ТЕНДЕНЦІЇ РОЗВИТКУ НАУКОВОЇ ДУМКИ В МЕНЕДЖМЕНТІ, ГАЛУЗЯХ СПОРТУ, ОБСЛУГОВУВАННЯ ТА ОХОРОНИ ЗДОРОВ'Я

Тези доповідей

ІІІ Міжнародної студентської наукової конференції

(26-27 вересня 2024 року, м. Львів)

За загальною редакцією

Наталії ПАВЛЕНЧИК

Львів -2024

УДК 330.113.2

CONTEMPORARY PROBLEMS OF THE INTERNET AND THE NEED FOR INTERNATIONAL LEGAL MEANS TO RESOLVE THEM

Serik TOLKYNAI
student DI 24/1
Scientific supervisor – R.K. **TANIRBERGENOVA**
Senior lecturer
Institute of Design and
Technology «Symbat» ASEU (Kazakhstan)

Information technology, telecommunications and electronic computing equipment have already become inseparable parts of the everyday life of citizens of many countries. That is, life circumstances themselves are pushing the world towards complete digitalization and connection to the Internet. It is because of this that the relevance of understanding the operation of the fundamentals of computer networks is more relevant than ever. To clarify, digitalization or digital transformation is the process of creating and implementing digital technologies, as a result of which innovative products are formed, the appearance of the world economy and social interaction changes. Digitalization is continuously linked to the development of digital technologies, as a result of which such objects of activity as Big Data; Internet of Things; Virtual and augmented reality; 3D printing; Blockchain, etc. All these new phenomena relate to elements of the 4th industrial revolution, which is currently taking place in all the advanced countries of the Earth [1, p. 570].

The most frequently encountered cybercrimes in the media, as well as from statements by high-ranking officials of most countries, can be divided into several categories:

1) Cyberbullying is one of the types of aggressive behavior, or more precisely, the use of digital media for the purpose of psychological persecution of third parties. Bullying can cause emotional and mental harm, as well as affect a person's personality. Victims may receive harmful and offensive messages or posts on

social networks that imply a threat of violence, damage to property, harass victims or threaten their lives [1, p. 101].

2) Phishing (from English fishing - fishing) is one of the most popular attacks due to its direct connection with the end user. In such cases, the attacker tries to deceive the end user in order to provide him with confidential information. Phishing includes a combination of substitution and social engineering methods. The victim receives an email asking for sensitive information, warning about an attack, and asking to install new security software, which is actually malware. Alternatively, a phishing email may contain a link to a fake website. One important defense is to not click on the link that appears in a suspicious email. Other ways to protect yourself from phishing attacks include visiting only secure websites that have “https” in the URL and installing antivirus software, firewalls, and anti-phishing toolbars. 3) DoS Attack – Denial of Service (DoS) attacks are a serious threat in which an attacker compromises the availability of services. DoS causes compromised systems to crash with a huge number of requests, such as Internet Control Message Protocol (ICMP) and SYN flood, causing the systems to crash and the intended services to be terminated. Another type of DoS attack is called a Distributed Denial of Service (DDoS) attack, the attacker has access to many channels on the network and each victim becomes an agent to attack another system, like a zombie.

4) SQL Injection – this is a type of attack where the attacker compromises the databases using some SQL queries. The attacker can view the database and extract its contents before changing or deleting the data. One of the best strategies to prevent this type of attack is to set a high standard level of credentials, such as username and password, for all users.

5) Cyberespionage – this refers to any activity that involves illegal intelligence activities and theft of important and confidential information for the benefit of competing companies or foreign governments. Cyber espionage uses computers to carry out missions.

6) Cyberterrorism – this is an illegal act that involves violence against people and property. This concept is only partially related to the concept of “Act of Terrorism” in the Criminal Code of the Republic of Kazakhstan, since in domestic legislation this concept means the commission of an explosion, arson or other actions that create a danger of death of people, causing significant property damage [2, p. 95].
7) Cyberwarfare is a type of warfare that uses cyber attacks rather than weapons or physical methods. It can be carried out by organizations or groups of hackers without government permission, which can lead to political problems between countries. Today, cyber wars and cyber attacks are the most common type of military action.

Due to the heated political situation in the country neighboring Kazakhstan, namely the Russian Federation, hacker attacks on the services of companies from this state have intensified, it should be noted that Kazakhstanis are also users of these information services. In February 2022, the international hacker group "Anonymous" declared war on Russia in its Twitter account.

According to international expert communities, the damage caused by cybercrime will increase annually, reaching US$10.5 trillion per year in 2025. Cybersecurity Ventures expects global spending on cybercrime to grow by 15 percent per year over the next five years, reaching US$10.5 trillion per year by 2025, up from US$3 trillion in 2015. This represents the largest transfer of economic wealth in history, threatens incentives for innovation and investment, exponentially exceeds the damage caused by natural disasters in a year, and will be more profitable than the global trade in all major illicit drugs combined. The cost estimate is based on historical cybercrime metrics, including recent year-on-year increases, a sharp increase in hacking activity sponsored by hostile nation-states and organized crime groups, and the scale of cyberattacks, which will be an order of magnitude larger in 2025 than today [3].

Indeed, much of the discussion in recent years about equipping a beleaguered and under-equipped police force to deal with technology is quickly giving way to growing concerns about over-surveillance due to the gradual “hard-

wiring of society.” A delicate balance must be struck between the need to maintain order and the enforcement of laws, to ensure that the requirements of the law are balanced with the desires of law enforcement. Without such a balance, every violation of the law can be easily and automatically detected by technology, and we will begin to descend into a world of strict liability, characterized by an inverted burden of proof.

References:

1. Mogunova M. M. Cyberbullying as a New Danger. *Bulletin of the North Kazakhstan University named after M. Kozybayev*. 2022. No 2(51). P. 99–106.

2. Temiraliev T. S., Omarov E. A. Problems of Counteracting Crimes Committed with the Use of Information Systems and Ways to Solve *Them. Bulletin of the Institute of Legislation of the Republic of Kazakhstan*. 2019. No 1(55). P. 93–99.

3. Morgan S. Cybercrime to Cost the World $10.5 Trillion Annually by 2025. URL: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/