

THE RELEVANCE OF CYBER SECURITY IN GOVERNMENT AGENCIES

<https://doi.org/10.5281/zenodo.17297638>

Komilov Mehridin Malikovich

Bukhara State Pedagogical Institute

Faculty of military education

Stage 2 Cadet

Niyazov Erkin Shamsievich

Associate professor of special training period, Faculty of military education

Annotation: *The modern development of information technologies is ahead of the technology to ensure their security. Distortion or falsification, destruction or disclosure of certain information causes serious material and moral damage to many entities involved in the processes of automated information interaction. Cybersecurity is to strengthen and prevent the organization of work.*

Key words: *information, security, vishing, cybercrime, information technology.*

Relevance of the study: The relevance of this topic is determined by a number of reasons. First of all, the information society is characterized by a high level of development of information and telecommunication technologies and their intensive use by citizens, businesses and government authorities. Secondly, international experience shows that high technologies, including information and telecommunications, have already become the engine of socio-economic development in many countries of the world, and ensuring guaranteed free access of citizens to information is one of the most important tasks of States. Thirdly, the dynamics of information infrastructure and high technology development in Uzbekistan does not allow us to expect significant changes in the near future without joint targeted efforts by government authorities, business and civil society. It is necessary to realize the country's existing cultural, educational and scientific and technological potential in the medium term and ensure Uzbekistan 's worthy place among the leaders of the global information society.

Аннотация: *Современное развитие информационных технологий опережает технологии обеспечения их безопасности. Искажение или фальсификация, уничтожение или разглашение определенной информации наносит серьезный материальный и моральный урон многим субъектам, участвующим в процессах автоматизированного информационного*

взаимодействия. Кибербезопасность заключается в укреплении и предотвращении организации работы.

Ключевые слова: информация, безопасность, вишинг, киберпреступления, информационные технологии.

Актуальность исследования: Актуальность данной темы определяется рядом причин. Во-первых, информационное общество характеризуется высоким уровнем развития информационных и телекоммуникационных технологий и их интенсивным использованием гражданами, бизнесом и органами государственной власти. Во-вторых, международный опыт показывает, что высокие технологии, в том числе информационные и телекоммуникационные, уже стали локомотивом социально-экономического развития многих стран мира, а обеспечение гарантированного свободного доступа граждан к информации – одной из важнейших задач государств. В-третьих, динамика показателей развития информационной инфраструктуры и высоких технологий в Узбекистана не позволяет рассчитывать на существенные изменения в ближайшем будущем без совместных целенаправленных усилий органов государственной власти, бизнеса и гражданского общества. Необходимо уже в среднесрочной перспективе реализовать имеющийся культурный, образовательный и наукотехнологический потенциал страны и обеспечить Узбекистана достойное место среди лидеров глобального информационного общества.

INTRODUCTION

The issue of effective information security management is relevant for the modern information society. Knowledge and application of rules, standards, and approaches to information security are factors for the successful development of the information society in Uzbekistan, which should be conducted at the state level. Currently, information security is an essential component of national security. Its importance is increasing every day in all spheres of public life, including the economic one. Obviously, in the information society, information is both a subject of mass consumption and a powerful economic resource. The creation of an ideal information security system depends, first of all, on who and how it will be managed. In his greeting to the participants and organizers of the Information Society socio-economic forum, the President noted that the 21st century is rightfully called the century of information. And today it is extremely important to improve the communication infrastructure, more actively overcome the "digital inequality" of the regions, and switch to the most modern standards and technologies.

There are already concerns that the main constraining factors for the introduction of information security in the field of economics and.

The uneven development of the information sphere is becoming a problem for business. Therefore, one of the most important tasks and problems of the information society development in Uzbekistan remains improving the effectiveness of information security management.

Discussion and results

Today, the information society has all the necessary information resources, methods, technologies and means to meet both individual and public knowledge needs, to improve the intellectual, socio-economic, humanitarian and spiritual condition of man and society as a whole. There is a basic functional model of the information society – new management (business organization and widespread use of innovations and information technologies in management); new economy (primarily high-tech, innovative and digital); new information technologies; new systems of social relations (the system of "electronic social partnership" and the system of "electronic democracy", new forms of social movements with an integrating basis based on the Internet); new ethics (it is based on a person, respect for his life and dignity, his interests above the interests of the state, society and science).

Cybersecurity is a broad concept encompassing technologies, processes, and policies that help prevent and/or reduce the negative impact of events in cyberspace that may occur as a result of deliberate actions against information technology by a hostile or malicious actor. This includes physical security as well as cybersecurity, such as protection from internal threats. This entails all levels of the Internet and all the numerous actors involved in the provision and use of the network, from those who control and create this infrastructure to a variety of end users.

Given this broad definition, we need to answer the question of who is responsible for cybersecurity? Although responsibility most often depends on the specific activity and context. In particular, the worldwide adoption of the Internet has allowed end users not only to access information from all over the world, but also to create and otherwise receive their own information for the whole world.

In many ways, this has empowered users, as evidenced by the numerous ways in which users can challenge influencers such as the press with compensating information. However, this also means that responsibility for the security of information resources on the Internet has shifted to users around the world and the institutions they participate in, not just to technical experts involved in

cybersecurity. This does not mean that end users should be responsible for their own online security, but they are increasingly expected to share some shared responsibility with other participants.

During the monitoring of the national segment of the Internet, exposure to 132,003 cybersecurity threats was revealed. Threat research has shown that:

- 106,508 cases relate to hosts that have become participants in botnet networks;

- 13,882 is related to the blocking of IP addresses blacklisted by various services due to sending spam emails or brute-forcing passwords;

- 8,457 is associated with the use of the TFTP protocol (Trivial File Transfer Protocol) and related ports, the use of which may lead to downloading extraneous content due to the lack of authentication mechanisms;

- 2114 refers to the use of the vulnerable RDP protocol (Remote Desktop Protocol);

- 1,042 cases related to the use of software and a database that does not have an authentication mechanism.

Uzbekistan is no exception, and in 2021 alone, numerous projects were implemented to widely introduce information and communication technologies into the fields of government and economic management, local government and other organizations. All information and communication technologies and equipment used in Uzbekistan and the world collectively constitute cyberspace. This development also has a downside – cybercrime, which gives attackers new and sophisticated ways to extort funds and use cyberspace for malicious purposes. A comparative analysis of the number of incidents in 2018 and 2019 showed a positive trend, namely a 44% decrease in the number of incidents. In 2019, 268 incidents were identified in information systems and websites of the national segment of the Internet (of which 222 relate to unauthorized downloading of content, 45 to the destruction or modification of the content of the site and 1 to hidden mining. Of the total number of identified incidents, 27 were on government websites), 816 vulnerabilities and about 132,000 information security threats.

During the examination (audit) of information systems and websites for compliance with information security requirements, 816 vulnerabilities with various levels of criticality were identified. Using these vulnerabilities will allow an attacker to gain remote access to an information system or website, as well as to files and information, which in turn may lead to the leakage of personal data of 2,026,824 citizens of the Republic of Uzbekistan.

In 2020, according to the results of monitoring cybersecurity incidents committed against websites of the UZ domain zone, 342 incidents were recorded, of which 306 relate to unauthorized downloading of content, the remaining 36 are related to unauthorized modification of the main page.

At the same time, when monitoring information systems, the Cybersecurity Center specialists presented an overview of “Cybersecurity of the Republic of Uzbekistan. Results of 2021” by government agencies, in which 17,097,478 events were identified. As of 2021, 100,015 domains of the national segment of the Internet “.uz” have been registered in Uzbekistan, of which about 38,000 are active. Of the 38,000 active domains, only 14,014 are secure, i.e. they have an SSL security certificate. In all other cases, either the certificate is expired (613 cases), or it is missing. In 2021, the Center identified 17,097,478 cases of malicious and suspicious network activity originating from the address space of the national segment of the Internet. Most of this activity, namely 76%, is made up of botnet participants. In particular, when compared with the same period in 2020 (more than 20 million cyber threats), the number of cyber threats to cybersecurity decreased by 20%, due to coordinated measures to respond to identified cybersecurity vulnerabilities and network anomalies. In addition, using the Center's web application protection system, 1,354,106 cyber-attacks were detected and reflected against websites of the national segment of the Internet. The largest number of cyber-attacks were carried out from the territory of Uzbekistan, the Russian Federation, Germany, etc. During the monitoring of information systems of government agencies connected to the interdepartmental Data Transmission Network (IMTN), 33,317,648 security events were recorded, of which 347,742 events could lead to unauthorized access and leakage of confidential information. According to the results of monitoring of cybersecurity incidents committed against websites of the UZ domain zone, 444 incidents were recorded, of which the largest number accounted for unauthorized downloading of content - 341 and unauthorized modification of the homepage (Deface) – 89. An analysis of the incidents showed that websites in the public sector (134 incidents) are 3 times less likely to be attacked than those in the private sector (310 incidents).

A detailed analysis of the incidents showed that the most vulnerable (often attacked) websites are those developed on the content management systems WordPress, Joomla, Open Journal Systems and Drupal. The main reasons and ways to successfully implement hacker attacks are: the presence of vulnerabilities in web applications, in particular due to late updates (72%), the use of weak passwords (25%) and others. In particular, the investigations revealed 6,635 malicious files and

scripts that pose cybersecurity threats to information systems and resources, as well as their users.

Along with this, it was determined that in 97% of cases, the sources of illegal activity are the address spaces of foreign countries. In particular, the largest number of cases of illegal activity is associated with the following countries: the USA, Indonesia, the Netherlands, Romania, Algeria and Tunisia. At the same time, it must be remembered that attackers use proxy services to hide their true location and use chains of proxy servers to complicate their search. Such a large amount of illegal activity in the Republic's address space is due to the disregard of the majority of owners and administrators of national information systems and resources for information and cybersecurity requirements, which significantly increases the risk of unauthorized interference in their work.

Among the identified events, 245,891 may lead to the compromise of information systems (IS). The main factors determining the vulnerability of IP to information influence and increasing the importance of the problem of protecting processed information from unauthorized access (SDA) include:

- a long period of operation inherent in information and network resources, due to the emergence of new tasks, tools and technologies for information processing in computer systems;
- the possibility of errors and undeclared features in the software of computer systems in the case of using software products executed on closed source codes;
- significant remoteness of computer system nodes from each other and their possible interaction via public networks (Internet), which leads to the need to organize secure computer communication channels over open communication channels;
- the development of high-speed information acquisition and processing systems based on molecular computers and artificial intelligence from a potential enemy.

All of the above indicates the aggravation of cyber threats in Uzbekistan. And it is not difficult to conclude that today it is worth paying special attention to security in cyberspace, in particular, increasing the level of security and ensuring cybersecurity of information systems and websites, as well as regularly improving the level of user knowledge in the field of information and communication technologies and information security. Along with this, experts recommend:

1. Use licensed and certified operating systems and software.

2. Regularly update and keep up-to-date versions of the operating systems, software, and security components used. Updates should be made from official sources.

3. Use security plug-ins with search, removal and protection functions against malware in the future.

4. Regularly backup databases, files, mail, and more.

5. Removing unused plugins – any new plugin or extension increases the risk of an attack by intruders. In this regard, it is recommended to disable and remove unused plugins and, if possible, use the built-in mechanisms instead of installing a plugin for each special case.

6. Strengthen password authentication – it is strongly recommended to use a complex and non-repeating password for an administrative account, a personal cabinet on the service provider's website, and an account on the server (for example, for dedicated or "co-location" hosting). When changing a password, it is recommended to use the rules for forming passwords for accounts, which provide for password generation using numbers, special characters, upper- and lower-case letters with a minimum length of 8 characters. It is recommended to set up two-factor authentication (if possible). It is also recommended to set a limit on the number of login attempts (protection against password brute force attacks).

7. Access the information system or website from devices (computers, tablets) on which antivirus software with up-to-date databases of virus signatures is installed.

8. Periodically conduct examinations for compliance with cybersecurity requirements of information systems and resources. Timely eliminate identified vulnerabilities based on recommendations sent based on the results of the conducted examinations.

9. Regularly improve the skills and level of knowledge in the field of information and communication technologies and information security of users (employees). 10. Promptly respond and take appropriate measures to eliminate threats and eliminate the consequences of cybersecurity incidents.

The adoption of the above and other additional protection measures will significantly reduce the risks of cybersecurity threats, which in turn will make it possible to protect oneself from possible attacks and the subsequent need to eliminate the causes and consequences of information security incidents.

CONCLUSION

Thus, it can be concluded that the information sphere is becoming a system-forming factor in the lives of individuals and entire states. Modern technologies are

widely used in the management of fundamental objects of vital activity, which become vulnerable to accidental and intentional impacts.

A priority in improving information security. The Republic of Uzbekistan is working on a regulatory framework, as well as improving the mechanism of state regulation of activities in this area. Preventive conversations with the population are also an integral part of addressing the issue of information security for both the country as a whole and an individual in particular.

LIST OF LITERATURE USED:

1. О некоторых вопросах государственного управления в сфере связи, информационных технологий и массовых коммуникаций: указ Президента от 3 декабря 2008 г. № 1715 // КонсультантПлюс: сайт. URL: <https://www.consultant.ru>.

2. О системе и структуре федеральных органов исполнительной власти: указ Президента от 9 марта 2004 г. № 314 // КонсультантПлюс: сайт. URL: <https://www.consultant.ru>

3. Информационные технологии в бизнесе [Электронный ресурс]. - URL: <http://bit.samag.ru/uart/more/67/> // свободный (дата обращения: 16.11.2019).

4. Кеворкова Ж.А. Организационные аспекты экспертно-аналитической деятельности в организациях государственного сектора // Бухгалтерский учет и налогообложение в бюджетных организациях. - 2019. - № 2. - С. 48-52.

5. Конференц-центр. Интересы аудитории [Электронный ресурс]. - URL: <https://spymetrics.ru/en/website/conference-center> // свободный (дата обращения: 12.11.2019).

6. Роль государства и бизнеса в цифровой трансформации [Электронный ресурс]. - URL: <http://www.tadviser.ru/index.php/> // свободный (дата обращения: 25.11.2019).

7. Саунин А.Н., Бергаль Е.В. Внутренний финансовый контроль и аудит в государственном секторе экономики // Бухгалтерский учет и налогообложение в бюджетных организациях. - 2018. - № 7. - С. 31–37.

8. Система менеджмента информационной безопасности (ISO 27001) [Электронный ресурс]. - URL: <https://standartno.by/services/sistema-menedzhmentainformatsionnoy/> // свободный (дата обращения: 22.11.2019).

9. Цифровизация экономики [Электронный ресурс]. - URL: <https://www.securitylab.ru/blog/company/AngaraTech/341654.php/> // свободный (дата обращения: 24.12.2019).

10. IT-рынок в цифрах [Электронный ресурс]. - URL: <https://www.gartner.com/en> свободный (дата обращения: 30.11.2019).