International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 7.502 Impact factor
Volume-11| Issue-11| 2023 Published: |22-11-2023|

CHALLENGES IN COUNTERING AND PREVENTING SOCIAL MEDIA CALLS FOR MASS PUBLIC SAFETY VIOLATIONS

https://doi.org/10.5281/zenodo.10129845

A.Abduraxmonov
University of Public safety of the Republic of Uzbekistan
graduate student

Annotation

This article elaborates on the challenges that arise in combating and preventing calls for mass public safety violations from Social Media. An analysis of decisions in this area is provided as additional information. The author summarizes all the points through empirical research method.

Keywords

violations, cybercrime, analysis, virtual networks, offenses, preventing

Introduction. Among the global problems of our century are mentioned again and again with new types cybercrime has also become much more accessible. His viral programs known to us distribution, breaking passwords, credit card and other bank details funds embezzlement looting, as well as information contrary to the internet orgal law, in particular, great danger to the life of mankind with the dissemination of obscene, spiritually corrupted information we can't turn a blind eye to what is asking. The concept of "cybercrime" from the means of information and Communication Technology using, horror on the virtual network, viruses and other malware, to the law preparation and dissemination of contradictory information, mass distribution of electronic letters (spam), hacking attack, illegal access to websites, fraud, data integrity and copyright violation, credit card number and theft of bank details (fishing and farming) and it is explained by various other offenses[1].

Method. At the same time, the scale of cyberterrorism and its danger to the life of society also increases it is worth noting that it is going. Cyberterrorist movement (cyberattack) - computers and information implemented with the help of communication tools, to the life and health of people to material objects, which are directly dangerous or can pose a potential danger of socially dangerous consequences, which can cause great harm or the like is a political reason that has a beginning or purpose[2]. For modern terrorists the attractiveness of the use of cyberspace the implementation of cyberbullying is a huge financial related to the fact that it does not require costs. experts conclude that this is an assistance to the development of developing countries, influence on the minds of citizens under the guise of finding decisions of universal democratic principles the transfer is carried out by subjecting them to their goals in different ways.

Unfortunately, organizing cyber attacks in the process is unparalleled by the internet global network along the way attempts to "effectively" use their capabilities are increasingly underway. Social networks available on the internet, sovereign of their producers and sponsors it is because the role' interference[3] ' in the internal affairs of the state has not been studied until the end sometimes it is not yet recognized that such an" intervention " is against this state. Owners of social networks are encouraged to overthrow the state system on the pages of these networks the international legal framework for the prosecution of the case has not been established. However, according to the essence of the content of each committed criminal behavior or inaction, of course, it should not remain unanswered and unpunished. Internet sites appear suddenly, often changing their format and then their address. Shu bois some experts have abandoned early concepts such as the whole openness of the internet, it is offering a transition to its new system. The main essence of the new model is to abandon the anonymity of network users[4]. This makes it possible to ensure that the network is even more protected from criminal encroachments gave. As an example, the Chinese state, which switched to a closed network system, and to such a process we can cite the state of Russia, which is preparing. To the world community Information Communication Technologies, information in an integrated country consistent state on the effective use of systems and modern computer technologies the policy is underway[5].

Results Modern digital, which is being introduced in our country today technologies are opening the door to a number of amenities and opportunities for our citizens. This in addition to the process, ragamli technologies and information systems being created there is also the problem of ensuring safety, of course. This is one of the most pressing issues - the provision of cybersecurity, which can be committed it is considered a matter of preventing and combating cybercrime. Cybersecurity against cybercrime, which is improving day by day protection against them by fulfilling the following basic requirements in the provision, i.e. we can provide cyber security[6]`:

- teaching employees the basics of Information Security;
- continuous testing of vulnerabilities of software products in use;

- using reliable antivirus software;
- using licensed official software;
- the use of multi-factor authentication in the protection of Information Systems;
- compliance with a strong password storage policy when using passwords;
- encrypt data on computer hard drives on a regular basis.

Discussion the same time, to prevent cybercrime in our country and bring the fight against it to highlight the fact that certain tasks are also assigned to the outgoing competent government agencies l In particular, they are involved in the activities of the fight against cybercrime against the Republic of Uzbekistan and its to which the people are implemented through information technology and communications, or to which the individual, society and the state that allow their security and their interests are external and ensuring protection against internal cyberattacks, legitimacy and law in this area strengthening its priority[7], preventing cybercrime and cyberattacks, making them darcor that it performs tasks such as detection and elimination. Also, the investigation of cybercrime and cyberattacks and their detection, elimination.to make the necessary decisions on implementation and Prevention[8], to combat cybercrime participation in the development of draft regulatory legal acts on cyberterrorism, cyberextremism, struggle against organized crime, in the interests of state bodies and to identify and combat cyberattacks that threaten cybersecurity, conducting an investigation and preliminary investigation in advance of an investigation into cybercrime, prompt-search carrying out its activities, threatening the rights and freedoms of citizens determination of possible causes and conditions for the occurrence of cybercrime and they must perform such important tasks as elimination.

REFERENCES:

1. Handbuch Translation /M. Snell-Hornby, H. Honig,P. Kussmaul, P. Schmitt. - Tiibingen: Stauffenburg, 1999.

2. Alekseeva I. S. Text and Translation/I. S. Alekseeva. M., 2008.

3. Kushnina L. V. The theory of harmonization : The experience of translation-grated Approach / M. Snell-Hornby. - Amsterdam; Phila- nitive analysis of the translation space /delphia, 1988.

4. L. V. Kushnina. - Perm, 2008.Russian State Pedagogical University- Herzen State Pedagogical University ofRussia A. I. Herzen University

5. Pedagogical technologies: Textbook / Author. comp. T. P. Salnikova. - M.:Shopping center Sphere, 2008. - 128 p.

6. Selevko G. K. Modern educational technologies. - M.: Public education, 1998. - 256 p.

7. Shchepkina N. K. Modern pedagogical technologies in teaching: A textbook for students of higher educational institutions. - Blagoveshchensk, 2005

8. [Electronic resource]:// www.amursu.ru/attachments/article/6149 /Method%20posobie%20po%20 Ped%20 technol.pdf