INFORMATION SECURITY THREATS IN MODERN WORLD

Ramil Aslanov
(*aslanovram@list.ru*)
Doctor of law
(Baku State University)

Abstract

Among the most acute threats to information security in the current period of development of society, the following can be noted: Creation and use of means of influence and damage to information resources and telecommunication systems of the country; Purposeful informationnal influence on strictly significant bodies; Informational influence, implemented to undermine the political, economic and social systems of the government, moral processing of people for the destabilization of society; Unauthorized intrusion into information and telecommunication systems and information resources, as well as their illegal use; Global terrorist institutions threaten the information security of countries around the world; Illegal use of information technology to the detriment of fundamental human rights and freedoms; Unlimited state boundaries of computer networks has a global character. Cross-border dissemination of information contrary to the principles and norms of international law, as well as the national legislation of states.

Keywords: *threat, information security, information technology, information resources, information and telecommunication systems, the Internet, terrorist institutions, human rights and freedoms, computer networks, information dissemination.*

In the modern world, information technology plays a vital role in all spheres of life. The global information technology revolution has effectively changed the politics, economy and social life of the world community. To such a degree of development and application of information technologies, the question of protecting society from their use for illegal purposes inevitably arises. High-tech crime knows no limits and is a threat to global security.

The role of computer networks as an integral part of everyday life makes information security critical for people and organizations. The amount of personal and corporate information stored on the network, as well as the diversity of information threats, combine to form the urgent need to strengthen the protection of this information [12, 1].

In the modern world, the threat to information security is one of the main problems for humanity. Intensive maturation and widespread introduction of the latest information and telecommunication technologies, being a true period of economic, scientific and technological progress and a necessary condition for the further development of society, have simultaneously generated a complex of negative consequences.

The cyberworld has created a coordinate less ability to use slanderous comments to tarnish another person's honor and reflect this around the world. Cyber fraud is one of the most global problems in the internet world [11, 303-312].

With the development of the Internet, the role of information technology in the period of hostilities has increased. A prime example of the role internet technology can play in modern politics is the much-publicized Wikileaks scandal, which began publishing secret US government diplomatic documents. The scandal prompted the United States to ponder how to balance security and freedom when using the Internet.

WikiLeaks is an international non-profit organization that publishes classified information that is appropriated from unknown sources or when this information is leaked. The authors of the website, which was launched in 2006 by the Sunshine Press, announced that they have a collection of 1.2 million documents that they have collected in the first year of the website's life [17].

Contact with the Internet gives not only benefits and pleasure; even experienced users face many threats that can take away their time and finances. Computer villains use the Internet to steal data, extract illegal profits, and damage rivals. Fraud on the Internet brings a lot of damage to the user. Fraud on the Internet means: theft of personal confidential data, luring large sums of money.

In recent decades, the scale of information threats has increased significantly. The scandalous events of recent years give reason to believe that information can be stronger than any of the previously known weapons of mass destruction. In the conditions of the most powerful computerization, insufficient level of protection of computer information from unlawful encroachments, it is possible that the problem of information security has become the first global problem of our time. Law remains the main means of ensuring information security. With its help, you can solve problems with such an object of law as information.

In the current circumstances, information becomes a strategic resource, on the successful use of which the possibilities of forming an economy, the development of an information civil society, and a guarantee of the security of the country and people depend. Information as a phenomenon of the public sphere is subject to legal regulation [13, 6]. The consumption of information and the means of its transmission was initially imposed freely and only over time, therefore, by a rite, an object of customary law. Nevertheless, even in the mid-1980s. the experts noticed that the information did not contain any general establishment, including in the law.

At least 2 types of computer crimes are distinguished: 1) in the first category of crimes, the object of encroachment is a computer, and they are carried out through attacks on the secrecy and completeness of the Internet; 2) and the second category of crimes includes fraud, theft, forgery carried out by the computer itself. The emergence of new social problems leads to the typical emergence of new rights and the fight against these problems, at the same time preventing their consequences [3, 771-823].

Fraudsters often use social engineering, phishing, pharming, malware, spam, etc. to fulfill their selfish goals. Phishing is an Internet fraud technology that involves theft of personal data (passwords, debit card credentials). The fraudster, by deceiving the user, coerces him to give personal secret information. At the same time, it should be noted that the victim performs all actions unconditionally unconditionally, without realizing what she is truly doing. For this, social engineering technologies are used.

Phishing is currently divided into two types. Mail phishing - a special letter is sent by e-mail with a request to send some data. By clicking on the link shown, the victim goes to the site. But this site, despite the outward absolute similarity to the original, was designated only for the victim to enter confidential information herself.

In online phishing, scammers copy certain sites (for example: an online trading site). In this case, similar domain names and a similar look are used. The victim, getting into such a site, decides to buy some product. All suspicions are dispelled due to the popularity of the copied site. By purchasing the product, the victim is registered and enters the number and other details of the personal credit card [14, 112-113].

Pharming is a procedure for stealthily redirecting a victim to a false IP address. It consists in automatically redirecting users (visitors) of an Internet resource to another fake site. As a result, the victim does not visit the original pages, but those to which the fraudsters redirect him to receive confidential information.

The term "farming" is a neologism based on the word's "agriculture" and "phishing". Phishing is a type of social engineering attack to obtain access credentials such as usernames and passwords. In recent years, pharming and phishing have been used to obtain information for online identity theft. Pharming has become a major concern for e-commerce and internet hosting business. Sophisticated measures known as anti-farming are needed to defend against this serious threat [9, 36]. Even antivirus software and spyware removal cannot protect against pharming.

Social networks - in social networks, numerous users receive notifications from strangers or from friends in the contact list, with a request to visit the designated site or vote for them by sending SMS to a short number.

On social networks, scammers often change the status of users and post the information they need. Visiting these resources or sending SMS to the designated number. Most likely, the profile of the user from whom such messages come has been hacked, and a large mailing is being implemented on his behalf. When switching to the shown resources, there is a high possibility of infecting the computer with this or that malicious program, and then sending to the shown number can lead to the loss of a large amount of money from the account.

Voice phishing is a criminal practice of using social engineering through the telephone system to gain access to private, personal and financial information for financial reward. It is sometimes referred to as "vishing", a word that is a combination of "voice" and phishing. Voice phishing exploits public trust. Voice phishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals [6, 55]. Some scammers use features supported by Voice over IP (VoIP).

The construction of lies is identical with phishing, only in the case of vishing, the information contains a request to call a specific phone number. But a message is read out where the likely victim is asked to provide his personal data. It is difficult to find the owners of such a number, since with the development of Internet telephony, a call to a number can be directed to a virtual number anywhere. The caller does not think about it. This technology was used by many scammers.

According to information from Secure Computing, fraudsters also use the following scheme: the consumer receives a call and warns him that fraudulent transactions are being carried out with his card, and asks to immediately call back at a certain number. When this number is called back, a characteristically computer voice answers on the other side of the wire, saying that you must go through identification and enter the card number. As soon as the number is entered, the visher becomes the owner of all the necessary information. Further, using this call, you can save other information [15].

Malicious programs are also used to steal login and password. One stolen password can give access to many accounts and provides numerous opportunities for fraud 10, 114]. More than 13 million consumers fell victim to identity theft in 2014.

We also note other types of fraud, such as online store of confiscated goods; generator of express payment cards WebMoney; dummy programs; gold wallet, etc.

The United States Computer Emergency Readiness Team (US-CERT) identifies denial-of-service symptoms, which include:

- unusually low network performance (opening files or accessing websites);
- unavailability of a specific website;
- inability to access any website;
- a sharp increase in the number of spam emails received (this type of DoS attack is considered an email bomb);
- disconnect wireless or wired internet access;
- long-term denial of access to the network or any Internet services [8, 101-102].

If an attack is carried out on a large enough scale, entire geographic regions connected to the Internet can be compromised without the knowledge of the attacker or the intent of misconfiguration or contrived network infrastructure equipment.

One of the most popular ways to carry out a DDoS attack is to send multiple requests to the victim computer or site, which leads to a denial of service if the attacked computer's resources are insufficient to process all incoming requests.

On December 24, 2009, there was a massive DDoS attack on NeuStar's UltraDNS DNS service, which served a large number of large organizations. According to preliminary investiga-

tions, it was revealed that the NeuStar servers in California (USA) were most affected. A similar DDoS attack resulted in the shutdown of all online stores for about an hour. On August 26-27, 2009, the largest massive DDoS attack in the history of the country was registered in Ukraine. All attacks took place directly from computers on the territory of Ukraine. This time, hackers hacked the Imena.UA/MiroHost.net resource. According to the chief technical administrator, the load on the point of the provider's server increased to 2 Gb / s, which, of course, led to a collapse of the entire system.

The first computer hackers appeared at the Massachusetts Institute of Technology. They take their name from a term used to describe members of a train group who will "hack" electric trains, tracks and switches to make them run faster and differently. Several of the members transferred their skills to the new mainframe computing systems that were studied on campus. The malicious code of this time can be divided into two different categories: those intended to deceive the employer (back door, hatch, Trojan horse) and intended to blackmail or damage (logic bomb).

Phone hackers (phreaks or phreakers) are interrupting regional and international phone networks to make free calls. One intruder, John Draper (aka Cap'n Crunch), learns that a toy whistle given off inside Cap'n Crunch generates a 2600-hertz signal, the same high-pitched tone that accesses AT&T's long-distance switching system ... D. Draper builds a "blue box" that, when used in conjunction with a whistle and sounded into the handset, allows free calls. Shortly thereafter, Esquire magazine publishes Secrets of the Little Blue Box with manufacturing instructions, and fraud in the United States escalates. Among the criminals are two college kids (Steve Wozniak and Steve Jobs) later founders of Apple Computer.

Malicious code in computing remained broadly the same as in the 1960s. After a lengthy investigation, Secret Service agents carried out raids and arrests in 14 American cities. The organizers and prominent members of the BBS were arrested for credit card, telephone, and other fraudulent activities. The result is a breakdown in the hacker community. In 1990, self-modifying viruses such as Keith were created. In 1991 the GP1 virus appeared which is "network sensitive" and tries to steal Novell NetWare passwords. Since their inception, viruses have become more complex [7, 47-53].

Hacktivism represents a whole new level of activity on the World Wide Web. This is electronic civil disobedience. If we had widespread use of computers and the Internet in the 60s, the anti-war movement would have been carried out in the virtual space, not on American university campuses.

There are many topics today - globalization, human rights, environmental protection, and for each of them there were acts of electronic defiance against him. Hacktivism is more focused on political causes around the world and is truly global in nature, with examples such as the Hong Kong Blonde Anonymous Digital Coalition, X-ploit, the Dead Cow Cult and many more. It is likely that the Internet environment will continue to be exploited for civil disobedience and propaganda purposes.

The Shadow Server Foundation, which conducted statistical research on this topic, provides the following data on botnet activity for 2009-2010.According to researchers from Symantec, there is more than 5,000,000 botnets in the world, including more than 1,000,000 in the United States [2, 264].

DDoS attacks are classified into local and remote. Local exploits include various exploits, fork bombs, and programs that open a million files each time or run a specific cyclic algorithm that consumes memory and processor resources. Remote DDoS attacks are divided into two types: 1) Remote exploitation of software errors in order to render it inoperable; 2) Flood - sending a huge number of meaningless packets to the victim's address [1, 9].

Flood is divided into three types. Syn-flood - in this form, a significant number of SYN (synchronize) packets are sent to the attacked node via TCP (open requests). Moreover, after a

short time, the number of open sockets on the attacked server runs out and the server stops responding. Corresponding to the TCP "three-time handshake" process, the client sends a packet with a specific SYN flag. The server must then respond to the SYN + ACK (acknowledges) flag system. Then the client is obliged to respond with a packet with the ACK flag, after which the connection is calculated as entered. The order of the attack is that the attacker, by sending SYN requests, overflows the connection sequence on the server. But it ignores the target's SYN + ACK packets by not sending any reply packets, or spoofs the packet header so that the SYN + ACK reply goes to an imaginary address.

After connecting, the so-called half-open connections appear, waiting for confirmation from the client. After a certain time, these connections are thrown. The attacker's goal is to keep the turn full so that no new connections are missed. Because of this, legitimate customers cannot find a connection, or find it with significant interruptions.

UDP flood - this type of flood attacks not a computer, but its communication channel. ISPs reasonably believe that UDP is more successful than TCP. A significant number of UDP packets of various sizes awaken the communication channel, and the server operating over the TCP protocol stops responding. ICMP flood - in a distributed attack (from several thousand sites), ICMP requests arrive at the usual test speed (about 1 packet per second from a site), but at the same time from many thousand computers. In this case, the final overload on the aggregate, which is the target of the attack, can reach the bandwidth of the channel (and deliberately exceed the rate at which the device processes packets) [4, 23].

A malicious program is any software specialized in order to ensure the extraction of unauthorized access to information stored on a computer in order to cause damage to the owner of the information or the owner of the computer [2, 265].

Malicious programs reach computers in different ways: from a malicious site (for example, when downloading files); from a deliberately created site that contains malicious code; from a friend, an official website where the attackers installed malicious code; via flash cards, CDs, etc .; from a computer "neighboring" on the local network (Internet cafe, public wi-fi).

Malicious software injected on a user's computer can overwhelm passwords and other personal information, emit spam, and attack other computers on the network. When connected to the Internet, malicious software can automatically update itself and take orders from attackers. Consequently, they discreetly dispose of the taken computer. And the user, as a rule, does not think that someone else is using his computer. There are three main types of malware: 1) Computer viruses; 2) Network worms; 3) Trojans.

Activities related to malicious software include: the creation of malicious programs for electronic computers (computers) (viruses, Trojan horse programs, bots, sniffers (interceptors), etc.); introduction into existing programs of modifications that knowingly lead to unauthorized destruction, blocking, alteration or imitation of information, disruption of the operation of a computer, computer system or their network; the use of malware; distribution of malware or machine media with such programs.

Among the top ten malicious leaders as of February 2011, there were some programs for stealing funds from bank accounts, similar to the well-known Trojan, PWS, Panda, also eminent as Zeus. They are all transformations of one viral prototype [5, 178].

Modern technologies and societies, constant internet connections provide more business opportunities than ever before, including on the black market. Cybercriminals are carefully discovering new ways to target the world's most sensitive networks. Protecting business data is a growing concern. Here are the top threats to information security today: technologies with weak security; social attacks of media; mobile virology; third party records; neglect of the correct setting; outdated security software; social engineering; lack of encryption; corporate data on personal devices; inadequate security technologies[16].

Among the most acute threats to information security in the current period of development of society, the following can be noted: The creation and use of means of influence and damage to information resources and telecommunications systems of the country. Such means include: the capabilities of radio-electronic and other influences used for transient or irreversible containment of radio-electronic mechanisms and systems; means of influencing the software resources of the electronic manuals of the modules with the intention of disabling them; means of influencing the process of obtaining information with the intention of stopping it due to the influence on the environment of propagation of signals of influence; means of disinformation created in the information space of a virtual picture.

Usually the most expected result is the spread of doubt, rather than the adversary's acceptance of a certain untruth; means of influencing the psyche and subconscious of a person with the aim of disorganization, suppression of will or incapacitation; one of the types of informational influence is a combination of fiction with a metered amount of truth, as a result, this approach can lead to what is called a "political myth".

All of these listed information threats are directly experienced by the countries of the world. The peculiarity of this kind of offenses is that the victim may be in one country, and the one who committed the crime - in another. The Internet gives this type of crime an international character.

References:

1. Alguliev R.M., Aliguliyev R.M., Nazirova A. Classification of textual e-mail spam using data mining techniques // Applied Computational Intelligence and Soft Computing, 2011, vol. 2011, p. 9

2. Baron R.M.F. A critique of the international cyber crime treaty. / Comm-Law Conspectus, 2002, N.10, p. 265

3. Barr K., Beiting M. & Grezeskinski A. Intellectual property crimes. / American Criminal Law Review, 2003, N. 40, p. 771-823

4. Bick J. Spam is still lawful / New Jersey Law Journal. Retrieved June 4, 2004, p.23

5. Calkins M.M. The shoot Trojan horses, don't they? An economic analysis of anti-hacking regulatory models./ Georgetown Law Journal, 2000, N. 89, p. 178

6. Dawson Maurice. New Threats and Countermeasures in Digital Crime and Cyber Terrorism. (Advances in Digital Crime, Forensics, and Cyber Terrorism). Information Science Reference. 2015, 390 p.

7. Gelbstein Eduardo, Ahmad Kamal. Information Insecurity. A survival guide to the uncharted territories of cyber-threats and cyber-security. Published by the United Nations ICT Task Force and the United Nations Institute for Training and Research One United Nations Plaza, New York, 2002, 157

8. Kiyuna A., Conyers L. Cyberwarfare Sourcebook. Publisher: Lulu.com, 2015, 312 p.

9. Paquet Catherine. Implementing Cisco IOS Network Security (IINS 640-554) Foundation Learning Guide. (2nd Edition) (Foundation Learning Guides). Cisco Press, 2012, 704 p.

10. Power Andrew, Grainne Kirwan. Cyberpsychology and New Media: A Thematic Reader. 1st Edition, Psychology Press, 2013, 264 p.

11. Rowland D. Privacy, freedom of expression and Cyber Lapps: Fostering anonymity on the Internet? / International Review of Law Computers & Technology, 2003, N. 17(3). p. 303-312.

12. Shimeall J.Timothy., Spring M.Jonathan. Introduction to information security. A Strategic-based Approach. First edition. Elsevier publishing, Amsterdam, 2014, 360 p.

13. Smedinghoff J. Thomas. Information Security Law: The Emerging Standard for Corporate Compliance. IT Governance Publishing, 2008, 185 p.

14. Withers Katie. Brand on the run. British Retail Consortium. British Retail Consortium 2007. 185 p.

15. https://mmgp.ru/showthread.php?t=1169
16. http://scsonline.georgetown.edu/programs/masters-technology-management/resources/top-threats-to-information-technology
17. http://www.wikileaks.org/wiki/Wikileaks:About#Wikileaks_has_1.2_million_documents

Date of receipt of the article in the Editorial Office
(14.11.2019)