ENSURING PERSONAL INFORMATION SECURITY: PREVENTION AND PREVENTION

Gayrat SADULLAEV

Doctoral student of the Faculty of Postgraduate Education of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

Abbos ABDUGOFAROV

Lecturer of the Department of Crime Prevention Activities of the Academy of the Ministry of Internal Affairs

ABSTRACT

At the very heart of information technology, information security has become an issue of paramount importance. Information protection is the process of protecting confidential information from unauthorized access, use, disclosure, modification and destruction. A brief history of information security begins in ancient times. The thirst to transmit messages confidentially can be scrolled in the birth of writing. Over time, the methods only became more complicated with the use of ciphers, seals, signatures, and even pigeons-accomplices. Now in the age of electronics and digital processing, the process is becoming more complex and requires new methods of protection. In this blog, we will delve into the history of information protection and consider its significance in the modern world.

Even in ancient times, people understood how valuable it was to keep confidential information. And for this they used various methods. For example, encryption, which still remains one of the most common ways to protect information. However, in addition to encryption, seals and signatures were also used in ancient times to confirm the authorship and authenticity of documents. Cryptography was used to create correspondence that was incomprehensible to outsiders. Encryption machines appeared later, but they were a breakthrough in the cryptography of that time. And the use of pigeons-accomplices can be considered as the most ancient analogue of modern data transmission over the Internet. As you can see, ancient methods of information protection have largely determined modern technologies. And, although we will be able to find more advanced methods of protecting information, their basic techniques have also been discovered a long time ago.

Currently, information protection has become more complex and diverse due to advanced technologies and the spread of the Internet. E-mail, as a means of communication, allows you to exchange messages instantly, but at the same time greatly increased the likelihood of hacking correspondence. Creating passwords has become an integral part of protecting information on the Internet. However, many users prefer to use simple and easily chosen passwords. The electronic signature is intended to replace the traditional handwritten

signature and simplify the procedure for signing documents. Watchdog programs monitor the computer for unwanted changes and unusual activity, which helps prevent data leakage.

In a world where cybercrime is becoming more common, there are many ways to protect your digital data. One of the most important is the use of secure messengers, such as Telegram and Signal, which offer encryption to protect correspondence. Another effective method is the use of multi-factor authentication, which requires a combination of two or more forms of authentication, such as a password and a fingerprint, to access data. Data encryption is another way to protect information by encrypting data in digital files, making them difficult to read without a key. With Retina Scan technology and other biometrics technologies, you can now use your own biology as a form of authentication. This provides another layer of protection for your data. Some companies also create "whitelists" to block unwanted applications and websites, which helps reduce the risk of violating the security of your data. Using these methods together can provide a higher level of security when working with digital data. But remember that this does not provide one hundred percent protection, so do not forget caution and thrift when handling confidential information.

The development of artificial intelligence will forever change the way we regulate and protect our data. If earlier information security software was based on pre-written rules, then in the future it will be deep neural networks that will be able to detect and prevent data leaks. Quantum encryption is another way we can protect our data in the future. This is a new technology that can resist hacking by computer algorithms that are currently in use. Protecting your personal data is more important than ever. With the growing number of digital devices and online services, we have accumulated a lot of personal data. In the future, we will have to protect this data using new technologies and innovative methods. And finally, cyber wars. In the future, as more and more states switch to the digital economy, cyber warfare will become more common. It will be necessary to develop and improve information security methods to prevent serious consequences.

In the modern world, information protection plays an important role in various aspects of our lives. It affects politics and economics, including international relations and competition between countries and companies. Privacy is also becoming increasingly problematic, as many things cannot be hidden on the internet. The protection of national interests also depends on the protection of information from foreign agents. Finally, information protection is an urgent need as the world becomes more connected and information more accessible. The lack of adequate protection can lead to disastrous consequences, not only for individuals, but also for entire nations and the world community.

So, the history of information protection teaches us that we should value our privacy and rely on advanced technologies to ensure the security of our data. Over time, we have improved and developed information security methods to meet the modern challenges and threats that we face today. This shows how important and urgent our need for information protection is. You know what they say, it's better to be safe than sorry later!

In the modern information society, the issues of information security are becoming more and more relevant and important. Personal information security is becoming one of the priorities of every citizen, as threats from cybercriminals, hackers and other intruders can lead to serious negative consequences for a person.

In the Republic of Uzbekistan, the issues of ensuring the security of information and personal data are under special control and protection by the state. Criminal law protection of personal information security is an important tool aimed at preventing and combating crimes in the field of information technology.

The legislation of Uzbekistan includes a number of norms regulating information security issues. Thus, the Code of the Republic of Uzbekistan on Administrative Responsibility provides for punishment for violators engaged in cybercrimes, such as unauthorized access to computer information, the creation of malware, the spread of viruses and others.

Information security of the individual is ensured by creating the necessary conditions and guarantees of free access to information, protection of privacy, protection from illegal information and psychological influences (Article 13 of the Law of the Republic of Uzbekistan "On principles and guarantees of freedom of information"). This provision has been included in the provisions of a number of laws. The Law of the Republic of Uzbekistan "On Guarantees and Freedom of Access to Information" states that everyone has the right to request information directly or through their legal representatives. It is also emphasized that the mass media are obliged to verify the accuracy of the published information, and are jointly responsible with the source of information for its accuracy in accordance with the procedure established by law.

It should be noted that Uzbekistan is taking all necessary measures to prevent and investigate crimes in the field of information technology. For this purpose, special institutions have been created, such as the National Center for Information Security. They are engaged in prevention and investigation in case of threats to information security.

In addition, training events and courses on information security are held in Uzbekistan, as well as information campaigns aimed at raising public awareness of possible threats and ways to protect personal data.

Thus, the criminal law protection of information security of the individual in the Republic of Uzbekistan is a priority task of the State. Thanks to the system of laws and the measures introduced, the state creates conditions for protecting citizens from cybercrime and ensuring their personal information security. However, every citizen should also be aware of possible threats and take self-defense measures to ensure the security of their information.

References:

1. The Code of the Republic of Uzbekistan on Administrative Responsibility. https//lex.uz/acts/97661

2. The Law of the Republic of Uzbekistan "On Guarantees and Freedom of access to information" dated April 24, 1997 No. 400

3. Criminal Code of the Republic of Uzbekistan //lex.uz/acts/97661

4. Расулев, А., & Садуллаев, Г. (2021). Training of personnel in the field of countering cybercrime: the need and the requirement of time . in Library, 21(1), 123–130. извлечено от https://inlibrary.uz/index.php/archive/article/view/9137

5.   Sadullaev, G. (2022). Ensuring information security by internal affairs bodies: the requirement of time. Current trends in the development of digitalization in the field of justice, 1(1), 193–197. https://doi.org/10.47689/978-9943-7818-1-8-MTDDFJ-2021-pp193-197