Open Herald: Periodical of Methodical Research
Volume 1, Issue 2, May 2023
ISSN (E): 2810-6385
Website: https://academiaone.org/index.php/6

Ensuring Information Security Is A Factor In Ensuring The Stability Of Society

Khushruy Kirgizboyeva
Master's Degree Student, Journalism and Mass Communications University of Uzbekistan

Abstract

The article analyzes the processes of emergence of information security problems along with the globalization of information and communication technologies. In addition, the main focus of the article is on cyber attacks, the growth of cybercrime, the measures taken by the government of Uzbekistan against it, and the processes of combating this "plague" of the 21st century.

Keywords: information technology, information security, protection of information security, cyber security, cyber terrorism, cyber crime, electronic signatures, Internet users, cyber fraud.

Introduction

Work on computerization and informatization in Uzbekistan began at the beginning of the 21st century. It was the adoption in 2003 of the Law of the Republic of Uzbekistan "On Informatization" that determined the first steps in this process. The Law "On the Principles and Guarantees of Freedom of Information" regulates measures to ensure information security at all three levels: the individual, society and the state. The rapid development of the Internet and information technology has contributed to the emergence of an electronic digital signature (EDS). The Law "On Electronic Digital Signature" regulates relations in this area [1,2].

Methodology

Currently, a necessary condition for the development of the information society is cyber security, behind which there can be an almost endless list of security problems and their solutions from technical to legislative. For this purpose, the Law "On Cyber Security" was adopted, according to which the protection of the interests of the individual, society and the state from external and internal threats in cyberspace is a priority. In addition, the Decrees of the President of the Republic of Uzbekistan "On measures to further improve the sphere of information technologies and communications" dated February 19, 2018, "On approval of the Strategy "Digital Uzbekistan - 2030" and measures for its effective implementation" dated October 5, 2020, the Resolution of the President "On measures to improve the system of control over the implementation of information technologies and communications, the organization of their protection" dated November 21, 2018 2020 were adopted.

An information security management system is to provide a model to guide its implementation and operation. This includes international standards defining ISMS requirements, risk control, metrics and measurements, and implementation guidance [3,4,5].

ISO/IEC 27000 is a series of international standards published jointly by the International Organization for Standardization (IOS) and the International Electro technical Commission (IEC). It contains best practices and recommendations in the field of information security for the creation, development and maintenance of an ISMS [5,6].

Through the efforts of scientists in the field of information security, over the years of independence, Uzbekistan has become one of the countries that have their own algorithms for cryptographic information protection. For this purpose, a number of state standards have been developed. Among them:

O'z DSt 1092 Information technology. Cryptographic protection of information. Processes of formation and verification of electronic digital signature.

O'z DSt 1105 Information technology. Cryptographic protection of information. Data encryption algorithm.

O'z DSt 1106 Information technology. Cryptographic protection of information, hash function and others.

Since 2017, a Specialized Production Department has been opened in the structure of Unicon.uz State Unitary Enterprise, where small-scale production of cryptographic information protection tools has been established.

The main tasks of ensuring information security in the provision of electronic public services and the processing of confidential information are:

- protection of information resources from disclosure, loss and unauthorized access, ensuring their integrity, availability and confidentiality;
- ensuring the reliable functioning of information systems and the services they provide, protection against unauthorized access;
- ensuring the confidentiality of information.

Since its inception, Unicon.uz, making a worthy contribution to the development of ICT, has become one of the leading scientific and technical organizations in Uzbekistan, which has sufficient potential to solve these problems. At present, complex scientific and technical problems in the field of information technology and communications are being solved with the direct participation of scientists and specialists Unicon.uz [7].

Results and discussion

As the experience of developed countries has shown, digitalization, automation, computerization are continuous processes. Therefore, the change of the calendar year is practically not a starting point. On October 1, 2019, the law “On Personal Data” came into force in Uzbekistan. Obviously, this is the very beginning of a long journey to protect personal data. The law only in the most general terms establishes the regulation of the sphere. On February 8, 2020, the Resolution of the Cabinet of Ministers No. 71 "On Approval of the Regulations on the State Register of Personal Data Bases" was adopted. It explains the procedural issues for registering personal data bases.

Another, perhaps inconspicuous, but significant event was the transformation of the Cyber security Center, which has undergone several reorganizations in recent years. A noticeable trend over the past couple of years has been the influence of new, non-traditional information delivery channels. First of all, these are social networks and telegram channels. Another important aspect of the interaction of people on the Internet is the ability to remain anonymous, this can give rise to a sense of permissiveness and impunity.

We hear almost every day about incidents, hacks, data leaks related to containers. Containerization technology is rapidly gaining popularity, especially among web developers. If the operating system was previously virtualized, i.e. it was possible to run several virtual systems at the same time on one physical computer, now each individual application can be run in a separate environment - a container. Now, to launch, for example, a website, you no longer need to install an operating system, then separately a web server, a database server. All this is "assembled" from "bricks" - containers. The ease of deploying containers is also a weak point of the technology. Enterprise security services may not know how many and which containers developers are deploying. Therefore, information security specialists should pay more attention to this technology so that it brings only convenience, and not new problems.

There has been a trend - more or less large enterprises create their own mobile applications. Banks are trying to "lure" users into mobile applications. It is clear that if you simplify the procedure for processing, for example, a term deposit, then a greater number of customers will be tempted to it, because not everyone has the time and desire to go to the bank office. Here, special attention should be paid to information security issues, because the development of such applications is carried out in time pressure. Even for full-fledged debugging and testing of the code, there is often no time, not to mention its verification (revision) of the code for safety. Therefore, here you need to soberly assess the risks, which is more important - to release a “raw” product faster or a little later, but more reliable [8].

Cybercrimes are characterized by a high level of economic damage. Their victims are about 559 million people a year; per day - more than 1.6 million people; per second - 19.

Cybercrime causes significant damage to trade, competition, development of innovations, and slows down the economic growth of countries. So, in 2020, the damage from cybercrime amounted to 1.23% of global GDP, while in this indicator, cybercrime exceeds drug trafficking (1.03% of GDP), counterfeiting of goods (the so-called "piracy") (0.93% of GDP), yielding only to international crime and terrorism (1.35% of GDP).

In the field of information technology, there is a tendency to reduce the age of the subject of crimes. Specialists of the largest media about IT and IT security "Hacker" claim that 90% of acts of vandalism on the Internet are carried out by teenagers and young people [8,9].

It should be emphasized that the Internet is a comfortable environment for the formation of a hacker's personality: there are a number of resources on the global network designed to teach hacker skills. The process of institutionalization of hackers is very dynamic, although they still strictly observe the principle of anonymity (aliases are used instead of their own name).

However, in addition to the negative links between hackers and criminal gangs, there has recently been a clear trend of interaction between the hacker movement and government and commercial structures. Moreover, some of the known hackers are actively involved in international information security organizations. So, the president and founder of the Chaos Computer Club (“Computer Chaos Club”) Andy Muller-Megan is a member of the global organization ICANN (Internet Corporation for Assigned Names and Numbers) [10].

In recent years, an average of 67 new incidents of ransom ware attacks have been detected daily in Uzbekistan. There has been an increase in scams linked to a fictitious helpdesk, where victims are told that they were asked to make bank transfers to foreign accounts or purchase large amounts with prepaid cards. Losses amounted to more than $347 million, which is 137% more than in 2020.

Only in Tashkent in 2022, 4,332 crimes in the field of information technology were committed, which is 40 times higher than in 2020, when law enforcement officers recorded 106 such facts. Such statistics were given by employees of the Main Department of Internal Affairs of the capital at a briefing on cyber security.

Compared with the data for 2021, last year the number of cybercrimes doubled - from 2281 to 4332. Of these, 2747 are cyber thefts, 625 are cyber fraud, 874 are offenses related to the distribution of drugs via the Internet [11].

According to information, there are more than 25 million Internet users in Uzbekistan. The results of the analysis showed that today in the country there is a tendency for the growth of cybercrime.

Over the past 3 years, the number of cybercrimes has increased several times. In particular, several types of cybercrime are reported:

- ➢ Fraudsters take the codes from the SMS messages sent to the plastic card users under the pretext of making a payment, giving the winnings, and embezzling the funds from it;
- ➢ extortion by threatening to acquire and disclose personal information (cyber extortion);
- ➢ intimidation, abuse, suicidal cases (cyberbullying) on social networks, etc. [12].

On April 15 of this year, the Law "On Cyber security" was signed by the President. According to it, protecting the interests of individuals, society and the state from external and internal threats in cyberspace is a priority in ensuring the state's cyber security. According to it, the unified state policy in the field of cyber security is defined by the President. The State Security Service is the competent state body in the field of cyber security.

Verification of compliance with cyber security requirements is carried out on a mandatory basis or at the initiative of cyber security subjects.

The following are subject to mandatory verification for compliance with cyber security requirements:

- – information resources of state bodies;
- – information systems of state bodies;
- – information systems classified as important objects of information infrastructure.

In addition, hardware and software used to ensure the cyber security of information systems and resources of state bodies and organizations must be certified without fail.

Information about vulnerabilities, cyber threats, cyber attacks and other malicious actions, as well as information about information objects found in information systems and resources, can be disclosed with the permission of the cyber security subject after taking appropriate measures to protect them [12].

Conclusion

The analysis shows that the fight against cyber terrorism and cybercrime, which is growing in Uzbekistan in the context of globalization, has intensified in the next five years, and its legal foundations have been created. In general, ensuring information security in the country has risen to the level of state policy. At the same time, the government considers information security reforms as an important factor in ensuring the stability of society. Reforms in this area are shown as an important component of the reforms in the formation of New Uzbekistan. During this period, ensuring information security in cyberspace became a priority of state policy.

References:

1. Ҳайитов Б. Ўзбекистонда сўнгги 3 йилда кибержиноятлар сони кескин ошган. 18.06.2022 й.// https://hordiq.uz/2022/06/18/uzbekistonda-sunggi-3-yilda-kiberjinoyatlar-soni-keskin-oshgan/
2. Джураев, Д., & Уралов, М. (2021). Совершенствование процесса дистанционного образования во время пандемии «covid 19» через создание многоязычного словаря по географическим объектам Узбекистана. *Психология и педагогика: Проблемы и решения*, *1*(1), 10-12.
3. Turgunov, A. A. (2022). The concept of improving the psychological service as a system for the development of preschool education. *Innovative developments and research in education*, *1*(11), 134-138.
4. Abduvakhidovna, Y. N. (2022). Directions for the Effective Use of Innovative Strategies in the Management of Industrial Enterprises. *Open Access Repository*, *8*(6), 125-129.
5. Yuldasheva, N. (2022). Features of the process of forming innovative strategy under conditions of modern realities. *Academic research in modern science*, *1*(9), 310-312.
6. Юлдашева, Н. (2022). Корхоналарда инновацион ривожланиш стратегиясини бошқариш хусусиятлари. *Экономика и образование*, *23*(2), 129-135.
7. Джаматова.Д. Нормативно-правовая база в области защиты информации. 26 авг. 2022 г. Текст: Анастасия Боровикова.// https://yuz.uz/ru/news/normativno-pravovaya-baza-v-oblasti-zait-informatsii.
8. Ракитский А. Чем живет информационная безопасность в Узбекистане? 23.03.
9. Abduvakhidovna, Y. N. (2023). Factors influencing the implementation of the innovation strategy at industrial enterprises. *World Bulletin of Management and Law*, *19*, 5-11.
10. Расулев А., Турсунов А. Противодействие киберпреступности – требование времени// https://iiv.uz/ru/news/counteracting-cybercrime-is-a-requirement-of-the-time.
11. Количество киберпреступлений в Ташкенте за два года увеличилось в 40 раз// https://fergana.media/news/129278/.
12. Ўзбекистон Ремпубликасининг “Киберхавфсизлик тўғрисида”ги Қонуни. 15 апрель 2022 й. Қонунчилик маълумотлари миллий базаси, 16.04.2022 й., 03/22/764/0313-сон.