Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021: 4887- 4894

Research Article

# Issues Of Ensuring Information Security In The Digital Economy

Abdumalik A. Ruziev

## Abstract

In the current conditions of the development of the digital economy, information security remains one of the most pressing problems at the global, state, economic and individual levels. The rapid penetration of digital technologies into all socio-economic spheres is an undeniable process that will exacerbate this problem. As a result, new types and methods of threats to information security appear. The article analyzes the main global trends in information security and considers ways to protect digital information. The information security of the Republic of Uzbekistan is analyzed. Suggestions and conclusions are made on information security both at the state level and at the level of individual economic entities.

## 1 Introduction

In the process of globalization and integration, the digital economy is being formed based on the development and introduction of advanced digital technologies in all socio-economic spheres. Improving big data analysis, the widespread use of mobile devices, the development of the Internet, and the advent of the Internet of things are, of course, innovative elements designed to address socio-economic problems at the regional and global levels [1]. Simultaneously, the acceleration and complexity of the processes taking place in the current context of the development of these technologies raise the issue of information security for economic entities. The theft of personal data of citizens and organizations is manifested in material damage and serious damage to their position in society and business reputation. It should be noted that cybersecurity threats are growing with the development of information and communication technologies. Cybersecurity is recognized as one of the major challenges on a global scale.

Currently, the following types of information security threats are distinguished in world practice:

1. An Incident (IT Incident) – is an event that goes beyond the normal operation of an IT structure, directly, indirectly or potentially, causing system processes to stop and adversely affecting the quality of its performance.
2. A deface – is a hacker attack that unauthorizedly manipulates the content of a page on a website, often turning it into a page that attracts advertisements, threats, or warnings. Besides, attackers can block access to the rest of the site or completely delete the previous content of the

[*1]Candidate of Economic Sciences, Associate Professor, Department of Electronic Commerce and Digital Economy, Tashkent Financial Institute, Tashkent, Uzbekistan. Email: aoruziyev@google.com_ Orcid: 0000000171817200

resource. Some do this to attract attention or to show the server administrator that there are security vulnerabilities.

3. Hidden miner (stealth miner, miner bot, botnet) – is a program that automatically performs mining without the user's knowledge. It is external software installed on a computer, uses its resources, and transfers all the money earned to the developer's wallet.

## 2 Material and Methods

In the 21st century, when information is used as an economic resource in world practice, the protection issue of economic information has always been recognized as one of the major global problems and is an ongoing process. Experience with existing information and computer systems shows that the information security problem has not been fully resolved. Various manufacturers provide the system of protection tools in terms of problems and methods used, and the results achieved differs significantly from each other. The novelty of this approach as economic security raises several issues related to the study and research of methodological aspects of information security assessment in the world economy [10]. Therefore, it is necessary to take appropriate measures in the field of information security at the level of the state, a separate organization. Today, cyber-attacks or crimes are also global problems: in May 2017, computers in more than 150 countries were infected with the WannaCry virus, resulting in the UK's National Health Service (NHS), Spain's Telefonica, Germany's largest Deutsche Bahn. Disrupted the activities of the railway operator, the American logistics company FedEx, and many other organizations around the world [8]; Nissan Motor and Renault have suspended production at several production sites [12]. Creating a secure information environment in the context of digital interdependence between different economic entities will become an integral part of building a sustainable digital economy [7]. From the point of view of information security, many digital technologies include data, the Internet, and artificial intelligence technologies that are difficult to manage. Today, companies such as Amazon, Apple, and Google have created digital platforms using artificial intelligence. Facebook has launched DeepTex technology, which can recognize the behavior of users through messages [4,3]. The potential benefits of these digital technologies are undoubtedly significant, but their introduction poses a threat to the security of the population's personal data, and even a small amount of data leakage undermines confidence in innovation and the economy as a whole [2]. In the context of the digitalization of the economy, the growing number of threats to information security is associated with the constant complication and improvement of digital technologies. In recent years, as in large organizations, there have been frequent and severe information attacks on the business activities of small organizations. Data loss can have many negative consequences: damage to business reputation in the event of fraud, loss of competitiveness, financial losses, and disruption of production and delivery plans due to the need to recover lost data and increased costs. The study examined and analyzed the impact of information and cybersecurity for economic entities operating based on information and communication technologies, the work of foreign and domestic scientists in this area. The article effectively uses methods such as theoretical observation, systematic approach, observation, generalization, analysis, synthesis, and conclusions and recommendations on the problems of information and cybersecurity of real sector enterprises and their solutions.

## 3 Results and Discussion

In the current context of the digital economy, every organization needs to regularly assess the level of information security it has by addressing the following questions [11]:

1. How effectively are financial resources for information security distributed between the organization's staffing and digital technology? Hiring a new employee without raising awareness of existing digital technologies is a less effective way to increase an organization's information security. Digital technologies are also constantly evolving, and it is essential to take advantage of all the opportunities offered by modern means of data protection to remain competitive in the market.

2. Is the importance of information security measures properly assessed? Determining the level of information security of data helps to assess the contribution of various information security tools optimally.

3. Is the organization created conditions to introduce modern digital technologies in the information security system? In order to use new technology effectively, it is necessary to plan and create conditions for its practical use, which reduces the number of failures and errors and reduces the cost of setting up the technology.

4. How rational is information security in a service or work chain? As the organization interacts with many information-sharing partners, it will be necessary to analyze the security of data transmission to foreign economic entities [5].

5. Can the organization's management effectively deal with information security issues? Since the success of security measures depends largely on the coordination of employees' actions, the organization's management is an important element in the formation of information security.

We believe that improving the organization's level of information security can be achieved through a multi-stage analysis of emerging threats:

**Step 1:** Perform the analysis. At this stage, the analysis of emerging information threats identifies the need to review the organization's data security practices. As a rule, existing measures of partial information protection are identified, and the organization's internal standards for optimal data protection are required.

**Step 2:** Process management. Information security is divided into separate processes, each of which is responsible.

**Step 3:** Implementation and control. Ensuring information security integrated into the business model will be adapted to the organization's development strategy. The implementation of measures will be monitored, and the effectiveness of innovations will be evaluated.

**Step 4:** Forecasting. There is a need to review the measures taken to ensure information security and introduce advanced digital technologies to address potential threats better.

**Step 5:** Optimization. The information security system is constantly being improved; data protection becomes a fully automated process integrated into all areas of the organization's activities. In the context of the digital economy, information security is an issue that needs to be addressed not only at the individual level but also at the state level.

Currently, Uzbekistan pays special attention to the tasks and problems of cybersecurity at the state level and takes strict measures to identify threats, vulnerabilities, and incidents in cyberspace. In particular, in accordance with the Decree of the President of the Republic of Uzbekistan dated November 21, 2018, No. PP-4024, the "State Inspectorate for Control in the field of informatization and telecommunications", was established. In 2018, there were about 65,000 domains in the national domain zone "UZ" in 2019 - 73,674 domains, and as of October

2020, 83,925 domains were active. However, it should be noted that the more actively the global network is used, the greater the number and sources of threats. In 2019, 268 cybersecurity incidents were detected on the websites of the national segment of the Internet (diagram 1), of which 222 were related to unauthorized content download (RKYuO), 45 were defaced, and one was hidden by mining. In particular, 27 of the identified incidents occurred on government websites.

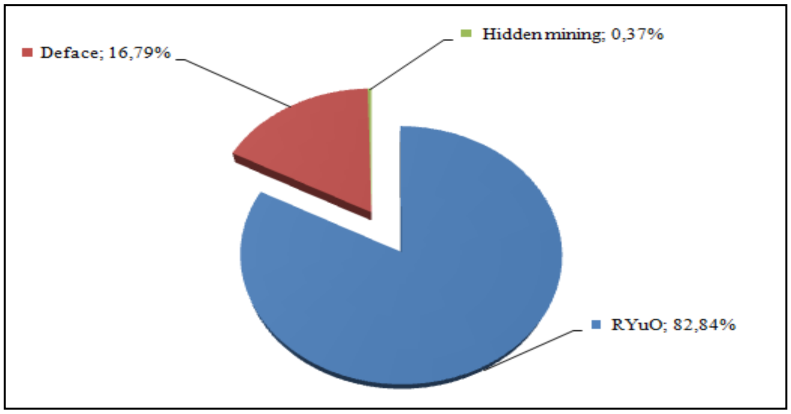

**Fig. 1. In 2019, a total of 268 incidents were detected in Uzbekistan**[†]

A comparative analysis of the number of incidents from 2017 to 2019 shows a positive trend resulting from the effective implementation of cybersecurity measures in Uzbekistan. The number of incidents in 2019 decreased by 61% compared to 2017 and 44% compared to 2018 Diagram 2). The comparative chart shows that the threat of unauthorized download of content is still relevant, but it should be noted that in 2019, for the first time in cybersecurity in Uzbekistan, a new threat appeared - the hidden mine.

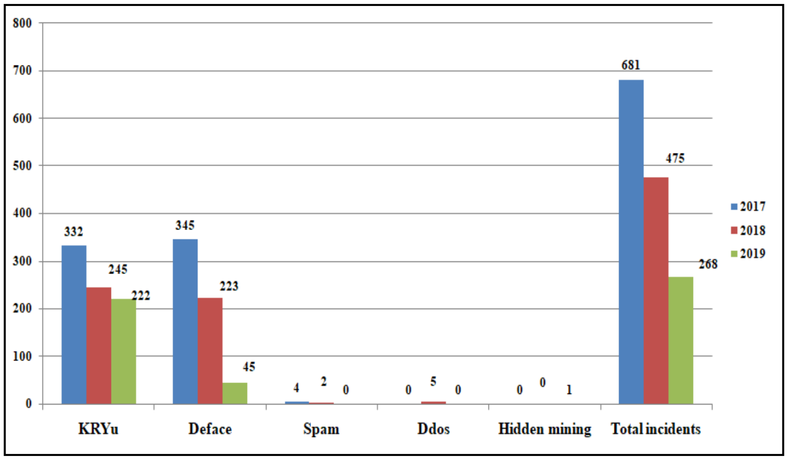

**Fig. 2. Comparative analysis of the number of incidents in 2017-2019**

Simultaneously, the analysis of incidents in the public sector during this period showed a decrease of 62.5% compared to 2017, but more than two times more than in 2018, including a negative increase in threats to KRYu and defies. However, Spam and DDoS attacks were eliminated (Diagram 3).

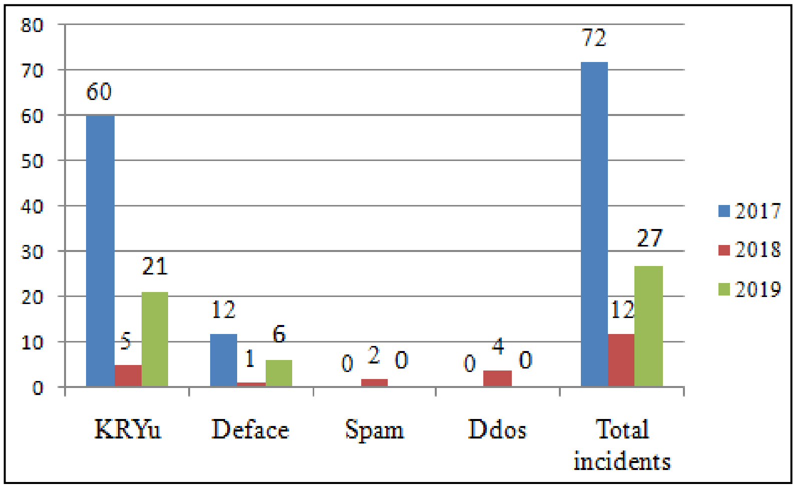

**Fig. 3. Dynamics of organized threats to the public sector in 2017-2018**

The highest number of cyber security incidents was detected in the Word Press CMS, the most popular web developer in Uzbekistan, and this figure remains high. Comparison of the identified events in 2017-2018 revealed deficiencies in the content management systems Magento, Drupal and 1C-Bitrix (Diagram 4).

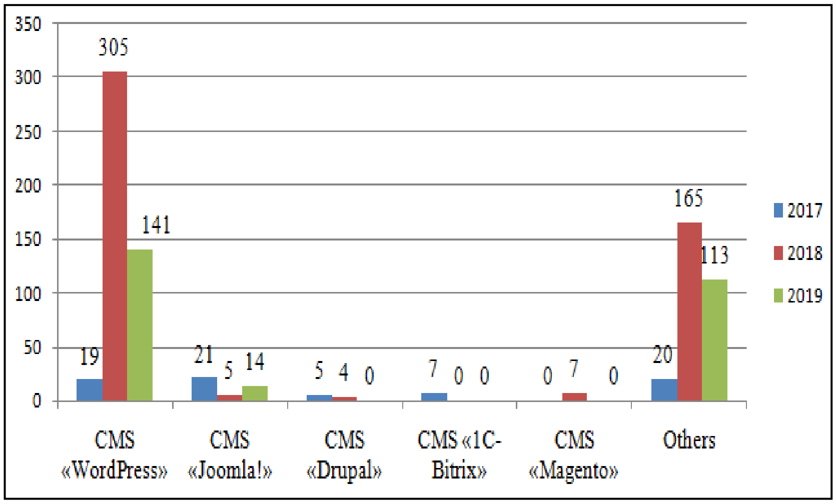

**Fig. 4. Dynamics of incidents in the field of content management systems in Uzbekistan**

69% of the incidents (down 6% compared to 2018) were detected on websites hosted by hosting providers in Uzbekistan, and the remaining 31% were detected on hosting in foreign countries (Diagram 5).

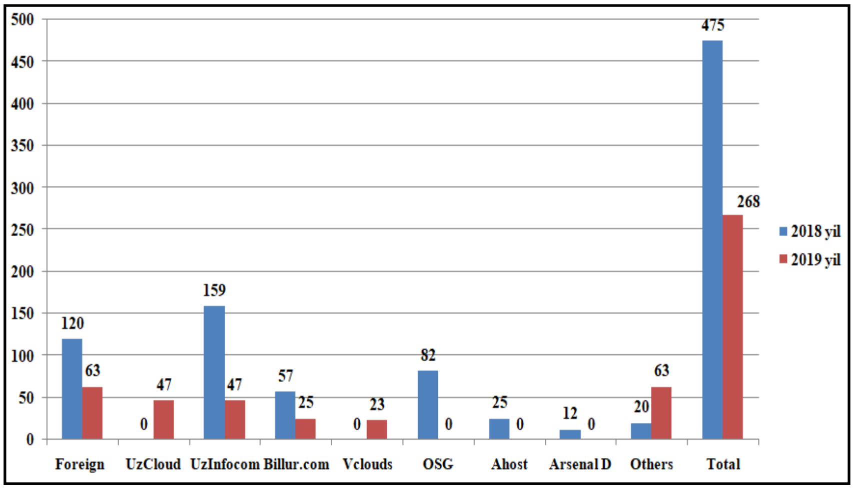

**Fig. 5. Dynamics of Web site incidents in Uzbekistan in terms of hosting**

A study of the various threats in the country's cyberspace in 2017-2019 shows that in most cases, incidents are detected in the following cases:

- outdated versions of the content management system (CMS) and errors in the security code as a result of their additions;

- simplicity of passwords;

- templates and extensions downloaded from unsafe sources;

- viruses on the computers on which the website is managed/configured;

- not available or lack of protection on the website;

- consumers use authentication;

- password recovery ("brute force" attack)

- connection of information systems to the external Internet;

- use of VPN-service;

- system malware;

- targeted attacks similar to SQL injection;

- use of MBBT software and data without authentication mechanism, as well as expired or invalid SSL certificates;

- use of RDP (Remote Desktop Protocol) protocol with weak protection system;

- hosts that are members of botnet networks;

- use of ports that can lead to the download of third-party content due to the lack of TFTP-Protocol (Trivial File Transfer Protocol) and associated authentication mechanisms.

## 4 Conclusion

In the process of digital transformation in many sectors of the economy, the expansion of the activities of economic entities leads to the emergence of entirely new types of risks and threats in the field of cybersecurity, economic security and information security. World practice shows that the proper formation and effectiveness of the digital economy largely depends on information security. The emergence of threats to digital data security is becoming one of the main security areas at the level of all - the state, individual organizations and citizens. Today, as attacks on data storage systems become more complex and common, the country's economic stability and Information security should prioritize competitiveness. Given the above, we believe that the following organizational and technical measures will be taken to prevent and eliminate internal and external threats to cyberspace and information systems to eliminate and protect information security threats to the websites and corporate networks of economic network organizations:

- constantly update the content management system (CMS);

- backup.

The essence of backing up a site is to copy the database, site files, mail, FTP accounts and many other hosting settings. Backups can be done using the tools installed on the CMS site, a special plugin, tools provided by the hosting provider, or any other convenient method;

- delete unused plugins. Any new plugin or extension increases the likelihood of an external attack. In this regard, it is recommended to disable and remove unused plugins and, if possible, to use built-in mechanisms instead of installing plugins for each case;

- strengthening password authentication. It is strongly recommended to use a complex password that is not repeated on other services and sites for the administrative account in the CMS, the personal account on the service provider's website and the server account;

- safe administration. It is recommended to access the administrator's account in the CMS, personal account on the service provider's website and server account from devices (computers, tablets) with updated antivirus software;

- security plugins. It is recommended to use security plugins that have the functions of searching for, removing, and protecting against malware in the future to protect your website from various attacks;

- examining a website. Regularly explore the website for compliance with information security requirements and vulnerabilities;

- installation of necessary software and hardware to eliminate internal threats to information security, as well as information security tools;

- ensuring information security and improving the skills of users (employees) working with information and communication technologies and direct information systems;

- not to use information systems that interact with other information systems through the global Internet within the inter-branch data transmission network.

Adopting the above and other additional protection measures will significantly reduce the risk of information security threats on the websites, information systems, and resources of organizations in the future, which will protect against potential attacks and eliminate the causes and consequences of subsequent information security incidents.

## List of references

1. I. Gartner. Information Security, **12** (2018)
2. T. Ablyazov, V. Asaul. New industrial base formation, **23** (2018)
3. D. Guillaume. Currency of the digital age, **45** (2016)
4. Digital Economy Outlook. OECD. 2017.
5. M. Harrey. Privacy risk, **10** (2013)
6. R. Matniyazov, U. Asraev, A. Ruziev. Psychology and education **58** (2021)
7. R. C. Mayer, J. H. Davis, F. D. Schoorman. The Academy of Management Review, **20** (1995). Vol. 20. № 3. P. 709-734.
8. NHS cyber-attack: GPs and hospitals hit by ransomware. [Elektron resurs]. [Electronic resource]. : www.bbc.com/news/health-39899646 (access date 03.10.2020).
9. A. O. Ruziev, R. R. Matniyazov, U. M. Asraev. Journal of Critical Reviews, **2 (**2020)
10. S. Culp. Cybercrime: A Major Threat To Trust In The Digital Economy, **10** (2020)
11. S. Moor. The State of Cybersecurity and Digital Trust, **11** (2020)
12. J. Sharman. Cyber-attack, **34** (2020)