NOVATEUR PUBLICATIONS
JournalNX- A Multidisciplinary Peer Reviewed Journal
ISSN No: 2581 - 4230
VOLUME 6, ISSUE 9, Sep. -2020

INFORMATION SECURITY POLICY AND THE PROCESS OF COMBATING CYBERCRIME IN UZBEKISTAN

ALIEV OLIMBEK AYBEKOVICH
Researcher of Andijan State University
Political Institutions, Processes and Specializes in Technology

ABSTRACT:

Consistent work is being done in our country to ensure the transparency of public authorities, the development of the media, freedom of speech and information, as well as the consideration of citizens in making decisions of social and public importance.

KEYWORDS: State, cyber security, society, information security, public, internet.

INTRODUCTION:

At the beginning of the 21st century, the concept of "cyber security" began to be used as a synonym for the concept of "information security". Because by this time, computers began to be recognized as the source of information. In the broadest sense, cyber security is defined as technical, legal and organizational measures to combat cybercrime, protection of personal, corporate and government information, fostering a culture of cybersecurity, the development of technical interconnection of Internet service providers.

However, in Uzbekistan in 2013-2015, information attacks on society and the state increased significantly. According to the analytical site Secure List, the country was rated as belonging to the group of countries at high risk of disabling the media and technology used in the country with various malware. A 2014 report by Kaspersky Lab ranked Uzbekistan as one of the "five" countries with the highest risk of virus infection and the highest risk of theft of information from bank customers.

MAIN PART:

The presence of Computer Attack Response Teams (CERTs) as the most important component of cyber security in Uzbekistan has become a criterion for determining the country's activities in this area. The launch of such a national service in Uzbekistan began in 2013. It was created as a UZINFOCOM structure and later transferred to the Information Security Center.

At the same time, another state structure - UNICON.UZ under the Agency for Communications and Information, began to deal mainly with information security in business. With his participation, he contributed to the development of the use of electronic digital signatures by providing online banking services in secondary banks. However, during this period, Lex.uz lawyers admit that in the field of information security in the country has not been adopted any conceptual document that would legally systematize this area.

To date, the concept of "cybercrime" has included many types of crimes in the field of ICT. These include the development and distribution of malware, the dissemination of illegal information, the mass sending of e-mails (spam), hacker attacks, hacking of websites, extortion, copyright infringement, theft of credit cards and bank details (phishing and farming). , and dozens of other criminal acts. In all cases, the perpetrators inflicted material and moral damage on their object.

Acting on behalf of the state institution "Center for Information Security" under the Ministry of Information Technologies and

Communications of the Republic of Uzbekistan on the basis of the Resolution of the President of the Republic of Uzbekistan dated June 27, 2013 No PP-1989 was established as a non-profit organization in the form of a state institution.

However, due to insufficient resources of the center, lack of new foreign technologies, lack of good specialists, it was not able to perform its functions and tasks at the required level. However, in 2017, at the initiative of President Sh. M. Mirziyoev, significant changes began to take place in this area.

On implementation of the Resolution of the President of the Republic of Uzbekistan dated August 29, 2017 No PP-3245 "On measures to further improve the project management system in the field of information and communication technologies" and measures to ensure information and public safety, as well as law enforcement using modern technologies In order to ensure the timely and quality implementation of the project to create a single hardware and software complex "Safe City", the Information Security Center of the Ministry of Information Technologies and Communications of the Republic of Uzbekistan was reorganized as a supply assistance center.

Activities of the State Inspectorate for Informatization and Telecommunications of the Republic of Uzbekistan on behalf of the State Unitary Enterprise "Technical Assistance Center" in accordance with the Resolution of the President of the Republic of Uzbekistan dated November 21, 2018 "On measures to control the introduction of information technologies and communications" began to operate as an organization in the form of a state unitary enterprise.

The policy of information security, the process of its unification, the implementation of deep reforms in this area began in the last quarter of 2016 - with the coming to power of President Sh. M. Mirziyoev. In the same year, the Ministry of Information Technologies and Communications and law enforcement agencies signed a Regulation on the identification and analysis of offenders using methods and tools for the use of illegal and destructive behavior in the information field, and it came into force. In order to intensify the struggle in this area, a new department was established under the Prosecutor General's Office.

From 2018, the Center for Technical Assistance began to constantly monitor all incidents involving the information security system of government agencies connected to the interdepartmental network of e-government data transmission. As a result of monitoring the events in the field of information security in the information system of public authorities in the first quarter of 2018 and 2019, 54953759 cyber crimes and violations were detected. Of these, 2,502,353 were rated as high risk. In 2018, the majority of government information security attacks were detected on CMS (Content Management System) websites running WordPress.

In 2019, 268 cyber attacks (including 222 illegal downloads, 45 failures, 1 covert mine), 816 injuries and 132,000 cyber security threats were detected in the national segment of information systems and Internet websites in Uzbekistan.

During 2019, the examination of information systems and websites in the country for compliance with information security requirements (as a result of audits) revealed 816 violations in the information system as threats of various levels.

Of course, such injuries could allow criminals to access information systems or websites remotely, eventually leading to the theft of the personal data of more than 2 million citizens in the country. At the same time, in the framework of the "Information Security Monitoring Information System" in the process

of monitoring the information systems of government agencies 17 mln. 620025 adverse events were detected.

During the monitoring of the national segment of the Internet, 132003 takiber security threats were identified. The study and analysis of these threats showed the following:

-106508 events related to hosts of botnet network participants;

-13882 cases are related to blocking of IP-addresses, which are blacklisted by various services due to sorting reasons for sending spam messages or opening passwords;

-8457 events are related to ports that download foreign content due to the use of the TFTP-protocol (Trivial File Transfer Protocol), as well as the lack of authentication mechanisms when using it;

-2114 cases occurred due to the use of damaged RDP protocol (Remote Desktop Protocol);

-1042 cases were caused by the use of software and SUDBs that do not have an authentication mechanism, as well as expired or questionable and unreliable SSL-certificate signatures.

It is known that from the end of 2018 to the beginning of 2019, the British research company Comparitech will analyze the ranking of countries on the level of cybersecurity. The ranking is based on the participation of 60 countries, with Japan leading the ranking. The last place is taken by Algeria, and Uzbekistan is in 56th place.

A botnet is a computer network consisting of several hosts run by autonomous software. Often, a bot is a program that is secretly installed on an attack object within a botnet, in which the criminal allows access to compromised computer resources. Typically, it is used to covertly engage in unwanted activity - sorting passwords on a remote system, sending spam, carrying out cyber-attacks (DoS- and DDoS-attacks) when a service is denied, and so on. However, bots are not viruses.

According to a study conducted by an ESET expert on cyber security in Uzbekistan, 72% of companies are exposed to external cyber threats and 55% to internal threats. The study's press release states: “One in ten companies in Uzbekistan (10%) has an encryption problem: a cybercriminal blocked access to files and demanded money to recover it. The danger of these threats is that the codes for restoring the blockade will not be available to the perpetrator, so the consequences of this crime cannot be changed".

While businesses in Uzbekistan tend to increase their budgets for information security, spending is often ineffective. This is because it is limited to installing antivirus software without a deep understanding of how destructive the threats are. As cyber-attacks become more complex year by year, the consequences of which can lead to financial losses and damage to the company's reputation, the business sector needs DLP-technologies (Data Leak Prevention), early response and monitoring systems, zero-day protection against threats.

CONCLUSION:

In short, the development of ICT in Uzbekistan in 2017-2020 has accelerated, modern technologies in this area have been introduced in the country, a large amount of money has been spent in the field of ICT. As this development progresses, threats to information security are increasing, and new forms of these threats are emerging. Therefore, in 2017-2020, the country has formed a system of information security, the legal framework and institutions for it. International cooperation in this area has also strengthened.

REFERENCES:

1) Xurramov Sh. V Uzbekistane rastet interes k informatsionnoy bezopasnosti // https: //digital.report/v-uzbekistane-rastet-interes-k-informatsionnoy-bezopasnosti/
2) Raxmatullaev Z. Aktualnaya tsel - borba s kiberprestupnostyu. 03.04.2017 // http: //uzbekistan.nsk.ru/ index.php? Catid = 1: 2010-03-12-13-22-28 & id = 6515: 2017-04-03-15-42-52 & option = com_content & view = article.
3) Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 838 "On measures to organize the activities of the Center for Information Security and Public Order of the Ministry of Information Technologies and Communications of the Republic of Uzbekistan." 2017 y. October 17.// National Database of Legislation, 18.10.2017, No. 09/17/838/0130, May 1, 2018, No. 09/18/318/1108; March 27, 2019, No. 09/19/254/2839.
4) About the Center for Information Security // https: //tace.uz/uz/company/
5) Cybersecurity of Uzbekistan in tsifrax: itogi 2018 year // https: //ictnews.uz/24/04/2019/cyber-security-2018-2/.
6) May is a program that uses computing resource devices to generate various cryptocurrencies. It can also be installed by the users themselves. However, this is about their illegal and covert species.
7) Cybersecurity of the Republic of Uzbekistan: results for 2019 (review). 03.03.2020 // https: // review. uz / ru / post / kiberbezopasnost-respubliki-uzbekistan-itogi-2019-goda
8) Isaev T. ESET: kajdaya desyataya kompanika v Uzbekistane postradala ot shifratorov. February 18, 2020 // https: //www.podrobno.uz/cat/tehnp/eset-kazhdaya-desyataya-kompaniya-v-uzbekistane-postradala -ot-shifratorov /.