serious information attacks on their businesses. Digital technologies used in the organization are gradually becoming the main value of the company, so cases of industrial espionage for political or economic purposes are not rare[2].

Assessing the economic consequences of information attacks is very difficult; some organizations try not to report information security breaches if it is not related to the legal consequences of theft of trade secrets. We can say that data loss leads to many negative results: undermining business reputation,

[1] Digital Economy Outlook. OECD. 2017.
[2] Klahr R., Amili S., Shah J.N., Button M., Wang V. Cyber Security Breaches Survey. 2016.

reduced competitiveness, financial losses in the event of fraud, disruption of production plans, deliveries, as well as increased costs due to the need to recover lost information.

In modern conditions of the digital economy, every organization must regularly assess the level of its information security, answering a number of questions and improve the level of information security. Increasing the information security of organizations can be ensured through a multi-stage analysis of emerging threats

Stage 1: Initiation of analysis. At this stage, based on the analysis of emerging information threats, the need is determined to revise the organization's methods of ensuring the safety of data. As a rule, partial implementation of existing measures to protect information is detected, and the development of internal standards of the organization for optimal data protection is required.

Stage 2: Process management. Information security is divided into separate processes; responsibility for each of them is distributed.

Stage 3: Implementation and control. The process of ensuring information security is integrated into the business model, is consistent with the development strategy of the organization, control over the implementation of the measures taken is carried out, and the effectiveness of innovations is assessed.

Stage 4: Forecasting. Determination of the need to adjust the measures taken to ensure information security, further implementation of digital technologies in order to more fully cover possible threats.

Stage 5: Optimization. The information security system is being continuously improved; data protection becomes a fully automated process, integrated into all areas of an organization's activities.

In the context of the formation of the digital economy, information protection issues should be considered not only at the level of individual organizations, but also at the state level. Initially, it is necessary at the state level to form a group of experts who, through intersectoral cooperation, will develop an information security policy. The result of the work should be an information security strategy with clear goals, objectives and an action plan for its effective implementation; the developed strategy should take into account various specific aspects of the economic sectors. The state strategy should also include provisions on assessing risks in the field of information security in order to optimally respond to their occurrence in various areas. Moreover, the critical

information infrastructure, on which the national security of the state depends, should become a separate element of the strategy.

The next step is to improve the regulatory framework for information security, as well as develop new legal norms for certain cases of fraud that are not covered by existing laws. This stage of ensuring information security should become a continuous process of updating the regulatory framework, since every day there are threats to the safety of data that have not previously been encountered by society, or they have not manifested themselves on such a large scale.

Based on the adopted strategy and updated regulatory framework in the field of information security, we can say that it is necessary to develop and approve industry standards for information security. It is also important to establish reliable data collection on data breach cases. Moreover, education policy is also associated with ensuring information security: in the modern conditions of the development of digital technologies, the amount of collected and analyzed information is constantly increasing, which creates new threats that require special professional skills to combat. Consequently, the development of the country's human resources is an important element in maintaining information security at all levels of the economy.

Thus, the digital transformation carried out in many sectors of the economy has led to the fact that the scale of the activities of economic entities has changed and new risks and threats have appeared, which the world has not faced before. The formation of the digital economy largely depends on ensuring information security: the emergence of threats to the safety of digital data is becoming one of the main areas of security, both at the state level and at the level of individual organizations and citizens.

At present, attacks on data storage systems are becoming more and more complex and frequent, therefore, information security issues should be a priority in maintaining the stability of the economy.

References:

1.ISO/IEC 27001:2022 - Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements. International Organization for Standardization, 2022.

2.von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

3.Whitman, M.E., & Mattord, H.J. (2022). Principles of Information Security (7th ed.). Cengage Learning.